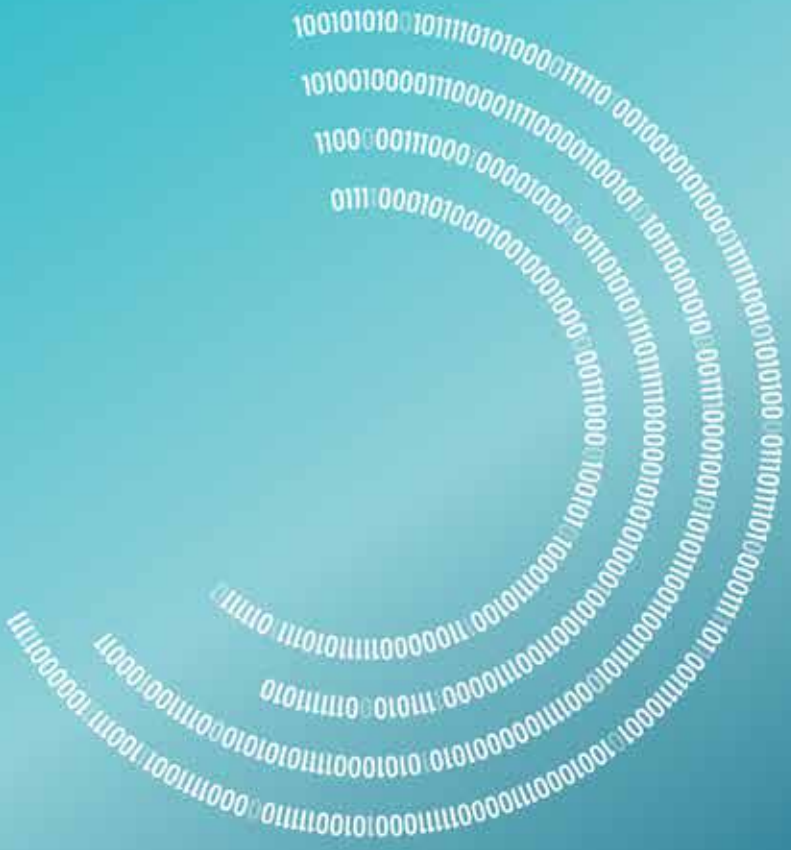

Regulation in Cyberspace

Gabi Siboni and Ido Sivan-Sevilla

Memorandum
190

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Regulation in Cyberspace

Gabi Siboni and Ido Sivan-Sevilla

Regulation in Cyberspace

Gabi Siboni and Ido Sivan-Sevilla

Memorandum No. 190 April 2019

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

רגולציה במרחב הסייבר

גבי סיבוני ועידו סיון־סבילה

Institute for National Security Studies (a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556 Israel

Tel. +972-3-640-0400
Fax. +972-3-744-7590

E-mail: info@inss.org.il
http://www.inss.org.il

Copy editor: Ela Greenberg
Graphic design: Michal Semo Kovetz and Yael Bieber,
TAU Graphic Design Studio
Printing: Digiprint Zahav Ltd., Tel Aviv

April 2019

ISBN: 978-965-92713-6-8

Contents

Executive Summary 9
Insights from the Literature 10
A Proposed Regulatory Model 11
Recommendations 14

Introduction **17**

Chapter 1: Introduction to Regulation in Cyberspace 25

Chapter 2: Survey of the Literature 37
The United States 37
The European Union 59
Britain 68
France 77
Germany 84
Israel 94
Other Regulatory Issues 109
Overall Insights from the Literature Review 117
The Development of Regulation in the West—
A Comparative Summary 120

Chapter 3: Regulatory Models in Other Domains 123
The Regulatory Model in the Domain of Environmental
Protection 123
The Regulatory Model in the Nuclear Energy Sector 135

Chapter 4: Proposed Regulatory Model for Cyberspace in Israel 141
Self-Regulation 143
Binding Regulation 143
Incentive-Based Regulation 160

Chapter 5: Recommendations for Implementing the Proposed Model 165
The Self-Regulation Model 166
The Binding Regulation Model 166
Incentive-Based Regulation 168

Conclusion 171

Acknowledgments

First, we would like to thank Maj. Gen. (ret.) Amos Yadlin, the director of the Institute for National Security Studies, for his helpful comments. Similarly, we would like to thank the researchers of INSS who provided highly insightful comments during the writing and reviewing of the essay: Dr. Anat Kurz and Brig. Gen. (ret.) Shlomo Brom. Thanks also go to the researchers Hadas Klein and Dudi Siman Tov for their comments on the variety of topics discussed in this essay. Many thanks also to Judy Rosen and Moshe Grundman for their comments and efforts in publishing the essay.

We wish to thank the many interviewees who helped explain the complexity of the regulatory efforts in cyberspace. Following is a partial list of those who can be named: Gideon Confino, the head of the Unit for Cyber Protection in the Government ICT Authority (Yahav); Aviram Atzaba and Yuval Segev of the National Cyber Directorate; Limor Shmerling from the Privacy Protection Authority; Nir Heller of the Director of Security of the Defense Establishment; Natan Hershkovitz, the director of the Information Systems Department at the Israel Securities Authority; Rachel Yaacobi, the director of Technology and Cyber in Banking Supervision at the Bank of Israel; and Shlomo Harnoy, CEO of the Sdema Group, which works with the Ministry of Energy.

In addition, we would like to thank the dear interns who assisted in the analysis and gathering of information for this essay: Benjamin Goh of Harvard University, David Futscher of University of Texas at Austin in the United States, and Sanjana Rathi of the London School of Economics and Interpol. Finally, we would like to thank members of the Cyber Forum at INSS for their helpful suggestions along the way and the sharing of information.

Gabi Siboni and Ido Sivan-Sevilla
April 2019

Executive Summary

Regulation in cyberspace is an emerging challenge. It is a complex and dynamic domain that is largely driven by the business-civilian sector and has the potential to cause significant damage to national security. This essay surveys the unique characteristics of cyberspace and the various strategies adopted in other countries in order to manage cyber risk. It proposes a multi-layered regulatory model together with concrete recommendations for the regulation of the business-civilian sector in cyberspace.

The resilience of the private sector in cyberspace is directly related to national security. The private sector usually constitutes the weak point where a cyberattack develops. Nonetheless, the survey of regulation in cyberspace in Western countries, including Israel, points to the lack of an appropriate response to this weakness. This essay attempts to fill that gap and, in order to do so, it makes use of the regulatory principles used by other countries—the United States, Britain, France, Germany, and the European Union—and also learns from other regulated domains, namely environmental protection and nuclear energy. National approaches, the variety of regulatory tools, and the systems of incentives used in the attempts to regulate cyberspace worldwide, together with models for collaboration between the public and private sectors and state compensation mechanisms that were observed in environmental protection and nuclear energy domains, have contributed to the development of an innovative regulatory model for cyberspace in the business-civilian sector in Israel.

The model proposed in this study is presented together with practical recommendations. The model is divided into three components: self-regulation in which organizations impose practices on themselves; binding regulation in which the state hierarchically imposes and enforces required practices; and incentive-based regulation in which the state creates incentives for organizations to adopt self-regulation. The first innovation of the model is related to the use of an existing statutory tool, namely the Business

Licensing Law. It can be used to map the potential damage to national security as the result of cyberattacks on the business sector in a very early stage. The second innovation is the mapping and emphasizing of central resiliency points in Israel's cyber economy and the assessment of possible state intervention whose benefit is many magnitudes larger than its cost. The third innovation is the strengthening of incentive mechanisms for the economy by the establishment of a cyber insurance market, the removal of barriers to data breach notification, tax breaks for installers of cyber protection, and the provision of incentives in the form of exemption from responsibility for intra- and inter-sectoral threat information sharing.

Insights from the Literature

The main insights from surveying the literature on cyber regulation demonstrate the high degree of variation in cyber regulation across countries. The activity of each country in cyberspace began at different points in time and focuses on threats to national security, such as attacks on critical infrastructure or protection against cyber crime. All the countries surveyed devote large budgets to cybersecurity, which are designated for state capabilities and institutions that can supervise and influence developments in the local cyber economy, including its various threatened domains. This is based on both the conception that risk assessment in cyberspace is one of the most challenging tasks for regulators and there is need to increase expertise through the broadest possible understanding of developments in this domain. Nonetheless and despite the investment of budgets and the creation of state capabilities to deal with cyber risk, there is a glaring lack of state activity to deal with these risks in the business-civilian sector. There are currently no countries that systematically regulate the business-civilian sector and relate at an early stage to national security threats as a result of cyberattacks on this sector.

The Israeli approach to cyber threats in the business-civilian sector is innovative and relatively decentralized. The regulation of the business sector is in the hands of various regulators and is sometimes overseen directly by the relevant government ministry (such as in the case of healthcare), the relevant state authority (for example, the supervisor of the banks) or a private organization with expertise in the domain that is hired by the state as a regulatory intermediary (for example, in the case of the Ministry of Energy). During the past two years, attempts have been made to centralize the process

of decision making with respect to the cyber domain for the entire economy, whereas the Cyber Law—which is still in the stage of negotiations—is meant to serve as a guiding framework for selected organizations in the economy. However, even this development has not yet created a systematic and organized process for the early identification of potential damage that cyberattacks could cause to national security.

The lack of a comprehensive response to deal with the multiplying cyber threats in the business-civilian sector and the current focus on only localized incentives create a major gap in this domain. Based on the activity in the economy in recent years, it appears that the market is compensating companies for technological innovation far more than for appropriate cyber protection. As a result, companies do not invest sufficiently in order to create comprehensive protection for themselves. In the absence of systematic state oversight in this domain, a vacuum has been created that needs to be filled.

In order to find the proper model for successfully tackling cyber threats in the business-civilian sector, the authors of this essay turned to other regulated domains. It was assumed that an analysis of what is being done in environmental protection and nuclear energy—domains in which private players account for a large share of the activity and in most cases constitute the state's "first line of defense" against risk—will benefit in developing a sophisticated model for cyber protection in the business-civilian sector in Israel. The analysis led to the conclusion that the regulatory model for environmental protection in Israel is an appropriate foundation for the development of regulation in Israel's cyberspace.

A Proposed Regulatory Model

The advanced threats in cyberspace create an immediate need for smart state intervention that combines a variety of regulatory tools. This is in order to ensure the adoption of appropriate protective measures and to encourage the market to protect itself in response to incentives, while identifying the main locations where the benefit of protection exceeds the cost.

The proposed model for cyber regulation is based on what currently exists, while introducing improvements and extensions. The model differentiates between self-regulation, binding state regulation, and incentive-based voluntary regulation as follows:

1. **Self-regulation**: Defense organizations with a high level of sensitivity, such as the Israel Defense Forces (IDF), the General Security Services (GSS),

the Mossad, and the Israel Police, will be subject to internal regulation only, which the risk management mechanisms of each organization will oversee at periodic intervals.

2. **Binding regulation**: The state will impose regulation on entities should an attack on their cyber infrastructure result in significant damage to Israel's national security.
3. **Incentive-based regulation**: This involves the structuring of state incentives to encourage the creation of cybersecurity mechanisms within organizations. This regulation will, in part, encourage businesses to acquire insurance against cyber events, based on a regime of mandatory reporting. In addition, various models for the provision of tax breaks, subject to an organization's investment in cybersecurity, will be presented and efforts will be made to develop information-sharing mechanisms, with the goal of strengthening overall resilience in cyberspace.

The bodies that will be subject to **binding regulation** are divided into the following five categories:

4. **Defense industries and sensitive facilities:** These will be supervised by the Director of Security of the Defense Establishment (DSDE). The directives of the DSDE are intended to maintain the confidentiality of the work done by defense organizations under its auspices. It is worth mentioning in this context that DSDE regulation includes both security directives in cyberspace for supervised organizations and regulatory governance. In other words, the DSDE regulation is meant to achieve both national security and the functional continuity of the supervised organizations.
5. **Organizations defined as critical infrastructure:** The supervision of these organizations will remain as it is today; that is, supervision by both the National Cyber Directorate and the GSS. The steering committee, which will be composed of representatives of the GSS, the National Cyber Directorate, the ministries of government infrastructures, and private companies involved in the protection of critical infrastructure, will examine and redefine critical infrastructures if necessary, and these will have to meet strict standards, including frequent periodic inspections, according to the type of infrastructure. The steering committee will also periodically consider adding new organizations to the list of critical infrastructures or removing existing ones. The National Cyber Directorate

will accumulate knowledge and expertise, in collaboration with the GSS, with the goal of protecting critical infrastructure organizations.

6. **Economic sectors essential to Israel's functional continuity:** In addition to the bodies defined as critical infrastructure, numerous systems and entities are important to national security but have not been defined as critical by the state. These include, for example, hospitals, traffic lights, election systems, banks, and food industries. Therefore, the sectoral regulators in these domains need to develop expertise and to direct the entities under their responsibility on how to deal with cyber threats, in order to prevent harming Israel's national security. The proposed model recommends to continue and rely upon the sectoral regulators that work against those organizations having the potential of damaging national security. The model also supports the sectoral regulators to rely upon external experts who will be hired under the direction of the National Cyber Directorate, enabling professional guidance of bodies that are significant to national security and, in parallel, the binding guidance of the sectoral regulators in the domain under their responsibility.
7. **The business-civilian sector:** The proposed model requires every business organization that requests or renews a business license to check for feasible damage to national security as a result of a cyberattack. This will create a structured process that will substantially improve the protection of private sector projects that are exposed to a cyberattack, the effect of which might be felt on the national level. The cyber regulators in this sector will be both the National Cyber Directorate, whose job is to develop knowledge, tools, and methods that organizations can use to improve their level of cyber protection, and the sectoral regulators who develop expertise according to the needs of their specific sector and make the necessary adjustments to the general directives issued by the National Cyber Directorate. The proposed process makes use of existing statutory tools and introduces cybersecurity as a built-in component of the business sector, while making use of the existing statutory process. The regulator will establish standards that will define the projects required to submit a cyber resilience review, which will be a condition for receiving a business license. The model also suggests several guidelines for the content of the cyber resilience review, as well as the entities that should be certified to implement and submit it, and those that should be certified to evaluate it.

8. **Increasing the resilience of cyberspace by means of intervention at central points:** Binding regulation according to the proposed model will also apply to central points where state intervention in protecting them will produce major benefit at little cost. The rationale behind identifying these critical points is that their supervision has substantial benefit to national security. It should be emphasized that the state will not serve as the executive arm with respect to these points and that its function will be restricted to mapping the points and cooperating with the relevant suppliers, with the goal of encouraging their security and thus increasing the resilience of Israeli cyberspace. Examples of such points are internet hosts; service providers that horizontally span the supply chains of organizations in the economy; application software and centralized information systems used in clearing credit card transactions, upon which most private businesses rely; and integrative companies that provide support for information systems. After identifying these points, the state will need to employ third-party suppliers who will be responsible for the quality assurance of these critical service providers.

Recommendations

Following are the main recommendations that will support the implementation of the proposed regulatory model:

1. Evaluation of the need to create a professional and independent auditing unit within the National Cyber Directorate that will be active among bodies, organizations, and institutions within the framework of self-regulation (the security organizations, the IDF, the Israel Police, and so forth).
2. Creation of a forum within the government's ICT Authority that will generate a cross-sectional picture of the regulatory techniques chosen by the government ministries and authorities to protect the various sectors under their responsibility, with the goal of learning and improving efficiency.
3. Strengthening enforcement by the Ministry of the Economy in order to improve compliance with the Business Licensing Law.
4. Establishment of an executive arm within the National Cyber Directorate for overseeing the reviews of cyber resilience in the economy.

5. Promoting the standardization of cyber professions with the goal of, among others, establishing standards for testing the quality of cybersecurity and carrying out reviews of cyber resilience.
6. Creation of a forum of the National Cyber Directorate, the government's ICT Authority, and leading technological companies in the economy for the purpose of identification, analysis, and protection of critical points in cyberspace, in order to strengthen national resilience.
7. The promotion of a law that will require all organizations in the economy to report a "significant" cyberattack. Its purpose will be to motivate organizations to acquire protection and to facilitate the creation of an actuarial database for the use of insurance companies and thus encourage them to develop a market for cybersecurity insurance policies.
8. The allocation of a designated government budget to the Capital Market, Insurance, and Saving Authority with the goal of creating a state guarantee for insurance companies in the event of a mass cyber event.
9. Examination of the possibility that the government will provide tax breaks for the installation of sufficient cyber protection.
10. Creation of a designated cyber unit in the Tax Authority that will consider the provision of tax breaks for the installation of sufficient cyber protection.
11. Promotion of legislation that would provide an exemption from responsibility in the case of a cyberattack as a result of inter-organizational sharing of knowledge of cyberthreats.

The conclusion of the essay presents insights from the regulatory efforts in cyberspace and describes future challenges. The development of the reference threat originating from the Internet of Things[1] and the use of artificial intelligence in cyberattacks intensify the need for a multi-layered regulatory model for the business-civilian sector in a way that anticipates future challenges.

---

1 The Internet of Things is made up of home and industrial devices, such as security cameras and thermostats, whose interconnectivity has been facilitated by the internet. Its existence means that cyberspace now includes not only computers and information systems but also more simple devices that send information and can be controlled remotely.

Introduction

The cybersecurity challenge cuts across disciplines, sectors, and methodologies. Understanding how the state should intervene in order to ensure the resilience of its cyberspace and prevent harm to businesses' continuity and national security has numerous dimensions and exposes interests and forces that often operate in opposite directions.

This essay presents the core of the problem, surveys the background and the historical development of cyber regulation in the leading Western countries, and proposes an integrated regulatory model that will strengthen national security through cyberspace protection.

Countries worldwide use multiple tools for cyber protection, which combine binding regulation with one that encourages cooperation between the private and public sectors. In contrast, the business-civilian sector remains largely without a systematic solution in this domain and protects itself according to self-discretion and business interests. This situation constitutes a risk of the first order to national security. The vulnerability of the business-civilian sector as a domain without territorial borders creates fertile ground for attackers by providing access to defense systems, business services, and highly personal information.

This essay attempts to meet the challenge posed before national security and does so by examining the cybersecurity situation in other countries and in other regulatory domains, namely environmental protection and nuclear energy. The essay proposes a conceptual framework and a new regulatory model that will reinforce cyber resilience in Israel and, as a result, will increase national security. The proposed model can be implemented in any country dealing with similar challenges.

The research questions of this essay are as follows:

1. What are the laws and the institutions that form the basis for the State of Israel's efforts in the area of cybersecurity?

2. How do Western countries regulate cybersecurity in general and in the business-civilian sector in particular?
3. What can be learned from the regulation of environmental protection and nuclear energy and can be applied to cyber protection in the business-civilian sector?
4. What is a possible model for the regulation of cybersecurity in the business-civilian sector in the State of Israel?

The methods for examining these research questions consist first and foremost of the systematic gathering of policy documents—laws, secondary regulations, regulatory directives, and temporary orders in Israel, the United States, the European Union, Britain, France, and Germany—which deal with cybersecurity and information security, starting from the 1990s until today. After mapping the policies implemented in each country, the essay describes what is being done in Israel in this domain and surveys additional regulatory models in the areas of environmental protection and nuclear energy. This is part of an effort to adopt—at least in part—regulatory models that have been successfully implemented in the business-civilian sector. The development of proposed model is based on information gathered and on interviews with decision makers in Israel and is meant to offer a regulatory framework that will ensure Israel's national security.

The difficulties encountered in this research stemmed primarily from the need to understand a domain in which threats change rapidly and the pace of development is faster than policymakers' response. Offensive and defensive cyber technologies develop at a rapid pace and the domain itself is expanding to include a wide array of connected devices in the age of Internet of Things. In contrast, the state regulation of cyberspace rests on regulatory institutions and decision makers that usually operate in a way that lags behind the pace of technological development. Another problem is the challenge of creating a new regulatory model that is based on the experience of other countries in dealing with parallel challenges and on the regulation in other domains. The shift from theory to practice is a challenge for any policy recommendation and this is all the more so in cyberspace, since the applicability of the model must be based on the regulator and the feasibility of implementation by decision makers on the one hand and acceptance by the potential beneficiaries of the regulation on the other, a hurdle that cannot always be predicted.

Dealing with these problems calls for frequently updating the survey of sources and considering all the challenges up until the last moment. Therefore, we have added to the literature review an overview about the challenges in the era of the Internet of Things and a survey of the cyber insurance market, which have recently been the subjects of intense interest both in the business-civilian sector and among various regulators around the world. In addition, and in order to formulate a model that is feasible to implement, we took into account the directives and incentives that exist in other countries, which lead to a model that does not solely focus on stringent enforcement by state command and control mechanisms but also integrates dialogue and self-regulatory mechanisms across actors in the economy.

This is also the source of some of the research's innovation expressed in this essay. To date, no comprehensive model has been presented that combines binding regulation, self-regulation, and the creation of incentives for the economy, together with a comparison of what is being done worldwide and in other regulatory domains. The current research also provides a comprehensive review of how leading Western countries are dealing with the cyber challenge and makes it possible to understand the similarities and differences in how countries choose to construct their regulatory regimes. Another innovation involves the recommendations to decision makers, which emerge from this research's broad perspective, and the mapping of key critical points in cyberspace, including a variety of incentives that are intended to create efficient cybersecurity self-regulation.

The essay is structured as follows: Chapter 1 is an introduction to regulation in cyberspace and surveys the challenges to the domain's resilience, the inherent market failures in the domain—which create significant gaps in the economy's defense—and the potential harm that these gaps create for national security. The survey strengthens the insight that although Western countries are expanding risk management for society, cyber risks are being handled with a more narrow and localized perspective, without an overall strategy or systematic processes in the case of most players in the economy. The chapter also defines the concept of "regulation" according to the academic literature, describes the concept's historical development in the United States and Europe, and reviews the most important research literature on the subject, which deals with, among other things, justifications of regulation, explanations of how it has developed, and changes in the way it has been implemented in contemporary governance mechanisms. The

claim of this research is that regulation is the main tool available to the government for increasing state presence in various domains of activity. Regulation is expanding despite the dominance of neoliberalism and free market principles and plays an important and ongoing function in building markets and protecting the public interest.

Chapter 2 includes a review of the literature on cyber regulation in the United States (on both the federal and state levels), the European Union, Britain, France, Germany, and Israel. The table of comparison between the countries at the end of the chapter illustrates the variation in the development of cyber regulation, with respect to institutional structure, the influence of the defense establishment, and the incentives provided in order to strengthen the economy's protection. Nonetheless, it is possible to discern a great similarity in the way that countries deal with the business-civilian sector, which includes localized and usually declarative solutions that lack any organized process for the management of cyber risk.

The survey of the literature also looks at two new phenomena faced by decision makers. The first relates to the Internet of Things; that is, the new devices that have connective ability, in a manner that is changing the domain of the traditional cyber threat. The second relates to the developing cyber insurance market and suggests a new approach to the distribution of risks in cyberspace. These two phenomena cut across countries and are still in the early stages of development. The survey of the literature looks at the roots of the disagreements surrounding the regulation of these domains and raises fundamental questions about the future faced by decision makers.

Chapter 3 looks at lessons to be learned from other domains, namely environmental protection and nuclear energy. The chapter surveys and then adopts regulatory principles that are successfully applied in these domains, with the intention of using them to strengthen cyber protection and national security. The survey of environmental regulation includes a description of how it has developed in Israel and highlights the similarities between the domains of environmental protection and cyber. In this context, the chapter analyzes the regulatory tool of environmental impact assessments and its implications for regulation in the business-civilian sector.

Several of the regulatory principles in the domain of environmental protection can be adopted in cyberspace. This includes the overall approach to environmental protection, which rather than focusing on a particular kind of pollution seeks to achieve a general understanding of the direct and

indirect implications of each environmental threat. In addition, the incentive mechanisms for industry and the avoidance of an excessive number of decision makers in the domain of environmental protection (in parallel to the problematic culture of compliance in Israel) are important and relevant principles for implementing any potential regulatory model for cyber protection in the economy. Finally, adopting environmental impact assessments as a policy tool for the early mapping of cyber threats should help to change the narrow and localized way in which the business-civilian sector currently deals with cyber risks.

The domain of nuclear energy provides an example of cooperation in the private sector, which has led to high professional standards and the development of knowledge. It also illustrates the ability of an international body to enforce compliance with uniform norms among a broad cross-section of countries and presents examples of state intervention to provide compensation in the event of a nuclear accident. The aforementioned enable industry and the insurance market to develop and flourish and can serve as a reference point for cyberspace regulatory challenges as well.

Chapter 4 presents the proposed regulatory model. This model is divided into three components: self-regulation, binding regulation, and incentive-based regulation. The model is based on the regulation that already exists in Israel and seeks to extend it in order to provide a solution also in the business-civilian sector. Improvements and upgrades to existing regulation are proposed for each of the model's elements.

The **self-regulatory model**, which applies to sensitive organizations in the defense establishment, includes the addition of monitoring capabilities and the development of defensive expertise in cyberspace by auditors. The **binding regulatory model** applies to a variety of sectors—defense installations, critical infrastructures, sensitive organizations in the business sector that are regulated on a localized basis, long-term initiatives and projects that require approval and licensing, and service providers that have major importance for economic activity. This variety of sectors is currently regulated and supervised by designated state authorities. There are two main innovations in the proposed model: The first relates to the use of the Business Licensing Law for the mapping of potential cyber harm in the business-civilian sector. This is accomplished by introducing a review of impact on national security as a result of potential cyberattacks on the relevant organizations. Any organization that requests a license will fill in

a questionnaire on potential damage, under the supervision of the National Cyber Directorate, which is responsible for the development of knowledge and expertise in the domain. This questionnaire will be used to formulate the instructions for reviewing and mapping cyber risks before they develop.

The second innovation in the binding regulatory model relates to the mapping of the main points that are important to the economy as a whole and for localized state intervention, with the goal of ensuring the optimal and secure supply of services to the various companies. Possible examples include internet service providers, the main service providers in supply chains, site hosts, integrators of technology in various sectors, and providers of business services to the economy as a whole. The aforementioned can decisively affect the potential for harm by various cyber threats. Improving the protection against these threats, combined with supervising how that is accomplished, will reinforce the resilience of the Israeli cyberspace and national security in general.

The **incentive-based regulatory model** deals with areas in which the business sector can be incentivized to work toward improving its cyber resilience as well as its national strength. Encouraging the creation of a cyber insurance market in Israel, together with removing the barriers to transparency with regard to cyber incidents in organizations, will help to attract players with a strong financial base, such as insurance companies, to become involved in cyber protection efforts. An additional incentive is the provision of tax incentives to organizations that install sufficient cyber protection. Such an incentive can help change the problematic equation according to which the market prefers to promote innovation and technology over security and privacy in cyberspace. Finally, incentives for the sharing of knowledge among competing private actors for the purpose of creating a collective knowledge of threats that allows the implementing of pro-active steps to prevent cyber incidents will help to forestall cyberattacks. Such incentives can include removing business responsibility in the case of cyber events as a result of information that was shared. This will make it possible to create a basis for cooperation and to view cyber protection as a shared challenge and a public good.

Chapter 5 presents the recommendations for implementing the proposed model, which has three components. The recommendations relate first to sensitive organizations that are subject to self-regulation. Expanding supervision over these organizations can be expected to encounter organizational barriers,

and it is recommended to implement it through a designated government decision and in close collaboration with the National Cyber Directorate. The recommendations also relate to expanding the binding regulation to large parts of the business-civilian sector by way of the Business Licensing Law, which is not sufficiently enforced by Israeli authorities. Efforts should be made to strengthen the powers granted by this law and improve the culture of compliance, while at the same time appointing an oversight body—the Ministry of the Economy—that will be the sole responsible for implementation and enforcement. In addition, it is recommended that incentives for establishing a cyber insurance market be put in place, together with devising norms of transparency regarding cyber events. This can be accomplished by primary legislation, as many other countries have done. Additional incentives, such as tax breaks and encouraging information sharing among competitors, should be introduced, in collaboration with the Tax Authority. Finally, incentives to promote information sharing between sectors should be anchored in primary legislation.

The concluding chapter analyzes the insights and challenges that inform the regulatory efforts in cyberspace. Policy makers throughout the world are involved in the management of cyber risk, although an optimal formula for supervising the management of these risks in the business-civilian sector has yet to be found. The proposed model seeks to meet this challenge. A variety of tools implemented across sectors in the economy can provide a multi-layered regulatory solution that will protect national security even in the face of growing cyber risk. The technological development of the Internet of Things and artificial intelligence further intensifies the challenges from the cyber world. A formal model that provides an appropriate regulatory infrastructure is required to address these challenges.

Chapter 1
Introduction to Regulation in Cyberspace

Cyberspace constitutes a major challenge to decision makers. First and foremost, this challenge stems from the state and society's dependence on cyberspace, which by nature is a vulnerable domain. On the one hand, this domain facilitates the flow of information that supports economic activity and social welfare, and on the other hand, it is exposed to security, criminal and commercial threats. The challenges to the resilience of cyberspace[2] are the result of a number of factors:

1. There is clear asymmetry between the low entry barriers for attackers and the high costs of defending against them. While a successful attack needs only one successful vector, cyber defense efforts should cover all possible directions of attack.
2. Cyberspace relies on outdated communication protocols, which provide a large measure of anonymity to attackers and make it difficult for law enforcement agencies to identify the source of an attack.[3]
3. Cyberspace facilitates both the exploitation of the many existing weaknesses in hardware or software and the use of existing cyberattack weapons that have proven to be highly effective in previous attacks. These phenomena have led to an accelerated arms race, which lowers the level of security even further. Proof of this can be found in the existence of a flourishing

2 Cyber resilience refers to the ability to withstand possible harm as a result of weaknesses in software/hardware, unsecured protocols, or unauthorized access to information.

3 These protocols were developed to meet the needs in the early days of the internet during the 1960s when the need was for connectivity between several dozen computers. No one at that point predicted that a network of billions of users would rely on these protocols.

market for the exploitation of zero-day weaknesses.[4] In addition, there have been recent reports of commercial companies selling exploits and cyber weapons to governments spying against their citizens and "opponents of the regime."[5]

4. The absence of a mechanism for the sharing of information on cyber threats and the means of protection used by commercial companies makes it difficult to take collective and pro-active measures to prevent cyberattacks. There is only partial sharing of information and limited transparency of commercial companies that operate in the civilian sector.[6] The military sector and the government also are not contributing their share.
5. Economic incentives and technological tools for developing the appropriate protection are also lacking. Although damage from cyberattacks—currently estimated in the billions of dollars—creates an incentive for companies to protect themselves, on the national level the civilian sector is, for the most part, not obligated to report a cyber breach. Therefore, the costs resulting from a successful breach, as well as the reputation of the breached company, are not taken into consideration in a way that will incentivize companies to protect themselves ahead of time.

Despite the growing awareness of shareholders and customers in the private sector, there is no legal obligation to report cyber events and the damage they do. Furthermore, the capabilities of the technological tools currently

---

4 Zero-day weaknesses are hardware or software weaknesses that are often unknown to the manufacturer and have not been corrected. In some cases, these weaknesses become known before a fix is distributed to all the relevant systems. On the flourishing market in this area, see Andy Greenberg, "New Dark-Web Market is Selling Zero-Day Exploits to Hackers," *Wired*, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

5 In recent months, internal documents of the Hacking Team, an Italian company involved in the exploitation of weaknesses and in the development of cyber weapons, have come to light. The documents reveal the company's scope of business with various regimes around the world. On the general phenomenon, see Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *New York Times*, May 29, 2016, https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidatedissidents.html.

6 Jason Mallinder and Peter Drabwell, "Cyber Security: A Critical Examination of Information Sharing versus Data Sensitivity Issues for Organizations at Risk of Cyberattack," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2014):103–111.

available are insufficient for creating hermetic protection.[7] In addition, most of the users in cyberspace are unaware of the implicit dangers and feed it with sensitive and critical information that is not suitably protected. Finally, many users fall victim to the efforts of social engineering, choose weak passwords, and, in most of the attacks, they constitute the weak link through which systems are breached.[8]

Thus, it is not surprising that from time to time there are reports from around the world of the exposure of new weaknesses and breaches of databases, theft of sensitive information, and damage to computer systems.[9] This is the result of misalignment between the ease with which commercial companies and countries gather and store critical information and the insufficient efforts made to protect cyberspace. Thus, we find ourselves completely dependent on the smooth functioning of a highly vulnerable domain.

The state is trying to intervene and prevent the realization of cyber risks or, at least, to reduce them after the fact; however, it encounters structured market failures that lower the level of protection for the entire economy. The main failure is the tendency of organizations to negatively externalize its own cyber damage. Thus, an organization does not completely bear the costs resulting from a cyberattack while its customers—or even more abstract interests such as national security—are harmed in ways that exceed the boundaries of the organization. Since the executives of an organization do not bear any of the costs resulting from a successful cyberattack, they tend to invest less than is needed in cyber protection. This is also because the benefit from investing in cyber protection is not always quantifiable.

Another market failure is the lack of company responsibility for damage to software and hardware products in cyberspace. The market for technological services and products incentivizes and rewards companies that are the first to develop an innovative product but does not provide any advantage to companies that develop products that are more secure and protected than others. Therefore, the market is flooded with software and hardware

---

7 Gabi Siboni and Ofer Assaf, *Guidelines for a National Strategy in Cyberspace*, Memorandum 149 (Tel Aviv: Institute for National Security Studies, 2015), pp. 17–40 [Hebrew].

8 Bruce Schneier, "Credential Stealing as Attack Vector," *Xconomy*, April 20, 2016, http://www.xconomy.com/boston/2016/04/20/credential-stealing-as-attack-vector/.

9 Nate Lord, "The History of Data Breaches," *Digital Guardian*, September 28, 2015, https://digitalguardian.com/blog/history-data-breaches.

infrastructures that contain vulnerabilities and, unlike other consumption products, the producers do not have any legal obligation to their customers in the event of cyber damage resulting from the use of their products. This lack of responsibility exacerbates the problem and causes a situation in which products with insufficient security gain a significant share of the market.

Another important market failure originates from the Antitrust Law, which prevents competing companies from sharing information on cyber threats and their efforts at protection. The lack of information sharing reduces the ability of organizations to protect themselves ahead of time or in real time and creates a lack of trust between players in the economy who could potentially provide assistance to one another in raising overall cyber resilience.[10] In addition to these major market failures, the state deals with the fact that cyberspace is a central component in an organization's internal risk management and that any state intervention is perceived as invasive. Therefore, state intervention in the core activity of a private sector organization encounters difficulties and opposition.

The risks originating from cyberspace, including disruption of the organization's functional continuity, theft of intellectual property, violation of privacy, third-party damage, and reduced reliability of information systems,[11] are the natural extension of risks in a modern state, as described by the sociologist Ulrich Beck in his book *Risk Society*.[12] According to Beck, modern society and its technological developments generate numerous opportunities but also new dangers to humans and their environment. States have responded to the proliferation of risks to society, and according to the economist David Moss, there are various risk-management strategies that states deploy.[13] Moss showed how the US government, which manages risk

10 For an exhaustive survey of cybersecurity market failures, see Nathan Alexander Sales, "Regulating Cyber-Security," *Northwestern University Law Review* 107, no. 4 (2013): 1503–1568.

11 For a discussion of the risks and challenges faced by decision makers in the digital domain, see OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* (Paris, OECD Publication, 2015).

12 Ulrich Beck, *Risk Society: Towards a New Modernity* (Thousand Oaks, CA: Sage Publishing, 1986).

13 David Moss, *When All Else Fails: Government as the Ultimate Risk Manager* (Cambridge, Harvard University Press, 2002).

for the entire American society, has gone through three sequential stages in developing its risk management. The process began in the nineteenth century when the government aggressively intervened in risk management in order to encourage investment and economic growth (by means of legislation, such as the law that limits the risk of investing in a corporation and bankruptcy laws that protect investors from losing all their assets). In the next stage, the government became involved in risk management in the domain of worker safety and the stability of the labor market (worker compensation laws and social security, products of the American welfare state). Finally, during the current stage, the American government has undertaken management of risks that results from modern inventions, which includes environmental damage, food safety, and now cyber risk, on behalf of society as a whole.

The risk strategies of the state range on a continuum from mitigation of risk to reallocation of risk within society. Risk mitigation primarily involves early prevention (such as safety regulations, speed limits, and so forth, and in cyberspace, it includes information security requirements to prevent system breaches) and also steps to mitigate the damage resulting from risk that has already been realized (such as fire regulations or in the domain of cyber, steps to mitigate damage from cyberattacks[14] and informing citizens and state authorities of breaches that have occurred so that they can protect themselves in a timely manner).

The reallocation of risk involves the distribution of responsibility for risk among various entities (such as product safety laws that shift the responsibility from the consumer to the producer). A current example from cyberspace involves information laws, which limit the responsibility of commercial companies that choose to share information on cyber breaches with the government. Reallocation of risk can be achieved through the dispersal of risk among insurers, such as insurance companies. In this case, every insured party pays a premium in order to cover the damage from a realized risk. Currently, the spreading of risk in the private sector exists primarily in the case of third-party risk,[15] without any state intervention.

---

14 On the "full defense circle," see Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015.

15 Third-party risk in the cyber world involves risks to the privacy of customers of commercial companies who suffer harm as a result of a cyberattack involving theft of personal information. In contrast, the insurance companies are not enthusiastic

Notwithstanding the various risk strategies, the state has not yet found the optimal format for intervention, especially in the private sector, in order to ensure the functional continuity of cyberspace, its resilience, and its stability. The civilian sector is highly important to the resilience of this domain. It accounts for the largest sector in cyberspace and therefore is exposed to most of the risks that exist within it. Damage caused in this domain has economic and national security implications for the resilience of the entire society, as described below.

In order to properly understand the regulatory challenge, it is necessary to examine the concept of regulation itself. At the basic level, regulation is the activity of organization, supervision, and enforcement carried out by the state or by independent state agencies in order to legally impose compulsory rules of behavior.[16] Regulation applies to "regulated entities," which constitute the target of the regulatory body. Regulation structures the relationships between the state and the various sectors within it, including the business sector, organizations, and even individuals. The term "regulation" was first used primarily to describe the state's supervision of business organizations and was based on explicit laws that included rules of behavior and appointed bodies to act as "regulators." The broadest definition of regulation relates not only to economic goals but also to social ones. According to this definition, regulation is more than monitoring and enforcing laws among private businesses, as it also deals with public frameworks and ensures the quality of life in a multiplicity of domains.

The concept of regulation originated in the United States at the end of the nineteenth century as a political and administrative way to organize and structure the market. Regulation became a central tool of the American government as a natural response to market failures, the lack of supervision, and the emergence of "natural monopolies." In contrast, regulation in Europe primarily involved the nationalization of markets. Supervision by way of nationalization delayed the development of regulation in Europe relative to the United States.[17] At the same time, starting from the 1970s and during

about insuring first-party risk (that is, the risk to the companies themselves) since there is a lack of actuarial data that can be used in the pricing of insurance premiums for such cyber risks.

16 David Levi-Faur, *Regulation: Conceptual and Historical Background* (Haifa University, 2010) [Hebrew].

17 Ibid.

the 1980s, the use of regulation spread also to Europe and independent regulatory agencies were established there as part of the momentum toward the economic unification of the continent.[18] When Margaret Thatcher came to power in Britain (1979) and Ronald Reagan in the United States (1981), there was an expansion of activity of the independent regulatory agencies, which sought to organize the markets, creating what came to be known as the "regulatory state."[19] The function of the state has gradually been transformed from subsidizing services and providing assistance in order to close socioeconomic gaps to increasing market efficiency through regulation (or deregulation[20]).

Regulation is usually included as primary or secondary legislation of the state or of independent regulatory agencies. It can also be manifested in directives, orders, or binding instructions. Its function is to organize market activity on the basis of government policy. The "regulatory state" assigns a central role to experts and the need for a high level of expertise is the primary motivation for establishing an independent regulatory agency.

The contribution of regulation to the public domain can be explained in several ways. First, regulation seeks to protect the values and liberties of the citizen, which are liable to be violated by powerful interests or as result of external threats. This explains the need for military and security forces and authorities that will restrain and balance them if necessary. Second, regulation has an economic function to correct market failures that result from free market activities that do not serve the interests of the public.[21] For example, a monopoly that prices and supplies products as it sees fit thus requires supervision. Third, regulation can also be justified when information lacks or is asymmetric, which can cause consumers, companies, or states to

---

18 Ibid.

19 Giandomenico Majone, "The Rise of the Regulatory State in Europe," *West European Politic*s 17, no. 3 (1994): 77–101.

20 Levi-Faur explains that deregulation does not eliminate the need for regulatory agencies and bureaucrats but rather creates the need for more in order to supervise the privatization and protect the interests of the state. See David Levi-Faur, "Regulation and Regulatory Governance," in *Handbook on the Politics of Regulation*, edited by David Levi-Faur (Cheltenham, Edward Elgar Publishing, 2011).

21 Shurik Dreishpitz, "Regulation – What, Where and When? A Theoretical and Comparative Perspective," *Parliament* 64 (March 2010), https://www.idi.org.il/parliaments/11097/11149 [Hebrew].

behave in a way that does not serve the public interest. In this case, it is the role of the regulator to maintain transparency and the flow of information. Fourth, regulation can be based on the desire to maintain the existence of public non-renewable resources whose consumption cannot be prevented, for instance air quality or overfishing. In this case, the regulator's role is to see that these resources are not exhausted, which would be the outcome of market forces.

The creation of regulation and the manner in which regulators operate in the domain of public policy are explained in the literature in several ways. The public interest theory (functionalism) claims that regulation seeks to promote the public interest and increase social welfare.[22] In contrast, the private interest theory analyzes groups in society and assumes that the configuration of power in a society is the result of confrontations between groups on a regulatory space. In this case, the regulator is motivated by private interests and its goal is to increase the welfare of interest groups that in general represent a small proportion of the population. From this point of view, regulation is the result of relationships between interest groups and the state and among interest groups.[23] The "influential" group in this case can vary over a continuum from pluralism—many equal and competing groups, where in each case a different group dominates—to the elites, small groups of industrialists, military officers, or politicians whose interests are promoted by state regulation. Between these two extremes is the neo-pluralistic approach, which theorizes that power in a society is dispersed in a liquid and unequal manner. In other words, interest groups with greater power and influence than other groups can "capture" the regulator and "win" a policy that primarily benefits them (known as "capture theory").

In contrast to theories that examine groups in society, a competing theory known as etatism[24] delineates that the state is autonomous and located

---

22 See, for example, Harold Demsetz, "Why Regulate Utilities?" *Journal of Law and Economics* 11 (1968): 55–65.

23 For empirical research that examines the activity of interest groups in the United States, see F.R. Baumgartner and B.L. Leech, "Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics," *Journal of Politics* 63 (2001): 1191–1213.

24 The popularity of the etatist theory stems from "Madison's Dilemma." Madison, the fourth president of the United States, said on the one hand, one cannot be a democrat without allowing groups to organize, but on the other hand, there is no

at the center of decision-making processes as an independent entity that constitutes the dominant entity in policy formation. It therefore has a decisive influence on regulation in society. According to this theory, the power of the state developed from a strong bureaucracy, which managed the creation of infrastructure and border fortifications (such as in Japan after the Second World War). Therefore, the state does not serve interest groups but rather imposes regulation on a society with a strong hand. Regulatory regimes can also be given an institutional explanation, according to which regulation is created on the basis of the capabilities of institutions,[25] or according to their historical place in the formation of public policy.[26]

A new theory to explain regulation began to emerge in the mid-1960s. Known as the ideational theory, it held that paradigms play a central role in the formation of public policy.[27] Thus, a particular idea is viewed as "correct" within a certain "window of opportunity" and it convinces decision makers to create regulation in the spirit of the paradigm and the interests implicit within it.[28] In other words, ideas and interests are often interconnected, such that a particular idea helps provide legitimacy and facilitates the expression of particular interests and, in turn, can lead to regulation that will serve those interests.[29]

---

guarantee that the organization of power groups will reflect the public interest and will work for the public good.

25 For research that examines how policy to protect privacy in Europe created strong institutions, which then passed stringent privacy laws that were not aligned with the spirit of the period, see A. L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62, no. 1 (2008): 103–130.

26 For a study that examines the consistency of the modern welfare state, see Paul Pierson, "The New Politics of the Welfare State," *World Politics* 48, no. 2 (1996): 143–179.

27 About the decline of the Keynesian paradigm and the shift to a monetary economy in Britain, see Peter Hall "Policy Paradigms, Social Learning and the State: The Case of Economic Policymaking in Britain," *Comparative Politics* 25, no. 3 (1993): 275–296.

28 The article by Kingdon coined terms such as "window of opportunity" and "policy developer," which provide a precise explanation of the formation of public policy. See John Kingdon, *Agendas, Alternatives and Public Policy,* 2nd edition (Boston: Little Brown, 1995).

29 Daniel Béland and Robert Cox, *Ideas and Politics in Social Science Research* (Oxford: Oxford University Press, 2010), Introduction.

All these explanations differ from one another according to the level of their rationales. Essentially, apart from the theories that emphasize functionalism and the public interest, the other theories help to understand why regulation is not necessarily rational with respect to the object of the regulation but rather is based on other interests.

The way in which regulation is implemented changes over time. Regulation began as top-down and was based primarily on deterrence and punishment. However, a new philosophy (known as "from government to governance") emerged in the mid-1990s and was based on the understanding that regulation by fiat and control was no longer sufficient to maintain order for the public good. Rather, it was necessary to involve other bodies, which possess knowledge and resources,[30] and in a distributed manner, in order to achieve the state's control and guidance. According to this approach, it is possible to take joint action together with interest groups in society to develop the knowledge necessary to solve complex problems. The "new governance" approach operates in parallel to the traditional approach rather than replacing it. The two approaches complement each other and make it possible to provide a regulatory solution to emerging challenges that cut across sectors. In contrast to the traditional and coercive approach, the new governance approach involves joint effort and division of power; multi-layered integration of all players in the regulated domain; giving discretion to players in the field; creating knowledge that is constantly evolving; and the possibility of flexibility and change according to a dynamic reality.

Another aspect of the new governance approach is embodied in advanced self-regulating arrangements, in which the supervised industry sets the rules for itself instead of—and sometimes in addition to—the oversight of an external regulator. In the context of this new approach, companies appoint compliance officers, whose job is to ensure that the company fulfills the regulations that apply to the organization and to report to management as needed.[31] This kind of regulation is known as "management-based regulation," as the supervision of the regulator is by means of assimilating processes within the supervised organization, and not necessarily by imposing standards or

30 Sharon Yadin, "Policy for Integrative Environmental Regulation of Industry in Israel – Background, Basic Principles and Recommendations," Ministry of Environmental Protection, 2014 [Hebrew].

31 Ibid.

specific regulatory targets. Self-regulation relies primarily on the resources of the organization and avoids the investment of public resources and the need for synchronization with the field. Similarly, it provides the supervised entity with broad discretion and a certain amount of freedom of action. One type of self-regulatory models is enforced self-regulation, in which the supervised entity organizes by itself the supervision of a particular domain, according to the instructions of an external regulator and under its supervision.[32]

In summary, regulation currently encompasses almost every facet of life. It has expanded and evolved over time and continues to develop on the basis of a variety of interests. Regulation has gone beyond the basic organization of business activity and the advancement of socioeconomic goals. It is now a major factor in governance with a leading role in the establishment of a multitude of institutions, and it has significant influence on life in the modern age. Therefore, an understanding of regulatory systems provides insight into the character of governance, on both the national and international levels. The expansion of the phenomenon of regulation provides fertile ground for introducing regulation in cyberspace, a domain that has not yet been organized sufficiently in any part of the world, including the State of Israel.

32 This has been the case, for example, for some of the directives issued by the Bank of Israel which have instructed each bank to set up its own internal procedures to implement the general guidelines that the Bank of Israel issues.

Chapter 2
Survey of the Literature

The survey of the literature on regulation in cyberspace describes the regulatory regimes in the United States, Israel, the European Union, and several countries in Europe (Germany, France, and Britain). In addition, it deals with regulatory issues that cut across national boundaries—protecting devices in the age of the Internet of Things and regulating the market through cyber insurance mechanisms—in which regulatory efforts are in their early stages.

The United States

Federal regulation in cyberspace

Cyber regulation in the United States is composed of assorted laws, executive orders, court rulings, government programs, technological standards,[33] and national security directives, which were added during the last thirty years. The starting point for understanding the accumulation of federal cyber regulations over time is the Comprehensive Crime Control Act of 1984, which for the first time dealt with computer crimes in the United States. Since then and until today, federal regulation has been introduced in a patchwork manner, which has created a body of law that consists of the sum of the government efforts to prevent and mitigate damage in cybersecurity risks in the United States. This domain includes government information systems, critical infrastructures, financial and healthcare systems, classified security systems,[34] and the business-civilian sectors' infrastructure.

Numerous sources of information address the development of the US regulatory regime over the years. Since the regulatory regime in cyberspace

33 By means of guidelines issued by the National Institute of Standards and Technology (NIST).

34 This sector is known as the National Security Sector (NSS) in the United States.

was not created in hierarchical form and with a formalized strategy,[35] many factors were involved in its design, some of which were a response to cyber events that had already occurred and some motivated by the goal of preventing future cyber incidents. The sources of information include the reports of the Congressional Research Service; official websites of the various regulatory agencies in the United States;[36] strategy documents published by the White House over the years;[37] reports of the investigative committees set up by the government following major cyber events;[38] empirical studies of regulatory regimes over the years;[39] websites that monitor the development of US legislation;[40] civil society organizations that examine the digital domains in the United States and emphasize the public interest in technological regulation;[41] classified documents that were published or leaked over the

35 On the patchwork manner in which the regulatory regime has developed, see Richard Harknett and James Stever, "The New Policy World of Cybersecurity," *Public Administration Review* 71, no. 3, (2011): 455–460; Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security," *Georgetown Journal of International Affairs*, International Engagement on Cyber IV (2014): 69–78.

36 These agencies include the Financial Industry Regulatory Authority (FINRA), the Securities and Exchange Commission (SEC), US Commodity Futures Trading Commission, the Federal Trade Commission (FTC), Federal Communications Commission (FCC), Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation, Nuclear Regulatory Commission, Department of Homeland Security (DHS), National Institute for Standards and Technology (NIST), and also the Department of Defense, the Department of Energy, the insurance sector, and the healthcare sector.

37 These strategy documents were the result of the administration's desire to bring about a change in perception and to promote cybersecurity in the United States. They have been published five times—in 2003, 2006, 2008, 2009, and 2011.

38 An example is the report of the committee assigned to examine and change the surveillance habits of the intelligence agencies following the exposure of Edward Snowden who had leaked classified documents. These reports provide a historical survey of what has been done in the United States in the area of digital regulation, including the implications for cybersecurity.

39 For example, about the information protection laws in the United States during the period 1965–1995, see Priscilla Regan, *Legislating Privacy*: *Technology, Social Values and Public Policy* (Chapel Hill, University of North Carolina Press, 1995).

40 The most prominent of which are trackgov.us and the Library of Congress.

41 The prominent organizations of this type are Electronic Frontier Foundation (EFF), American Civil Liberties Union (ACLU), and Electronic Privacy Information Center (EPIC).

years and describe the way in which the United States "marks targets" in cyberspace and uses offensive strategies for purposes of defense; analyses by consulting companies and legal offices that interpret legal rulings, with the goal of helping industry understand the changing requirements imposed by the state;[42] and leading blogs and websites that assist in shaping public opinion in this domain, combined with critical analysis of what is happening on the level of the state and its agencies.[43]

Stage I: The beginning of cybersecurity legislation in the United States—the development of threats

Decision makers in the United States became involved in the issue of cybersecurity only in the mid-1980s. Nonetheless, an understanding of the motives and context that led to the formation of US cyber policy until today requires going back to the 1960s and 1970s. It was then that the Department of Defense began to accumulate experience and insights in cyberspace, which was then beginning to take shape. During this period, there were power struggles surrounding the mandate of the state to gather information on its citizens. In this context, it is important to understand the historical perceptions of the Department of Defense, which influenced the positions of members of Congress and decision makers in the White House with respect to cybersecurity. According to the Department of Defense historian Michael Warner,[44] the prevailing perceptions during the 1970s can be divided into four main groups:

1. Sensitive information in the computer systems is not safe.
2. Computers contain various vulnerabilities and there is the possibility they could become another way of stealing information.
3. The offensive capabilities in cyberspace are a legitimate part of the state's military capabilities.
4. Other countries can attack the United States in cyberspace and apparently are doing so.

Computers started to communicate with one another by way of networks in the 1960s. The "machines," as computers were then called, took up entire

42 The leading one is the website of the Skadden legal consulting firm.

43 Two of the main ones are schneier.com and the blog of Brian Krebs, an information security investigator.

44 Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781–799.

rooms, were very expensive, and required abundant resources in the form of electricity and designated manpower in order to operate them. Owners of computers were forced to install them in separate rooms and were happy to lease their use to companies, agencies, and researchers in order to maximize the profit from their operation. This reality created demand for software programs that would be capable of working in parallel to other programs, without revealing information to unauthorized users working on the same computer.

Already in 1966, the US Congress held discussions in order to understand the problem of information leakage from computers. At the same time, the Rand Corporation, a research institute, was asked to prepare a report on information leakage from computers. The report, which was published at the beginning of 1967, warned that as long as unknown users worked simultaneously on the same machines, there would be no engineering solution to the problem of information security in computerized systems.[45] As a result, solutions were developed for the existing situation in the form of different levels of authorization in the systems, authorizations for access to files, churning of passwords, and encryption. When the IBM company proposed a commercial solution to the problem and asked to implement it in the federal government, disagreements arose regarding the involvement of the National Security Agency (NSA) in the matter. This followed the request by the NSA to enforce a lower encryption standard, so that it would be able to break the encryptions of commercial products if that became necessary for national security.

When computer networks became global in the 1980s, the issue arose of the risk implicit in the existence of vulnerabilities and malware and the ability of hackers to remotely penetrate computer systems. The commander of the US Air Force, Roger Schell, published a document in 1979 surveying the different ways in which computer systems could be breached, based on simulations carried out on the Air Force's systems. Schell differentiated between coincidences and errors on the one hand and systems that were fundamentally unsecured or systems developed outside the United States on the other hand, and concluded that in both cases there was major risk of

45 Willis H. Ware, *Security and Privacy in Computer Systems* (California, Rand Corporation, 1967).

breaches.[46] In 1983, the *New York Times* published an article on the attitudes in the US Department of Defense regarding the cyber issue and exposed that it was concerned about the inability to protect computer networks as a result of the growing quantity of classified information stored in them, the growing number of potential hackers, and the increasing sophistication of breaches.[47]

The Reagan administration related to the cyber challenge in a then confidential directive issued in 1984[48] on the protection of federal computer systems. The directive assigned responsibility for protecting the computer systems to the NSA, which included investigating new threats and determining the standards of dealing with them. In response, Congress expressed concern that an intelligence agency like the NSA would be exclusively responsible for federal-civilian information security, thus endangering the privacy of civilians and violating their rights.[49] During the period 1985–1987, Congress held a series of discussions on the issue of privacy and the protection of federal networks. At the same time, a coalition of banks and civil society organizations emerged over concerns about violations of privacy. This situation—which should be viewed against the background of Reagan's weakened administration following the Iran-Contras crisis—enabled Congress to pass legislation that divided responsibility for cyber defense of the federal systems between the NSA and the National Institute of Standards and Technology (NIST). The legislation was in the end implemented by a presidential directive issued by President George H.W. Bush.[50]

---

46 Roger R. Schell, "Computer Security: The Achilles' Heel of the Electronic Air Force?" *Air Force University Review* (1979).

47 William J. Broad, "Computer Security Worries Military Experts," *New York Times*, September 25, 1983, http://www.nytimes.com/1983/09/25/us/computer-security-worriesmilitary-experts.html.

48 National Security Directive No. 145.

49 Jack Brooks, a member of Congress from Texas, called Reagan's directive an "unacceptable extension of military powers in the citizens' sphere" (see Hearings to Consider H.R. 145, the Computer Security Act of 1987, to Amend the Federal Property and Administrative Services Act of 1949 Brooks Act to improve Federal Computer Systems Security Before the Subcomm. on Legislation and National Security of the H. Comm. on Oversight & Gov't Reform 100th Cong. 281 (1987)).

50 National Security Directive No. 42: "National Policy for the Security of National Security Telecommunications and Information Systems."

In the 1970s, the US military realized that modern weapons systems were dependent upon a constant flow of information. Against this background, a new concept of "information warfare" was adopted. It was based on the insight that the flow of information in advanced weapons systems is complex and subject to numerous threats. Furthermore, officers in the military reached the conclusion that information warfare could damage the command and control systems of the enemy's weapons. One of the first events in this domain was American sabotage of Canadian equipment bought by the Soviet Union for use in the Trans-Siberian gas pipeline, which, according to unconfirmed reports, caused the pipeline to explode in 1983. According to the same reports, the software system of the Soviet gas company, whose function was to operate the pumps and the control systems, was programed by hostile American code to vary the speed of the pumps in a way that would create pressure and cause them to explode.[51]

Information warfare was again used in the First Gulf War (1991) which was characterized by many as the first information war. Colin Powell, the chairman of the Joint Chiefs of Staff during the war, described the necessity of establishing dedicated information warfare units in the air force in 1993,[52] followed by the navy in 1994, and in the army in 1994. China and Russia, who wanted to be part of the information revolution but were forced to acquire American hardware and software for their infrastructures, understood that the American systems contained "smart bombs" that the United States could use when the time was ripe.[53]

In the mid-1990s, US decision makers also came to realize that damage in cyberspace was likely to be manifested not only in the loss of sensitive information but also in damage to the country's critical infrastructures. The Rand Corporation was asked to examine the issue and after a number of simulations concluded that the country's domestic security was vulnerable

---

51 The first report of this event was in Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Casemate, Presidio Press, 2005).

52 Chairman of the Joint Chiefs of Staff, "Command and Control Warfare," Memorandum of Policy, No. 30, March 8, 1993, http://www.dtic.mil/dtic/tr/fulltext/u2/a389344.pdf

53 The Chinese fears are described in Wang Pufeng, "The Challenge of Information Warfare," *China Military Science* (1995). The Russians expressed their fears in interviews in Adams James, *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (Simon & Schuster Publishing, 1997).

as a result of the growing dependency on cyberspace.[54] Institutions affiliated with the US government, such as the Comptroller General, also examined the issue and reached similar conclusions. The Pentagon and the White House also set up committees to examine the issue and they too arrived at the same conclusion that cyberspace had created a relatively cheap route of attack, which could lead to a fatal blow to the country's infrastructure.

Stage II: The growing power of the private sector

Another important trend that began in the 1990s was the increasing role played by the private sector in decision-making processes related to cyberspace in the United States. This trend emerged from the US administration's desire to adapt the existing personal information collection laws to recent technological developments. The Office of Technology Assessment[55] concluded in 1984 that the legal constraints on the government's gathering of information were irrelevant in the case of digital communication infrastructures. Following discussions in Congress, a consensus was reached that the laws should be updated and, indeed, in 1986, it passed the Electronic Communication Privacy Act, with the support of the business sector.[56] The act extends the parameters of existing legislation and includes telephone and digital communication infrastructure within the constraints that apply to the government's gathering of information.

The reaction of the executive branch to the congressional legislation was first seen in the early 1990s. In 1992, Congress rejected legislation proposed by the George H.W. Bush administration requiring companies operating digital infrastructures[57] to build technological interfaces that would allow the state to gather information from them. This was the first time that it is possible to identify proposed regulation, which, together with the legitimization that it provided to the act of information gathering, was explicitly intended to weaken digital infrastructures in cyberspace. This trend continued with the proposal to develop encryption hardware (the "Clipper Chip"), which, together with the encryption of information, would enable law enforcement

54 Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (California, Rand Corporation, 1996).

55 The Office of Technology Assessment was meant to assist lawmakers on issues of technological progress but was closed in 1995 due to lack of funding.

56 Regan, *Legislating Privacy*.

57 For example, telephony and communication companies.

agencies to decode encryption and access information. The private sector in the United States opposed this proposal on the grounds that it would not be able to compete with products available in foreign markets, which do not enable government access to information. Against this background, the National Institute of Standards and Technology (NIST) decided that the adoption of the cryptographic standard would be on a voluntary basis. The American market reacted accordingly and refrained almost across the board from adopting the controversial encryption standard. Computer scientists later demonstrated that the proposed technology made it possible for anyone to break the encryption and the US administration decided to abandon the standard.[58]

In 1994, Congress could no longer oppose the administration's initiatives and approved the Communication Assistance to Law Enforcement Agencies Act (CALEA), designed to facilitate the activity of law enforcement agencies and requiring suppliers of digital infrastructure to build interfaces into their products that would enable government access and information gathering. As a result, various companies, including Cisco, published their new architecture, which was revealed to be unsecured.[59] Under massive pressure from businesspeople and hardware producers in the United States, the administration removed the standard's restrictions on encryption in 2000, leading to a change in the order of priority and attributing greater importance to private sector interests.

Since the mid-1990s, as an increasing number of institutions and state service providers moved to digital platforms, the federal government began to allocate powers and responsibility for security in the various networks. In 1995, the Office of Management and Budget (OMB) was for the first time given powers to protect information in the possession of the federal

58 For further details on the government's strategy on this issue, see Diffie Whitfield and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MIT Press, 1998), pp. 212–223.

59 A prime example of the risks in the implementation of mobile phone architecture that allows information gathering came to light in 2007 when the Vodaphone company admitted that it had carried out illegal wiretapping in Greece, involving the phones of the prime minister, the mayor of Athens and about one hundred senior officials in the public sector. For additional details, see Vassilis Prevelakis and Diomidis Spinnelis, "The Athens Affair," *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair.

government. In 1996, these powers were updated by the Klinger-Cohen Act, which established that each government department would serve as a regulator in its domain and that the OMB would oversee them.

In addition to institutional regulation, standards were established during this period for the regulation of computerized systems outside the federal domain. Thus, for example, the second amendment to the Health Insurance Portability and Accountability Act (HIPAA) in 1996 required the US Department of Health to set standards for information security and the protection of privacy, which would apply to all healthcare providers. After receiving more than two thousand comments from the public, the Department of Health instituted the regulations in 2003 and began to enforce them in 2005.

In 1998, the issue of critical infrastructures came up for the first time. By means of Executive Order No. 63, President Clinton tried to regulate the activity of various government agencies, with the aim of mitigating possible harm to the country's critical infrastructures. The main goal of the executive order was to improve the defensive capabilities of federal agencies and the ability of the state in general to protect itself from attacks on critical infrastructures, which involved collaboration with players in the private sector.[60] The regulation included ten sectors that were defined as critical[61] and created four institutions within various bodies in order to improve defensive capabilities.[62]

A regulatory solution was also provided for the financial sector in the 1990s. In 1999, Congress passed the Gramm-Leach-Bliley Law, which required that financial institutions maintain transparency toward their customers in regards to the sharing of information and protecting sensitive personal information. It defines the state institutions to which the law applies and

60 Most of the critical infrastructures in the United States are operated by the private sector.

61 Critical infrastructure include communications, finance, water, transportation, emergency services, firefighting, healthcare, electricity, oil and storage.

62 The institutions include the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism; the Critical Infrastructure Assurance Office within the Department of Commerce; the National Infrastructure Protection Center within the FBI and various other law enforcement agencies; and the National Infrastructure Advisory Council (NIAC) within the Department of Homeland Security whose goal is to improve relations with the private sector.

requires them to formulate a risk-based information protection plan, according to the evolving threats.

The attack on September 11, 2001 led to increased activity in the regulation of the government's information collection from digital infrastructures and greater attention was now devoted to critical infrastructures and transportation networks. The two main laws concerning the resilience of cyberspace during this period were the Patriot Act of 2001 and the Homeland Security Act of 2002. The Patriot Act enables the US administration to exploit various channels of information gathering from digital systems. The Homeland Security Act included, in addition to the creation of the Department of Homeland Security, the Cyber Security Enhancement Act whose goal was to reduce the restrictions on the transfer of information to the government by internet providers and to tighten the sanctions on unauthorized access to computer systems.

In parallel to these two important laws, President George W. Bush issued classified directives[63] that would allow the NSA to gather information without the need for warrants, in order to better understand the map of cyber threats and to monitor international communications related to hostile cyber activity. The attorney general also played a role by announcing that the restrictions on information gathering on the internet do not apply to the FBI and that it could monitor chats, private databases, and other sites.

In 2002, the protection of government networks was reinforced by means of the Federal Information Security Management Act (FISMA), which required every federal agency to develop an information security plan for all the computer systems serving the agency, based on the NIST's strategy of prioritization and risk management and under the supervision of the OMB. Every federal agency adopted the Minimum Security Requirements for Federal Information Systems (FIPS 200) according to NIST Special Publication 800-53, and each agency on its own decided on its security category, based on the FIPS 199 standard.

---

63 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times,* December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-letsus-spy-on-callers-without-courts.html.

Stage III: The activity of independent regulatory agencies

In addition to legislation, in the last decade independent regulatory agencies have made increasing efforts in cyberspace, each in its own sphere of responsibility (see Figure 1 below). These agencies provide secondary legislation for federal statutes, and they are also responsible for implementation and enforcement.

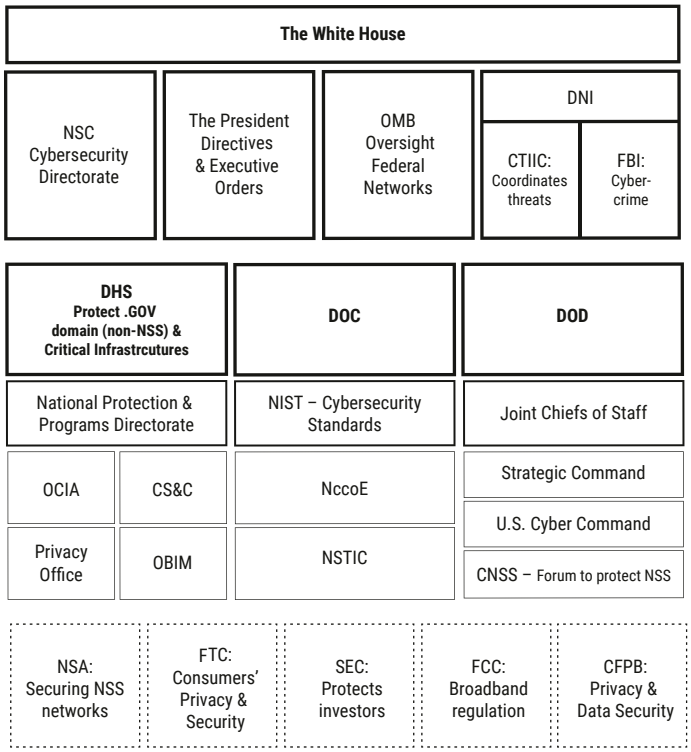

Figure 1: Agencies and institutions involved in cybersecurity in the United States

The agency most active in information security in the United States is the Federal Trade Commission (FTC). It essentially stepped into the vacuum created as a result of the lack of a central information security regulator for the private sector and it justified that move on the pretext of maintaining fair trade. The ability of the FTC to enforce information security in the business sector was confirmed in 2015 following a court ruling in its favor in a suit filed against it, which challenged its authority to enforce cybersecurity practices. The judge set a precedent by ruling that the FTC has the authority and the responsibility to act in the business sector when companies do not make sufficient effort to protect their customers' information.

The FTC played a dominant role in the implementation and enforcement of federal sectoral information security laws, in the domains of both healthcare and finance. The FTC, together with the Department of Commerce, issued non-binding directives for cyber and privacy protection among infrastructure organizations in the business sector that are defined as non-critical, but considered critical for the functioning of the US economy. The directives dealt with the development—in collaboration with the private sector—of information security standards, which were meant to become binding standards for American industry. These standards included ways of reducing vulnerability in cyberspace, incentives to achieve transparency with respect to cyber events, sharing of information, and the exemption from responsibility in the event of a breach. As mentioned, these were non-binding directives that provided broad discretion to each organization.

Another regulatory agency that has played a similar although secondary role in cyberspace is the Consumer Financial Protection Bureau. In 2016, it fined a company—for the first time—that did not meet basic cyber protection standards. Essentially, already in 2014 it had tried to increase transparency with respect to cyber events on the federal level but without success.

One federal agency that is very active in cyberspace is the Securities and Exchange Commission (SEC). It has been involved in the implementation of federal laws related to cybersecurity in the financial sector, especially emphasizing threats of identity theft and to the financial systems whose stability is essential to the entire economy. The SEC possesses a great deal of power, although it is restricted to the financial sector. The SEC's prominence and importance can be seen in the activity of the Financial Industry Regulatory Authority (FINRA), which brings together all of the companies that are subject to SEC regulation and provides them with guidance in the implementation of information protection in order to meet regulatory conditions. FINRA is essentially the executive arm of the federal government in the financial sector and serves as the intermediary for the regulation of the relevant bodies. Its goal is to increase financial resilience on the national level. In addition, it supports a similar process among small and mid-sized businesses, which includes mapping cyber weaknesses and prioritizing investment in protection according to their limited financial means. In 2016, it fined a company—for the first time—that did not meet the minimal conditions for cyber protection.

Another federal agency that has been active in cyberspace since 2015 is the Federal Communications Commission (FCC) whose main activity is in

communication infrastructures. The FCC provides guidance to communication providers on cyber protection, including how networks of communication operators should implement the NIST's strategy for federal networks. In 2016, the FCC published binding directives to communication service providers in the areas of information protection and consumer privacy. According to those directives, communication operators could no longer trade in the personal information of their customers without their agreement. In this way, the FCC set a regulatory precedent for the protection and maintenance of personal information in cyberspace.[64] When President Trump entered the White House in 2017 he appointed a new Director of the FCC, who decided to cancel the privacy regulations introduced by his predecessor.

The body that oversees the activity in cyberspace in the United States is the Department of Homeland Security. Apart from protecting the sites of the government, the department provides tools for the protection of critical infrastructures in the United States and is involved in the sharing of information, which is intended to strengthen the overall resilience of cyberspace. The Department of Homeland Security operates as a "meta-regulator" and provides guidance to all the government departments on issues related to the protection of critical infrastructures within their jurisdictions. In addition, each federal department has a designated protection plan to deal with the unique challenges facing critical infrastructures in its area of responsibility. Furthermore, the Department of Homeland Security provides assistance in managing cyber events in real time, deals with issues of awareness and the education of future US cyber leaders, and carries out research on the subject. Recently, it became involved in the development of a cyber insurance market for the private sector, with the goal of encouraging growth and providing incentives to achieve sufficient information protection. In addition, it assists other authorities that are dealing with cyber crime.

64 For further details on the setting of this precedent, see Ido Sivan-Sevilla, "The FCC's Latest Privacy Regulations: A New Stance on Private-Sector Protections?" *Columbia Science and Technology Law Review*, December 12, 2016, http://stlr.org/2016/12/12/the-fccs-latest-privacy-regulationsa-new-stance-on-private-sector-protections/.

Regulation of cyber protection by US states

Responsibility to prevent major cyber events is not limited to the federal government. There have been significant attacks on banks,[65] attempts to harm critical national infrastructures,[66] and damage to the cyber systems of cities.[67] Ransomware attacks on the computers of organizations and individuals as well as the collecting of sensitive personal information each day from personal computers and retailers do not always require federal intervention. These issues are considered to be "softer" in the context of cyber protection efforts. The various US states have stepped into this vacuum and are working to build an immune digital space to protect the privacy of their citizens.[68]

The states have demonstrated flexibility, quick response, and innovation, which allow them to keep abreast of the frequent changes in technology; this is in contrast to the feet-dragging that characterizes the legislation on the federal level.[69] In addition, the influence of charismatic "policy entrepreneurs"[70] in each of the states is many-fold greater than that of

---

65 On damage done to JP Morgan, one of the major banks, see "What Lies behind the JPMorgan Chase Cyber Attack," *The Economist*, November 12, 2005, http://www.economist.com/news/businessand-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itselfwhat-lies-behind.

66 On the damage to the electricity infrastructure in Ukraine, see Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

67 For example, the ransomware attack in March 2018 on the city of Atlanta, Georgia, required the state to invest $2.6 million. See Lilay Hay Newman, "Atlanta Spent $2.6M to Recover From A $52,000 Ransomware Scare," *Wired.com*, April 23, 2018, https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

68 The obligation to report cyber events, including violations of privacy, is applied at the state level in the United States The federal government has not yet managed to pass legislation in this area, despite the numerous attempts in recent years to do so.

69 On the differences between the federal and state levels see Paul Lipman, "Four Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective)," *Government Technology*, July 17, 2015, http://www.govtech.com/opinion/4-Critical-Challenges-to-stateand-Local-Government-Cybersecurity-Efforts.html.

70 The term "policy entrepreneur" is taken from John Kingdon (1988) who examined the process of public policy formation. In this process, a skilled policy entrepreneur

legislators on the federal level. States that lagged behind in cyber protection were able to quickly overcome bureaucratic barriers thanks to these policy entrepreneurs who were in the right place at the right time and knew how to promote cyber protection.

One of the main disadvantages on the state level relative to the federal level is the lack of sufficient cyber intelligence, to which most of the federal agencies have access.[71] The federal agencies benefit from the intelligence gathered by the NSA and the FBI on cyberattacks, while an investigation of attacks on the state level is carried out on the basis of local capabilities. Consequently, steps taken are according to the exclusive discretion of the state legislator.[72] The lack of high-quality intelligence can explain the risk strategies adopted by the states, which are based on cyber insurance and spreading of risk among insurance policies. This is in contrast to preventative and pro-active measures on the federal level, which are based on high-quality intelligence.[73]

One of the main challenges facing the states is the protection of critical infrastructures. The boundaries of these infrastructures in the digital age are not sufficiently clear and the division of responsibility between the state and federal levels is a subject of disagreement.[74] This lack of clarity creates a culture in which critical infrastructure operators try to meet regulatory requirements on both the state and federal levels but are less concerned about effectiveness and the degree to which these requirements answer their cyber protection needs.

Another challenge is the protection of consumer privacy and the enforcement of information security standards, goals that complement each other. The

---

is able to connect between a policy problem and its solution, to the extent that the political environment allows such a policy to be implemented.

71 On the gap in intelligence capabilities between the federal and state levels, see Amanda Ziadeh, "States vs. Feds: Who Does Cybersecurity Better?" *Government Cloud Insider*, November 4, 2015, https://gcn.com/articles/2015/11/04/fed-vs-sl-cybersecurity.aspx/.

72 An exception is the case of large-scale attacks that require federal intervention, such as those on the financial system, major fraud, the exposure of medical information, and so forth.

73 For example, on the level of the state, there is no ability to counterattack (known as hack-back methodology).

74 See the report by G. C. Wilshusen, "Cybersecurity Challenges in Securing the Electricity Grid," Government Accountability Office, July 17, 2012.

states have adopted various measures in order to establish protection standards and they implement strict policies with respect to the reporting of cyber damage, as well as compensating citizens whose privacy has been violated. There are states whose lack of financial means has led them to impose the costs on the companies themselves and to encourage the development of a cyber insurance market. The transfer of responsibility for cyber risk to the companies and the encouragement of a market to spread risk enables the states to demonstrate their effectiveness in protecting against these risks, despite an insufficient budget.

The various states play a broadly defined role in the context of cybersecurity, complementing that of the federal government. In what follows, we present a survey of the various aspects of the states' role, including the way in which they complement the regulation on the federal level and provide a solution in areas where the federal government finds it difficult to reach a decision.[75] In addition, we will explain how cyber protection legislation strengthens the powers of the various states in dealing with the organizations and companies in their jurisdiction. Finally, we will survey the way in which the states are able to promote local projects and collaborations whose goal is to provide a better cyber protection solution.[76]

The state as a complementary regulatory entity to the federal government

In December 2015, an "official" channel of assistance was established between the federal administration and government entities, including at the state level. This channel was based on the Cybersecurity Information Sharing Act (CISA), which provides, among other things, an almost automatic interface with the various states for the purpose of sharing information on security events in government networks. The federal government can also

---

75 The prime example is privacy, namely the protection of personal information. Many states provide laws and stringent regulation and thus not only do they contribute to the protection of privacy, they also indirectly help solve the problem of cyber protection. In practice, many information security managers point to this regulation as one of the incentives to encrypting their information systems.

76 For example, see the initiative being led by the state of New York to introduce strict and detailed cybersecurity regulation that will apply to the financial sector in Kevin Townsend, "New York State Imposes New Cybersecurity Regulation for Financial Services," *Security Week*, January 2, 2017, http://www.securityweek.com/new-york-state-imposes-new-cybersecurity-regulation-financial-services.

synchronize this information with other sources of information and provide early warning to states.[77] The law is also valid in the case of entities in the private sector and provides numerous incentives for information sharing, including the exemption from responsibility in the case of a system breach and a promise of information confidentiality. These are significant incentives for the private sector and are also attractive for the states, given that those same states receive assistance from the federal executive branches in order to identity threats originating from companies in their jurisdiction.

Sharing of information is highly important, particularly in the context of critical infrastructures within the states. About 90 percent of these infrastructures are under private ownership[78] and are within the jurisdictions of the various states. Therefore, this legislation enables the states to support the sharing of information between the private and public sectors. Furthermore, the Department of Homeland Security has a designated department for ensuring cooperation on the state level. Each state also has responsibility for protecting its government networks. For example, the federal government, under the auspices of the Department of Homeland Security, financed the scanning for weak spots in government networks in the state of New York and provided tools for resolving them.[79] In contrast, a designated local team of experts in California is formulating recommendations for decision makers on how to handle an emergency as well as a strategic plan for the protection of the local government networks during an attack.[80]

Designated teams for the minimization of risk and the formulation of states' responses to cyber events are—in addition to their role in managing

77 On the innovative law and the directives on how to share information with the federal government, see Daniel K. Alvarez and Naomi Parnes, "DHS, DOJ Release Final Cyber Threat Information Sharing Guidelines Under CISA," *Willkie Farr and Gallagher*, June 24, 2016, http://www.willkie.com/~/media/Files/Publications/2016/06/DHS_DOJ_Release_Final_Cyber_Threat.pdf.

78 Whitfield and Landau, *Privacy on the Line,* pp. 212–223.

79 For further details on the project, see New York State Division of Homeland Security and Emergency Service – Office of Cyber Security, "NYS Local Government Vulnerability Scanning Project," September 22, 2011, https://www.its.ny.gov/document/nys-local-government-vulnerability-scanning-project.

80 For a comparison of the policies in key states and discussion of the initiative in California, see Francesca Spidalieri, "State of the States on Cybersecurity," Pell Center, November 2015, http://pellcenter.org/wp-content/uploads/2017/02/state-of-the-states-Report.pdf.

events—also working to increase awareness among the public of these events. California is a special case: its designated team reports to the California Office of Emergency Services and is responsible for both cyber threats and physical threats to digital networks, particularly critical ones.

The various states are using existing standards for information protection such as Payment Card Industry Data Security Standards (PCI DSS), which apply to companies that provide online payment services, in order to encourage various companies to adopt them. The state of Washington, for example, adopted a law that exempts online payment companies that meet the PCI standards for bearing responsibility for a breach. The goal is to incentivize other companies to adopt these standards.[81] Following in the footsteps of Washington, Minnesota and Nevada adopted similar laws. They went even further by adopting "prescriptive regulation,"[82] which determines the standards that various companies have to meet. These states chose to adopt the standard for online payment companies as a binding standard and Massachusetts even required a written information security program from each company, which would include supervision of third-party suppliers, assessments of risk, and the imposition of sanctions for violations of the information security rules within the company.[83] In 2015, the state of New York passed the Data Security Act which establishes that organizations and companies in New York must protect every service that gathers and processes personal information. To this end, the definition of personal information was expanded to include driving license number, bank account number, medical information, email address, and password. Nonetheless, New York makes do with a certificate from a third-party supplier that guarantees the

81 Tom Kemp, "Buckle Up with Cybersecurity . . . It's the Law," *Forbes*, February 1, 2012, http://www.forbes.com/sites/tomkemp/2012/02/01/buckle-up-with-cybersecurity-its-thelaw/#5fa6b50b933f.

82 As opposed to "process regulation," "prescriptive regulation" is a more rigid and traditional form of regulation in which the criteria to be met are determined ahead of time. For a theoretical survey of the subject, see Gilad Sharon, "It Runs in the Family: Meta-Regulation and its Siblings," *Regulation & Governance* 4, no. 4 (2010): 485–506.

83 For the official state requirement, see Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, "A Small Business Guide: Formulating A Comprehensive Written Information Security Program," 2016, http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf.

level of security in that organization, such that it can be defined as "secure at a sufficient level."

The laws passed in the various states impose significant costs on commercial companies, in addition to the obligation to reexamine their information security policy as a result of these laws. In this context, special attention is given to the classification of personal information and the way in which it is stored. Thus, companies need to reconsider the way in which they react to events and their contracts with third-party suppliers, so as to ensure that their information is protected throughout the work process.[84] The differences in cybersecurity policy among the various states also constitute a challenge to companies and organizations that operate in those states and they are forced to deal with a number of different standards (such as in Florida and California) and also to fulfill the technical requirements imposed by the regulation (such as in Massachusetts).

The way in which states choose to assimilate information security regulation in order to protect businesses and organizations against cyberattacks in their jurisdictions shifts the costs almost completely onto the organizations themselves. In California, for example, the stringent requirements may be beyond the abilities of small and mid-sized businesses, which are often unable to bear the costs. They may ignore security problems or alternatively may choose to shut down, thus reducing competition in the market. An appropriate insurance policy may constitute an interim solution in this context.

The various states essentially dictate the developments in the reporting of cyber events. California became a pioneer in this regard when it passed a law in 2003 requiring companies to report the theft of their customers' personal information[85] and in this way paved the way for forty-six other

84 Jim Halpert, "State Breach Notification Laws – Updates from 2015 Legislative Sessions, 6 Action Steps for Companies," *DLA PIPER,* July 20, 2015, https://www.dlapiper.com/en/us/insights/publications/2015/07/state-breach-notification-laws/.

85 This is a common phenomenon in the domain of regulation in the United States and is known as the California Effect. Thus, regulation that originated in California trickles down to other states and influences the structure of the American market. For further details, see David Vogel, "Environmental Regulation and Economic Integration," Yale Center for Environmental Law and Policy, 1999, http://www.iatp.org/files/Environmental_Regulation_and_Economic_Integrat.pdf.

states to pass similar legislation.[86] California requires companies and state agencies to report a cyber breach and theft of information from their systems, including reporting to the state's attorney general, and also requires them to compensate their customers. Since the companies are not enthusiastic about bearing the costs resulting from the law in the case of a breach and the reporting that follows it, the legislation essentially constituted an incentive for them to acquire protection before a breach occurs.

An amendment to the California law passed in 2016 requires companies to adopt twenty different security criteria and establishes that those companies which comply will—in the event of a breach—be eligible for assistance from the state. In this way, California imposed the cost of defense and reporting on the companies, while threatening sanctions in the case of noncompliance. Other states, such as Florida, Arkansas, and Maryland, have gone even further by including requirements such as mandatory reporting of a breach and the timetable according to which customers must be notified of a violation of their privacy. Thus, for example, in 2014, Florida passed the Information Protection Act, which requires the reporting of unauthorized gathering of personal information as the result of a breach, as well as the unauthorized accessing of personal information by employees within the organization. According to this law, notifying customers of a violation of their privacy must occur within thirty days, rather than forty-five days as is the practice in other states.[87]

Increasing the power of the states in cyber regulation

Not all measures adopted by the states are the result of collaboration with the federal level. In some areas the various states have independent powers, such as in the case of state infrastructures and individual privacy, a subject that the federal government has to a large extent ignored. The various states take advantage of the fact that they are more familiar with the infrastructures in their own jurisdictions and work to reinforce the cybersecurity of these infrastructures. For example, infrastructure companies in Pennsylvania are

86 The National Conference of State Legislatures keeps track of legislation in the various states.

87 For a survey of the law in Florida, see George Grachis, "Florida Privacy Law Adds Breach Notification and Strengthens Compliance," *CSO*, September 2, 2016, http://www.csoonline.com/article/3112741/leadership-management/florida-privacy-law-adds-breach-notificationand-strengthens-compliance.html.

required to report any attack that causes damage of more than $50,000. In Texas, less "traditional" infrastructure systems, such as meter systems, are required to meet information security standards established by an independent company, in collaboration with the Texas Public Utility Commission.

According to the Bipartisan Policy Center, the power of the various states to protect against cyberattacks is limited not only to the Public Utility Commission (PUC) in each state but also includes the governor's office, the energy department, and the chief information officer. As part the governor's role in coordinating cybersecurity, the National Governors Association created a new resource center for cybersecurity on the state level. This center's function to examine the need of each state to formulate an appropriate cybersecurity policy for infrastructures located within its borders and under its ownership.[88]

The tension between the various states and the federal government in the area of information privacy and protection can clearly be seen in the banking sector. In the case of a bank that has customers in several states, it must comply with breach reporting regulations in the host state. In Massachusetts, for example, there is a law requiring financial companies to report in writing on the measures they use to protect personal information.[89] Other states, such as California, impose stringent standards for the protection of privacy, according to which companies that do not comply are defined as "lacking reasonable security," are subject to legal action and will have to provide answers in the event of a breach of their systems.[90]

---

88 Michael Hayden, Curt Herbert, and Susan Tierney, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," *Bipartisan Policy Center*, February 28, 2014, http://bipartisanpolicy.org/library/cybersecurity-electric-grid/.

89 On the official requirements of the regulation instituted by the Office of Consumer Affairs and Business Regulation, see http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf.

90 Paul Otto and Brian Kennedy, "Reasonable Security becomes Reasonably Clear to the California Attorney General," *Hogan Lovells Chronicle of Data Protection*, March 1, 2016, http://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear/. For a summary of the breach events in California, see the report of the attorney general in K. D. Harris, *California Data Breach Report 2012–2015,* California Department of Justice, February 2016, https://oag.ca.gov/breachreport2016.

The enforcement of the privacy standard by the various states began with California in 2002, with the passing of laws that required companies to report cyber breaches. The revelation by Edward Snowden of federal surveillance programs led those states to adopt a pro-active approach to issues of privacy violation. Thus, for example, in January 2016 a privacy law went into effect in Delaware (following a similar law that already existed in California), which reinforces the protection of privacy and broadens the definition of personal information that is to be protected.[91]

The promotion of initiatives and collaborations between the state and federal levels

In addition to separate activities, the federal government and the various states on regulatory issues sometimes collaborate, which raises the level of cybersecurity. Thus, for example, in 2015 the New York Department of Financial Services (NYDFS) published recommendations for the strengthening of cybersecurity and at the same time requested that federal legislators develop a broader regulatory structure to deal with the issue, without reducing the independence of the various states. According to the NYDFS, the federal plan should cover the issues of functional continuity of business owners, security in the supply chain with respect to external suppliers, and the security of the systems and networks themselves.[92]

Although there are few examples of cases in which states request additional directives from the federal regulator for the enforcement of cyber regulation, this model of collaboration was successfully implemented in 2003 when the Center for Internet Security (CIS), a non-profit center working to eliminate cyber threats,[93] established the Multi-State Information Sharing and Analysis Center (MS-ISAC) with the goal of increasing information sharing between the states and the federal government in this sphere. This institution has

---

91 In addition to the protection of social security numbers, Delaware requires the protection of any information that can be used to locate and identify private individuals.

92 Sarah V. Riddell and Melissa R. Hall, "NYDFS Issues letter to Federal Financial Regulators Seeking Collaboration on Cybersecurity Efforts," *Morgan Lewis,* November 11, 2015, https://www.morganlewis.com/blogs/finreg/2015/11/nydfs-issues-letter-to-federal-financialregulators-seeking-collaboration-on-cybersecurity-efforts.

93 For more details on CIS, see / https://www.cisecurity.org/about-us.

gained momentum over the years and is currently considered to be one of the most important players in cybersecurity in the United States. What started as a small group of states in the Northeast, which had come together to share information, became a national resource that works together with the US administration and the Department of Homeland Security in order to reinforce monitoring, tracking threats, and responses to events. The MS-ISAC does not collect any fees from its members, which include all fifty states, and provides a variety of services, including the monitoring of security standards and consulting. Thus, it has succeeded—in a non-conventional manner—in bringing together the federal government's activity and the efforts of the various states in defending against cyber threats.

The European Union

The European Union is a framework of democratic countries in Europe, which originated around creating a common European market. The European Union was not meant to replace existing states and is not a federation like that in the United States. Nonetheless, it can be viewed as a kind of umbrella organization to which European states have transferred part of their sovereign decision-making powers, including in the domain of cyber.

The European Union is made up of three main political institutions, which are responsible for its regulatory activities. The EU Council generally represents the political interests of the member states and its functions are to approve or amend legislation proposed by the EU Commission, to approve the EU budgets, and to sign international agreements. The third institution is the European Parliament, which represents the citizens of the member states, and is chosen directly by them. Its members can present queries to the EU Council and the EU Commission and can require them to report on their activities. The EU Commission is the body that represents joint European interests. It initiates and coordinates EU policy and legislation and supervises their implementation and enforcement and is also meant to supervise the implementation of EU legislation in the member states, to prepare and manage the EU budget, and to carry on negotiations with states outside the European Union and with other international entities. The EU Commission is composed of twenty-five representatives that manage the day-to-day affairs of the European Union in a wide range of domains, including agriculture, the environment, energy, taxation, budgeting, health, communication, the digital domain, internal security, and justice.

The European Commission is one of the main players in cyberspace in the European Union. Cyber protection regulation in the European Union differs from the patchwork situation in the United States, despite its convoluted institutional structure. Cyber security in the European Union is based on an organized and hierarchical strategy that places emphasis on the protection of personal information and the right to privacy. The main strength of the strategy is in deciding on cyber regulation of the EU member states, where each state implements the regulations by means of domestic laws and directives. The regulations, laws, and policy directives relate to most of the sectors of the economy, including manufacturing, critical infrastructures, and the main market players in the internet economy.

The European Union's regulatory regime in the cybersecurity domain includes the EU Commission's policy strategies, the binding directives that apply to the member states, and the creation of collaborations between the various agencies. The involvement of the European Union in the cybersecurity domain has broadened over the years. Thus, already in 1995, the EU Council decided on the need for joint criteria for the evaluation of cyber risk among the EU member states,[94] but only in 2004 did regulation become a pro-active effort, with the establishment of the European Network and Information Security Agency (ENISA).

ENISA's operations began with the acceptance of responsibility for emergency simulations of cyberattacks. It is involved in the development of strategies for risk management among the member states and it assists their institutions by creating mechanisms for information sharing in order to deal with cyberattacks in real time. ENISA's realms of responsibility have expanded over the years and decisions by the EU Commission in 2008 and 2017 enlarged its budget and powers, which is an indication of the growing importance attributed by the EU institutions to dealing with cyber risk.

In addition to the regulatory activity of ENISA, in 2012 the European Union established the EU Computer Emergency Response Team (CERT-EU) with the goal of protecting the EU networks from cyberattacks. Another EU institution that is responsible for cooperation between the states on the issue of cybercrime is Europol's Cyber Crime Center (EC3), which was founded in the same year.

---

94 Council Recommendation 95/144/EC, April 7, 1995, http://eur-lex.europa.eu/legal-content/ EN/TXT/PDF/?uri=CELEX:31995H0144&from=EN.

In addition to the institutional activity, the EU Commission publishes strategies for the regulation of cyberspace every few years. In 2001, it published a proposal for the protection of networks and information systems, and in 2006 this proposal was grounded in a new strategy called *A Strategy for a Secure Information Society*, which includes measures for the improvement of information security. The Stockholm Program and the Digital Agenda for Europe, which include recommendations and measures for ensuring information security in European systems, were published in 2010. They called for the establishment of event response teams, as well as measures to prevent cyberattacks.

The turning point in cybersecurity occurred in 2013, when the European Union adopted a comprehensive cyber policy. The new strategy brought together all the previous strategies and programs and emphasized basic European values, such as freedom of expression, privacy, democratic governance, and joint responsibility for security. The main goal of the new strategy was to increase the resilience of cyberspace, as part of the EU responsibility for the European common market and the security of its member states. In this context, the strategy created minimal requirements for the protection of cyberspace, including the reporting of cyber events. The strategy also includes efforts to reduce cybercrime, while strengthening the capabilities of the member states to eliminate it.

Cyber security strategy in the European Union is part of Europe's Common Security and Defense Policy, which the EU states agreed to at the Nice Conference in 2001 and which encourages cooperation between the states on issues of security and defense. At the same time, the strategy relates to the development of technological resources for the advancement of cybersecurity, with the goal of reducing the dependence on external sources and creating stringent standards for security products. As a result, the EU budgets were enlarged and efforts to promote this issue were reinforced. Since 2013, more than 600 million euro have been invested in R&D in these domains.[95] The European strategy also relates to the promotion of cybersecurity on the global level, as part of the European Union's foreign policy.

---

95 European Commission, "Cybersecurity Initiatives," January 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

In 2016, the European Union established the Contractual Public-Private Partnership (CPPP) to further cooperation with the business sector in cybersecurity and with the goal of promoting the development of new cybersecurity products for the member states.

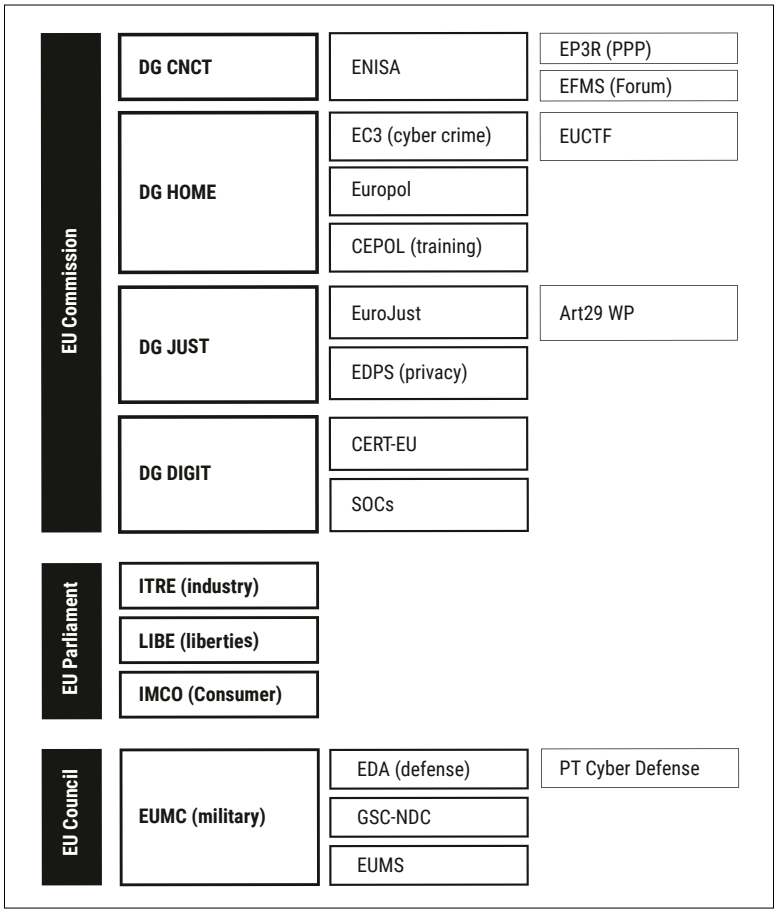

Figure 2: Agencies and institutions in the European Union that deal with cybersecurity

The EU institutions involved in cybersecurity (see Figure 2 above) can be roughly divided into four categories:

1. The defense of the civilian-business sector and the EU institutions is the responsibility of ENISA, which draws up the standards for the member states and coordinates the centers for reporting of cyber events throughout the European continent. ENISA gathers and analyzes information on cyber events; promotes the evaluation and management of risk in order

to exploit organizations' abilities to deal with cyber events; carries out simulations to test the resilience of the European Union in cyberspace; supports the CERT organizations in the member states; is responsible for information sharing to protect critical infrastructures; and raises awareness of cybersecurity and protection in organizations. The month of October has been declared as the designated awareness month.

2. The EU Computer Emergency Response Team (CERT-EU) was created, as mentioned, in 2012 with the goal of efficiently and actively managing the response to cyberattacks on EU institutions. Cooperation on this issue involves cyber protection experts from all the EU institutions, the member states, and business protection organizations.
3. Cybercrime is under the responsibility of EC3, which was established in 2012 as part of Europol, with the goal of creating a single address for fighting cybercrime on the level of the European Union. EC3 supports the member states and their investigations; it carries out strategic analysis of what is happening in the domain of cybercrime; it furthers cooperation between the relevant players, including law enforcement agencies, the business sector, academia, and relevant security companies; it supports simulations to eliminate cybercrime among the member states; it carries out investigations of cybercrime events; and it supports the efforts of member states in this domain.
4. The protection of national security systems is carried out by the European Defense Agency (EDA).

The EU institutions also deal with the protection of privacy. This is carried out by two bodies: the European Data Protection Supervisor (EDPS), which connects between all the information security officers in the various member states, and Article 29 Working Party. They provide guidance to the member states on controversial information security issues (such as the use of drones for photography). A large part of their activity involves information security in cyberspace.

Although the European Union as a body has no declared mandate in cyber legislation, EU regulation by means of legislation has been developing since 2005. In that year, the EU Commission's constitutional infrastructure for protection against cyberattacks was created. The goal of the infrastructure was, first and foremost, to strengthen cooperation between the various authorities in each EU member state. In 2013, this infrastructure became the Directive on Attacks against Information Systems whose constitutional basis is the

covenant on the EU functions, which makes it compulsory for EU members to cooperate on issues related to crime. In 2013, the EU Commission also laid the foundation for early protection of computerized systems, based on the economic justification that computer infrastructures must be protected in order to ensure the functioning of the EU common market.

In 2016, the Network and Information Security (NIS) directive and the General Data Protection Regulation (GDPR) directive, two binding directives dealing with cybersecurity and information security, were approved by the European Union. The former, which is expected to go into effect at the end of 2018, is the first attempt to create uniform minimal standards for cybersecurity in all the EU states. It requires that each member state create a cybersecurity strategy that is appropriate to its needs and at the same time the European Union is to create a designated agency that will ensure the implementation of the directive in the various states. In this context, each member state was also given the power to impose sanctions in its jurisdiction in the event of a violation of the conditions of the EU cyber protection strategy. The directive relates not only to the business sector in each country but also to the state networks themselves.

The 2016 GDPR directive, which went into effect on May 2018, updates the previous EU privacy protection directive, which was for twenty-one years the most important privacy and information protection regulation. The goal of the new directive is to allow users to make decisions regarding the way in which their personal information is to be transferred or shared with others. The directive relates to the "right to be forgotten," which makes it possible to request the removal of unreliable information; the explicit consent of individuals for the processing of their personal information; the reporting of information theft and violations of privacy as a result of cyberattacks within seventy-two hours; and the right of individuals to transfer information between various service providers.

The NIS directive also calls for the creation of mechanisms for strategic cooperation between member states and places special emphasis on the financial, energy, transportation, banking, health, and digital infrastructure sectors. The main innovation of the directive in this context is that search engines, cloud infrastructure providers, and online stores will be subject to binding cybersecurity directives and will be obligated to report occurrences of cyberattacks and information theft. Similar directives already apply on

the EU level to operators of internet and communication networks as part of the 2009 EU Telecoms Regulatory Framework.

Essentially, a constitutional infrastructure for cyber protection on the EU level was established already in 2001 when the EU institutions passed legislation against cybercrime, issued directives to eliminate fraud in online services, and required that member states broaden the definition of cybercrime. In this context, the European Union published directives in 2011 to deal with online exploitation of children and in 2013 issued a directive for the protection of computerized systems against crime. In addition to the request that member states refine the definition of cybercrime, the European Union asked them to impose more effective sanctions on cyber criminals.

It appears that the EU member states prefer directives that are less binding, while the EU institutions insist on clear and binding standards for information protection and have sought to create uniformity between the member states with respect to cyber protection. Currently, only seventeen of the EU members have any sort of cyber protection strategy and each of the existing strategies differs from the next. The European Union therefore sees a need to incentivize standardization of cyber protection in all the member states and wishes to establish a binding and uniform standard.

The history of privacy protection in the European Union was surveyed in a 2008 article by Abraham Newman.[96] The article discusses the policy that preceded the EU basic legislation on privacy passed in 1995. Until that point, there was no clear desire on the part of the member states to promote legislation at the EU level for the protection of information and privacy. It was, in fact, the information protection institutions on the state level that promoted this issue and formulated the legislation at a later stage. Nonetheless, the need for the protection of privacy, in view of the efforts by foreign states to penetrate this domain, was evident to legalists and academics who had been involved in the issue since the 1960s. The awareness of this need slowly trickled down to the member states and at the end of the 1970s, France, Germany, and Luxembourg instituted a reform that provided powers to state information protection institutions to enforce the local privacy laws. These powers also provided the institutions with independence from politicians

96 Abraham Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62, no. 1 (2008):103–130.

and ministers, which was critical in the formulation of later legislation. Other countries, such as Switzerland, adopted less binding legislation, which related to sensitive sectors only, such as health and banking. This legislation largely relied on market forces and self-regulation. Italy, Greece, Spain, Portugal, and Belgium had not passed any sort of privacy protection legislation and only in 1995 did they join the general trend in the European Union by adopting national legislation on this issue.

The advocates of information privacy successfully lobbied the EU institutions and finally managed to convince the European Parliament to adopt a series of decisions on the issue. In contrast, the European Commission did not exhibit any interest in the issue; it was hesitant primarily in view of the costs that would be imposed on the business sector. This attitude continued until the 1990s. The European Council, for its part, created a working group on the issue, although it did not have any real influence on the development of privacy protection in cyberspace.

The change in understanding that the protection of privacy must be dealt with also above the state level and that the European Union must adopt a uniform and stringent standard for all its members occurred, as mentioned, primarily as a result of the growing strength of the independent privacy protection institutions in each of the member states. In 1988, there were already eleven such institutions, which collaborated in promoting solutions to the issue of privacy in the European Union. This collaboration continued until the creation of the draft reform that introduced privacy protection at the EU level.

The variation among the EU countries with respect to the method of privacy protection cast doubt on the ability to formulate uniform norms on issues of privacy in Europe. This situation, together with the economic implications and trade barriers that were created from such variation, emphasized the very immediate need for uniform privacy laws in Europe. At this stage, the state-level privacy protection institutions were powerful enough that they threatened to block the flow of information within and out from the European Union, if the European Union did not pass privacy legislation by 1992. Against this background, and despite the opposition of industry, the European Commission was in the end convinced to support stringent privacy legislation. The business sector was not a major player in the process but cooperated in order to reduce its future regulatory costs. In the end, the

state-level privacy protection institutions managed to change the European Union's order of priorities on this issue.

The 1997 Treaty of Amsterdam, which updated the cooperation agreements between the EU members and reflected their agreement to promote legislation on this issue through the European Parliament, applied the information and privacy protection directives also to EU institutions. In this context the European Data Protection Supervisor (EDPS) was established to monitor the level of compliance with the privacy laws among EU institutions.

Another important contribution to personal information protection legislation in the European Union was in promoting cybersecurity. This was due to the fact that organizations and bodies in the EU states would now have to prove that they had adopted all of the potential protection measures for preventing the exposure of personal information by unauthorized entities. Furthermore, the regulation expanded the definition of personal information and defined genetic, psychological, economic, cultural, and social information as information that must be protected. As part of this move, it restricted the amount of time during which such information could be stored. In addition, the directive includes major fines and sanctions in the case of a violation of privacy and the lack of sufficient protection of personal information. Such fines can be up to 4 percent of any company's turnover or up to €10 million, whichever is higher.

The efforts of the European Union in the domain of cybersecurity and, in particular, its progress since the strategy was adopted in 2013 reflect the European Union's desire to become globally influential as well as the one that directs the protection efforts in the member states. This approach emphasizes the importance of both the public and business sectors and has been influential on various levels.[97] Nonetheless, cybersecurity is not explicitly mentioned in the various EU treaties, and in theory, even today the EU institutions do not have a clear constitutional mandate in cyberspace. Therefore, the European Union is working to develop a strategy that links the needs of cyber protection and collaboration in other domains by means of, among other things, incentives to the member states.

---

97 Ramses A. Wessel, "Towards EU cybersecurity Law: Regulating a New Policy Field," in *Research Handbook on International Law and Cyberspace*, ed. N. Tsagourias and R. Buchan (Cheltenham, Edward Elgar, 2016), chapter 19.

Britain

The British government became involved in cybersecurity already in 1997 with the development of a plan for protecting government ministries called the Government Secure Intranet (GSi). The goal of the plan was to facilitate information sharing between the various government ministries in security matters. In 1999, the government expanded its efforts by establishing the National Infrastructure Security Coordination Center (NISCC) whose goal was to minimize threats to critical infrastructures and protect them from electronic attacks.[98] The cyberattacks on Estonia in 2007 that affected most of the online services in the country were another wakeup call for the British government and led to the creation of the Center for the Protection of National Infrastructure, which consolidated the NISCC and the National Security Advice Center (NSAC), a unit of MI5, the British domestic intelligence agency. The goal of the new center was to ensure the security of national infrastructures in Britain and protect them from cyber threats.

The main British law dealing with critical infrastructures is the 2004 Civil Contingencies Act, which provides broad powers to the state in important sectors, such as communication, transportation, water, and electricity. These powers include the granting of licenses and suspension of operating permits held by businesses in the case of threats to national security that arise due to lack of protection of critical infrastructures. At the same time, the basic approach of the private sector in Britain was largely one of voluntary cooperation.

In 2009, the first national British strategy in cyberspace was published. It included the definition of both cybercrime and cyberattacks from five main sources and viewed the cyber threat as a threat to both national security and the national economy.[99] The strategy was updated in 2011 and became a five-year plan for cybersecurity in Britain (2011–2016) with a budget of 860 million pounds. The goals of the updated strategy were the elimination of cybercrime, the protection of economic and national interests in cyberspace, the fashioning of a stable cyberspace that would provide all citizens with

98 "The Launch of the National Cyber Security Center," *NCSC*, February 2017, p. 8.

99 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "The United Kingdom Cyber Readiness at Glance," (Potomac Institute for Policy Studies, 2016), p. 5.

the ability to express themselves, and the development of British knowledge and capabilities in cyberspace.[100]

In November 2016, the strategy was renewed for another five years and its budget was doubled to 1.9 billion pounds.[101] The new strategy warned that alongside the opportunities that have emerged in cyberspace, there are new threats and hostile elements that are interested in stealing information and causing damage to Britain.[102] The strategy also stated that the cooperation between the government and the business sector on issues of cyber protection is not creating sufficient protection against threats in this domain and that significant number of critical infrastructures are not sufficiently secured. Specifically, the British government claims in the strategic document that the business sector is not acquiring protection for itself at a satisfactory pace and therefore the government must be actively involved and must be present in a more forceful manner in the activity of the private sector in cyberspace.[103] The new strategy also identifies a number of market failures: The first is the insufficient effort on the part of various bodies to protect the public interest in the domain of information security and protection of privacy; the second is that the business sector does not sufficiently recognize the various threats and the ways to protect against them and there is a crisis of confidence between providers of protection and various organizations and companies.

The institutional structure

The British view of cybersecurity has three main characteristics: first, intelligence organizations are the leading players in the defensive and offensive efforts in cyberspace; second, players in the market and the various companies have a major influence on the government's cyber policies; and third, the government, as the body responsible for protecting the public, has a leading role to play and serves as an example to other players with respect to protection in cyberspace.

---

100 "The Final Annual Report on the 2011–2016 UK Cyber Security Strategy," UK Parliament, April 2016, p. 7.

101 "National Cyber Security Strategy 2016 to 2021," HM Government, November 2016.

102 "National Risk Register of Civil Emergencies," Cabinet Office, 2015.

103 "National Cyber Security Strategy 2016 to 2021," HM Government, November 2016.

The first characteristic—the dominance of the intelligence community in defensive and offensive efforts in cyberspace—has become increasingly clear over time. George Osborne, the former chancellor of the exchequer, was quoted as saying that the GCHQ, the British electronic intelligence organization, has a unique role to play and has a major influence on cybersecurity in Britain relative to other agencies. According to Osborne, other bodies, such as the Ministry of Defense, law enforcement agencies, and the business-civilian sector are important in their own right, but the importance and influence of the GCHQ are paramount.[104]

The other two characteristics—the role of market players and of the government—are manifested in, among other things, the imposing of non-binding regulation on the business-civilian sector, in parallel to the adoption of the state's cybersecurity regulations in the various government ministries. In addition, the state is trying to incentivize organizations in the business sector in Britain to adopt its recommendations in this domain by making their participation in government tenders conditional on doing so. The financial report of the British Parliament on the government's cyber activity for the period 2011–2016 places responsibility for the protection of national infrastructures on the business sector, while mentioning the fact that the government works in full cooperation with British industry and provides it with expertise and guidance as needed.[105]

The soft approach to the business sector can also be seen in the way that the state chooses to protect information privacy. The approach adopted by the British government toward the business sector is a friendly one and includes few binding directives. Furthermore, the majority of directives are accompanied by incentives. These incentives include tax breaks on cybersecurity expenditure and government grants to achieve sufficient cyber protection (which, as mentioned, is a criterion for participation in government tenders). The government has also refrained from issuing binding directives

104 George Osborne, "Conversation with the Intelligence Community on Britain's Cyber Efforts," November 17, 2015. For the full text of the speech, see https://www.gov.uk/government/speeches/ chancellorsspeech-to-gchq-on-cyber-security.

105 "The Final Annual Report on the 2011–2016 UK Cyber Security Strategy," UK Parliament, April 2016.

that would create a culture of compliance among companies but would not provide a full solution to the evolving threats in cyberspace.[106]

In order to outline the development of cyber regulation in Britain, we will describe the main players and their roles, including the decision in 2017 that consolidated the various agencies dealing with cybersecurity under one institutional umbrella. As mentioned, the main player in this domain is the GCHQ, which reports to the secretary of state for foreign and commonwealth affairs (who is not part of the British Foreign Office). This intelligence organization was established as the Government Code and Cipher School in 1916 and received its current name in 1946. It has more than 6000 employees and cooperates with the British intelligence organizations MI5 and MI6. Its declared mission in cyberspace is to protect government systems against cyber threats, to support military forces in both the physical world and cyberspace, and to protect the public in these same domains. The agency is responsible for the security of critical infrastructures, the support of industry in cyberspace, protection of cyberspace in general, and the promotion of cyber awareness.

In 2017, Britain established the National Cyber Security Center (NCSC), a new organization to deal with the cyber threat, under the auspices of the GCHQ. Following are the main agencies consolidated within the new framework:

1. Communications-Electronic Security Group (CESG) (which until then operated as part of the GCHQ)
2. Center for Cyber Assessment (CCA)
3. Computer Emergency Response Team UK (CERT UK)
4. Center for the Protection of National Infrastructure (CPNI)
5. Cybersecurity Information Sharing Partnership (CiSP).

The NCSC is meant to deal with all the sectors that operate in cyberspace, while giving preference to sectors related to national security and that have strategic and economic importance.[107] The approach decided on for the new framework enables the business sector to be involved in the formulation of cybersecurity directives. To this end, a designated forum of cyber regulators

106 "Cyber Security Regulation and Incentives Review," HM Government, December 2016, p. 3.

107 Conor Ward, "The UK's Cybersecurity Regulatory Landscape: An Overview," *Hogan Lovells Chronicle of Data Protection*, December 2016.

was created in order to share knowledge and information for the general good. NCSC operates in close cooperation with the Ministry of Defense, industry, and academia, with the goal of ensuring that the cyber protection that it provides is on a sufficiently high level.

The declared goals of the new institutional framework for cybersecurity are the gathering and sharing of information, the development of capabilities in cyberspace, providing a response to cyber events, and support of privately or publicly owned critical infrastructures. One of the reasons for the unification of the various British agencies in cyberspace was to foster a better understanding of the state's role in this domain and to create greater access to government entities that are active in it. This was the result of, among other things, a study of the cyberspace situation in Britain, which found insufficient awareness of the government's cyber programs among the various sectors.[108]

In order to understand the role of the new framework, its component agencies will be described in what follows including its development over time. CESG was the technological arm of the GCHQ in all aspects of information security. It has been in existence since the World War I and its main activity focuses on the branches of the military and the security of government networks. Its major activities include, among others, a program for the protection of the public sector called the Certified Cyber Security Consultancy Scheme, which provides certification of the level of information security and approves companies that have been authorized to provide protection to the public sector.[109] Another important program of the CESG is Cyber Essentials (in collaboration with the insurance industry) whose goal is to provide guidance in cybersecurity to organizations. The program has five main characteristics: a secure definition of services; an appropriate separation between the various realms in organizational networks; control of access and authorizations; management of software updates; and protection against malware.[110] Since October 2014, this program became binding upon suppliers and providers of services to the government. Those that choose to

108 Rebecca Klahr et al., "Cyber Security Breaches Survey 2017," *University of Portsmouth Research Portal*, April 2017.

109 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "The United Kingdom Cyber Readiness at Glance," (Potomac Institute for Policy Studies, 2016).

110 HM Government and MARSH, "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk," 2015.

adopt it receive a kind of seal of approval and benefit from lower insurance premiums. Since the program's founding in 2014, it has provided more than two thousand approvals to various organizations.

The large companies in the British economy (Barclays, Lockheed Martin, BAE Systems, and Hewlett-Packard) operate according to the standards proposed in this program. Nonetheless, a survey carried out in 2017 showed low rates of adoption in the business sector in Britain—only ten percent of small companies and twenty percent of large ones. One of the conclusions of the survey was to make the program mandatory. The survey also found that the program involves high costs and that cost-benefit analyses of the program are not always accurate.[111]

The second important organization in the NCSC is CERT-UK, which was founded in 2014. Prior to this, there were about twenty private and public bodies operating in collaboration with one another in cyberspace. The two main ones were the Computer Security Incident Response Team (CSIRT-UK), which operated as part of the CPNI, and GovCertUk, which functioned within the framework of CESG. During the two years since it was established and until it started reporting to NCSC, CERT-UK worked with industry, the state, and academia in Britain in order to improve the abilities to respond and recover from attacks in cyberspace. To this end, the organization held three simulations annually, which were intended to test the readiness of the systems and the depth of cooperation between them. The roles of CERT-UK are to respond to events in real time, to raise awareness of cyber risk, to support critical infrastructures, and to act as the liaison with the various CERT organizations around the world.

Another organization within the NCSC is the Center for the Protection of National Infrastructure (CPNI), which operates as part of MI5. It was established in 2007 following a merger of two institutions: NISCC for the protection of critical infrastructures and NSAD, which operated as part of MI5 and provided guidance to various bodies within the British government. The goal of the merger was to assist the government in the protection of national infrastructures and to deal with terror threats. Britain defined thirteen critical sectors (chemicals, the nuclear-civilian sector, communication,

111 Chad Heitzenrater and Andrew Simpson, "Policy, Statistics and Questions: Reflections on UK Cyber Security Disclosures," *Journal of Cybersecurity* 2, no. 1 (2016): 43–56.

security, emergency infrastructures, energy, finance, food, government services, health, space, transportation, and water).[112] A critical infrastructure, according to the British government's definition, is any facility essential to the normal functioning of the state.

Over the years, the CPNI has issued several directives, to both large organizations and small and mid-sized businesses, which include cybersecurity standards. The organization also provides infrastructure for the prevention of cyber events and the response to them and provides guidance to workers and business owners with respect to threats in cyberspace and ways of protecting against them. This activity is based on the vision of inculcating correct work habits and raising the awareness of network protection.

Another important institution is the Center for Cyber Assessment (CCA), which was established in April 2013. This body provides assessments of intelligence information and has access to, among other sources, classified intelligence information, which is the responsibility of GCHQ. The CCA provides guidance to relevant government bureaucrats and assessments of cyber risk to the state's critical infrastructures.

The efforts to share information about cyber threats in Britain are largely the responsibility of the Cybersecurity Information Sharing Partnership (CiSP). This program brings together industry, the government, and law enforcement agencies and facilitates the sharing of information on cyber threats in a confidential and secure manner. As of May 2016, there were about 2,220 British organizations that were members of the program and it has become an example to other countries. At the same time, surveys carried out among the program participants show that 58 percent of the respondents think that the cyber breaches they have experienced do not require reporting and that they do not know to whom to report.[113] Sharing of information by means of CiSP is an indication for the insurance companies of how to price protection policies in cyberspace. Essentially, the British market still does not offer competitive insurance policies that would provide genuine cyber protection at a reasonable price.

---

112 "Summary of the 2015-16 Sector Resilience Plans," Cabinet Office, May 2016.

113 Rebecca Klahr, Shah Jayesh, Sheriffs Paul, Rossington Tom, Pestell Gemma, Button Mark, and Wang Victoria, "Cyber Security Breaches Survey 2017," *Portsmouth Research Portal*, April 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf.

In addition to the large-scale activity of the NCSC framework, the British Ministry of Defense has the power and responsibility for developing offensive and defensive capabilities in cyberspace, with the goal of providing protection against the various threats in this domain. Britain's military activity in cyberspace is under the responsibility of the Joint Cyber and Electromagnetic Activities Group (JCG), which includes the Joint Force Cyber Group, whose task is to develop cyber capabilities. In addition, the Defense Assurance and Information Security (DAIS) organization is responsible for information security in the British defense system.

The development of offensive capabilities in cyberspace is under the responsibility of the GCHQ, which operates in collaboration with the Ministry of Defense. The British government recently allocated 40 million pounds to the development of the Cyber Security Operations Center (CSOC), which is part of the Ministry of Defense and also operates under the guidance of GCHQ. The goal of this body is intelligence analysis and research in cooperation with other agencies, with the goal of providing protection to national networks in general and those of the Ministry of Defense in particular.

Another important institution is the National Crime Agency, which deals with cybercrime. The strategic document published in 2016 describes the British activity against cybercrime on both the national and international levels. At the national level, the National Crime Agency focuses on crimes against British citizens and on supporting victims of cybercrime, as well as handling British cyber criminals. At the international level, it focuses on organized crime and reducing the profitability of cybercrime. Within the National Crime Agency is the National Cyber Crime Unit (NCCU), which coordinates the efforts to counter cybercrime and, during a crime event, it coordinates the activities of the law enforcement entities, such as the NCSC and the GCHQ. Each district of Britain has a unit to fight regional crime, which all have designated units to thwart cybercrime.

Legislation

British legislation regarding cybersecurity focuses on the protection of privacy and information, which is accomplished by means of two main laws: the 1998 Data Protection Act and the 2003 Electronic Communications Regulations, which relate to the gathering and processing of information. The legislative process began already in 1984 at the initiative of the Information Commissioner's Office (ICO), an independent agency whose task is to

protect privacy. It set down eight principles for the management of personal information. The original task of the agency was the registration of owners of new databases; however, in 1987 it established an investigations unit and when the Data Protection Act went into effect in 1998 its powers were expanded and it became responsible for ensuring that personal information would be handled according to the law and only for defined purposes. In this context, it was decided that sanctions would be imposed on anyone that does not provide sufficient protection of personal information.

In 2011, the ICO was also given the responsibility for implementing the Freedom of Information Act, which gave it the power to impose fines of up to half a million pounds for the violation of privacy. In 2015, the government removed the condition of proving damage in order to impose a fine, which increased the agency's power even further. Currently, it can demand information from organizations on the way in which they protect their customers' privacy; it can require them to adopt additional measures; and it can carry out audits, impose fines, and file suit in court against anyone that does not fulfill the requirements of privacy protection. Thus, for example, in 2015–2016, the ICO imposed fines of 2.6 million pounds and the pace at which fines are imposed has been increasing ever since. The fines have proven to be effective on two levels: as a factor that brings about change in organizational practice and as a deterrent to other organizations.[114]

Although there is no comprehensive law[115] that requires reporting of cyber events and a possible violation of personal information confidentiality, there is a consensus in Britain that the ICO is the address to report to and that it is the one to decide on a proper response, whether by imposing sanctions or by investigating an organization's cybersecurity situation.

The main British law that deals with the gathering of information in cyberspace and its monitoring by the state is the Regulation and Investigatory Powers Act (RIPA), which was passed in 2000. Another law in this area is Data Retention and Investigatory Powers (DRIP), which was passed in 2014 and which allows the secretary of state for foreign and commonwealth affairs to demand that communication companies submit information up

114 "Information Commissioner's Annual Report and Financial Statements 2013/2014," *Information Commissioner's Office.*

115 Apart from the communication sector, which is subject to designated regulation introduced in 2003, the Privacy and Electronic Communications (EC Directive).

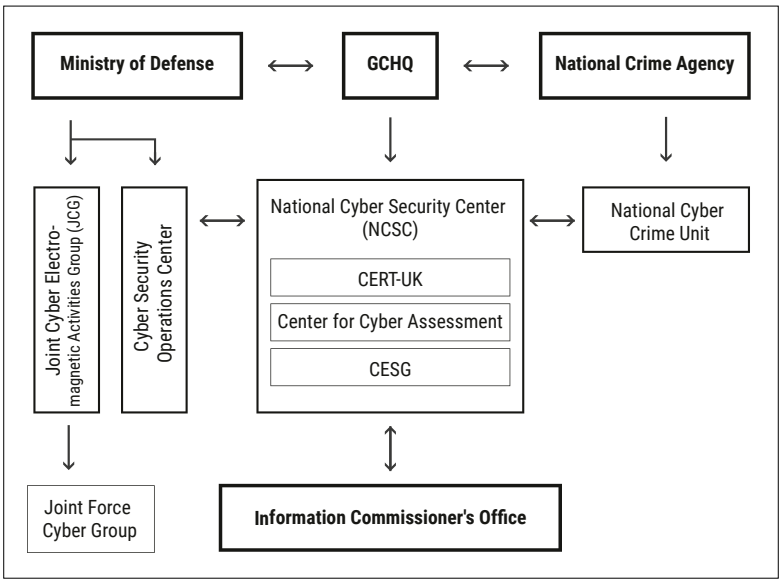

Figure 3: Agencies and institutions involved in cybersecurity in Britain

to one year back. In November 2016, the Investigatory Powers Bill was passed, which brought together the two laws and consolidated their powers and responsibility in cyberspace.

The spheres of privacy and monitoring of information in cyberspace form the core of activity of various British agencies, where the 2015 National Security Strategy embodies the government's goal of achieving a balance between promoting national security and protecting citizens' privacy.[116]

Figure 3 above describes the institutional structure of the bodies described above and provides a clear picture of the roles of the various players and the mutual relations between them.

France

Three major cyber events have demonstrated the importance and urgency of protecting cyberspace in the eyes of the French authorities: The first was the cyberattack on Estonia in 2007 that paralyzed state services. It formed the background to the French government's directive in 2008 giving top

116 UK Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015, p. 19 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

national priority to cyber protection. In the second event, in early 2009, the French Ministry of Defense was a victim of the Conficker worm,[117] which reinforced the understanding among French decision makers that more aggressive state intervention was needed in order to deal with the threats in cyberspace. The third event was the exposure of the Stuxnet attack in 2011, which led the French president to issue a directive, followed by a government decision, that emphasized the importance of cybersecurity.

Another development in the French government's position on cybersecurity occurred in 2015 when France experienced two major cyberattacks. In January of that year, the terror attacks by ISIS on the French newspaper *Charlie Hebdo* were accompanied by efforts against private and public French websites; and in April 2015, ISIS engineered a digital takeover of the TV5 television station and hacked it with messages in support of fundamentalist Islam and against the French government.

Only a few studies have investigated France's efforts in cyber protection. A study published in 2014 looked at the cybersecurity activity of the various agencies in France[118] and an evaluation published in 2016 examined France's cyber defense capabilities in the various domains.[119] The main insights from these studies will be presented below, with the goal of drawing a comprehensive picture of what is being done in cyberspace in France.

The main differentiation in the French regulatory regime is between cyber defense, which relates to the operational/pro-active defense capabilities in cyberspace on the one hand and cyber protection, which relates to the prevention of cyberattacks, on the other. These two goals are, of course, interrelated and sometimes complementary and are promoted and regulated by the various laws and agencies in France.

---

117 Conficker is a computer worm estimated to have infected about 12 million computers that use the Windows operating system. For a detailed description of the worm's effect, see Herzl Levi and Afik Kastiel, "Analysis of the Conficker worm," *Digital Whisper* 6, March 2010, https://www.digitalwhisper.co.il/files/Zines/0x06/DW6-3-Conficker.pdf [Hebrew].

118 Philippe Vitel and Henrik Bliddal, "French Cyber Security and Defence: An Overview," *Information & Security: An International Journal* 32 (2014): 3209–1–13.

119 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "France Cyber Readiness at a Glance," (Potomac Institute for Policy Studies, 2016).

The institutional structure

Four main players can be identified in French regulation of cyberspace. The first is ANSSI, the National Agency for Information System Security, the main body involved in cybersecurity in France. The agency was created in 2009 and reports directly to the Prime Minister's Office. Its main activity is the protection of critical infrastructures and the prevention of cyberattacks. Its budget grew significantly between 2010 and 2014, from €43 million to €83.8 million.[120] ANSSI is not an intelligence organization that gathers information for purposes of defense; rather it can be viewed as the counterpart of the Department of Homeland Security in the United States.

The French strategy in cyberspace since 2013 has centered on the powers of this agency to protect the operators of critical infrastructures. An attack on the public or private bodies that operate these infrastructures will cause significant damage to the state's economic abilities and/or its capabilities to defend itself. The list of critical infrastructure operators is classified for reasons of national security. The process to protect critical infrastructures essentially began much earlier than 2013 and acquired greater urgency after the major terror attacks in the United States, Madrid, and London.[121] An internal document of the French Ministry of Defense discussed critical infrastructures already in 2005 and 2006 and included twelve sectors in four domains: infrastructures for citizens (health, food, and water); infrastructures for the functioning of the state (military and civilian, including the court system); economic infrastructures (energy, transportation, and the financial sector); and technological infrastructures (industry, space, and information). The operators in each of these sectors were defined as "operators of critical infrastructures."

The main role of ANSSI is to introduce the desired standards for cyber protection, to receive reports on cyber events that occur in critical infrastructures, to carry out unannounced audits of cybersecurity, and to decide how to classify various networks. Essentially, these are the only binding directives in cyberspace in France. Another function of ANSSI is to encourage the cyber industry in France and to raise awareness of cyber risk

120 French Prime Minister's Office, "Politics of France Cybersecurity," February 20, 2014, https://www.ssi.gouv.fr/uploads/IMG/pdf/dossier_de_presse_web_20140220.pdf.

121 See the official document of ANSSI, which describes this process: https://www.ssigouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/.

among its citizens. Organizations that do not come under the definition of critical infrastructure operators are not subject to the binding cyber protection directives issued by the state.

In 2017, ANSSI published a document that included forty-two recommendations for cyber protection, as well as directives designated for small and mid-sized businesses. In addition, it created a special stamp—the France Cybersecurity Label—which is awarded to French information security solutions. The agency is also involved in the licensing of products and service providers according to three levels of expertise. Products and professionals with the highest classification granted by the state are authorized to work with critical infrastructure operators. In addition, ANSSI is involved in campaigns and conferences to raise awareness of cyber risk.

Another important player in France's cybersecurity is the Ministry of Defense. In 2011, it created a new position—the Head of Cyber Security—whose responsibility is to promote cybersecurity in the Ministry of Defense and to organize activities to strengthen cybersecurity in general. The Ministry of Defense has a designated taskforce whose function is to promote cybersecurity technologies and an operational branch that has the job of identifying and rapidly responding to cyberattacks anywhere in France. In December 2016, the French minister of defense announced changes in the organization of cybersecurity in the Ministry of Defense, including the establishment of a designated cyber unit, the Cyber Command.

The French Cyber Command is responsible for all the cyber capabilities of the Ministry of Defense and reports directly to the head of the joint chiefs of staff of the French military. Early on, developing cyber expertise within each of the branches of the military—sea, air, and land— was considered, but in the end it was decided to create a designated unit that would be responsible for all activity in cyberspace. The Cyber Command's roles include gathering information and intelligence, defense against cyberattacks and their prevention, as well as response to cyber events, if needed. Its realm of responsibility also includes critical infrastructures, and it operates in coordination with ANSSI, which has the overall responsibility for cyberspace in France. The development of automatic responses to cyberattacks is one of the major concerns of the French Cyber Command. Essentially, the responsibility for cybersecurity in France is divided between three agencies: ANSSI, which is involved in the protection of critical infrastructures and operates as part of the Prime Minister's Office; the Cyber Command of the Ministry of

Defense, which is responsible for military operations in cyberspace; and the French Intelligence Agency, which provides technological capabilities for the support of these processes.

The French Ministry of Defense also operates in the civilian sector. In 2014, the ministry announced the development of cyber defense capabilities for all French companies, with the goal of supporting local industry. In this context, the ministry instituted two significant measures: the creation of an elite unit for cybersecurity and a civilian body to raise awareness and connect between academia, industry, and society in order to generate cyber defense solutions.

A third institutional player in French cyberspace is the Ministry of the Interior, which is primarily involved in countering cybercrime. In 2014, the ministry upgraded its capabilities when it created a position designated to thwart cybercrime. The new position was grounded in legislation that provided the powers to deal with cybercrime while also expanding the definition of cybercrime. The Ministry of the Interior also created statistics on cybercrime in order to improve the response to the problem and it also issues an annual report on cybercrime. In addition, the ministry operates in cooperation with other bodies in France that are involved in the protection of cyberspace, with the goal of raising awareness of the problem among minors and encouraging industry to invest in cyber R&D.

A fourth player with a significant role in cybersecurity in France is the National Commission on Information and Liberties (CNIL), which regulates the protection of privacy. This institution has played a leading role in privacy protection not only in France but in all of Europe. Its current budget is €16 million, and it includes 192 employees. Its powers include investigation and control of the use of various information databases in France and the ability to impose sanctions on organizations that do not operate according to the security directives. The CNIL also receives enquiries from citizens who claim that their privacy has been violated by organizations and institutions that possess their personal information. It also approves automatic processing of information, expresses its opinion of government policy with respect to personal information, advises on matters related to the constitutional infrastructure for privacy protection, and helps private companies understand possible violations of information privacy. The European directives for information protection require that an organization with a large database must inform the CNIL of information theft or a breach of its systems.

Those who are critical of CNIL claim that it is invasive and overregulates, while others claim that it is ineffective in confronting the large technological monopolies, such as Google and Facebook. Nevertheless, French legislation since 2016 has expanded the powers of CNIL, enabling it to impose sanctions for violations of privacy, even on large organizations. This provides it with the ability to demand that even Facebook pay closer attention than it did in the past to the privacy of its users.[122]

Legislation

The legislative infrastructure in France that governs the gathering of information for national security needs, including cyber defense, began to take shape in 1978, with the passing of a national law for the protection of personal information and privacy. France was one of the pioneers in the protection of privacy and information security, both in Europe and worldwide. The law also created the influential privacy agency CNIL. This was followed in 1988 by a law for the prevention of cybercrime, which included the imposition of sanctions, and legislation in 1991 providing the French intelligence agency with broad information-gathering powers. This law constitutes the regulatory platform for France's surveillance programs starting from 2008.

Cybercrime again became an issue in 2001 and 2004, when legislation was passed that updated enforcement powers in order to address technological developments. In 2006, a law was approved giving priority to state security over the privacy of citizens and instructing organizations that gather information on its customers to provide law enforcement agencies with access to their information without a special court order. The priority given to state security was also the goal of a law passed in 2011, allowing for massive gathering of information from computer systems during a "serious" security event, such as a terror attack.

In 2015, the state's security efforts in cyberspace received further constitutional support in the form of new intelligence-gathering legislation, which specified the tools that the security authorities could use and also widened the areas for information gathering in cyberspace beyond just terror, financial intelligence, organized crime, and counterintelligence,

122 Hathaway, Demchak, Kerben, McArdle, and Spidalieri, "France Cyber Readiness at a Glance," p. 10.

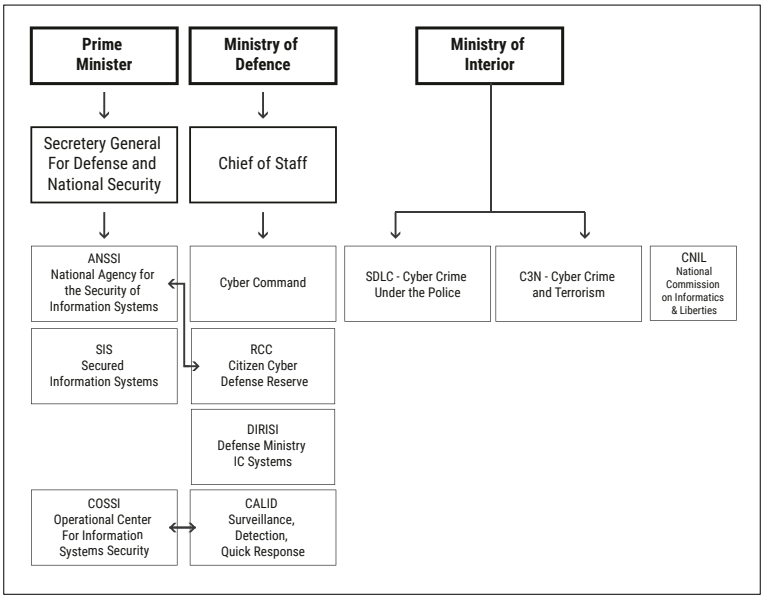

Figure 4: Agencies and institutions involved in cybersecurity in France

such that the state could now gather information even for the purpose of "furthering the interests of French foreign policy" or for preventing violence and damaging public places. The law also permitted more invasive surveillance and information gathering, including in the case of citizens with any kind of connection to a national security threat. The terror attacks in Nice in July 2016 made this law even more invasive.[123]

In October 2016, France tabled the Digital Republic Law, which sought to provide some balance to some extent. The law facilitates the protection of privacy and personal information in cyberspace, while at the same time it raises awareness of the dangers and emphasizes the importance of protecting individuals' interests in this domain. For example, it included the right of an individual to receive all the information gathered about them and the right "to be forgotten" in internet searches. In addition, the law establishes free access to cyberspace for all. However, various terror incidents in France since the law was passed have caused the law to not be fully enforced. Finally, regulation in France was relatively well prepared for the adoption of the

123 Felix Treguer, "Intelligence Reform and the Snowden Paradox: The Case of France," *Media and Communication* 5, no. 1 (2017): 17–28.

Network Security and Information (NIS) directive issued by the European Union. The relevant French regulatory body in this regard is ANSSI.

Figure 4 above describes the hierarchy and relations between the various agencies and bodies in France that are involved in cybersecurity. At the top of the hierarchy are the government ministries; underneath them is the next level within the hierarchy in each ministry; and finally, at the lowest level are players directly involved in drafting cyber regulation.

Germany

The German approach to cybersecurity regulation rests on both state and international players. The first German strategy document on cybersecurity was published in 2011 by the Ministry of the Interior and already in its opening words it had adopted an approach that emphasized "the joint responsibility of the state, industry, and society in promoting cybersecurity in Germany."[124] The most recent strategic document published by the German Ministry of the Interior in 2016 reinforced this approach and even extended it to the scientific domain and the business sector.

The institutional structure

The main entities that play a role in cybersecurity in Germany are the Federal Ministry of the Interior (Bundesministerium des Innern – BMI), the National Cyber Security Council, the Germany military (Bundeswehr), the Federal Intelligence Service (BND), and other government initiatives, as well as information security organizations and civil society organizations.

The German Ministry of the Interior

The Ministry of the Interior is the main regulator for cybersecurity in Germany. Essentially, it brings together most of the state efforts to ensure all aspects of cyber protection, including technology, intelligence, cybercrime, and critical infrastructures. A number of large agencies involved in cybersecurity operate under the aegis of the Ministry of Interior: the Federal Office for Information Security (BSI), which is involved primarily in the technological side; the Federal Office for the Protection of the Constitution (BfV), which is involved primarily in domestic security; the Federal Criminal Police

124 See the strategic document "Cyber Security Strategy for Germany 2011" on the internet site of the German Ministry of the Interior: http://www.bmi.bund.de.

Agency (BKA), which focuses on cybercrime; and the Federal Office of Civilian Protection and Disaster Assistance (BBK), which is responsible for critical infrastructures.

The BSI was created in 1991 and since inception has been responsible for the design and implementation of cybersecurity in Germany, while at the same time it promotes prevention, detection, and response to events. Currently, it is responsible for implementing Germany's cyber strategies and for cybersecurity in all of the sectors: state, business, and civilian. Similarly, it carries out research and produces annual status reports on cybersecurity in Germany. At the beginning of 2017, the BSI had more than 650 employees divided among five departments (one general and four designated): advisory, coordination, encryption, development of standards and certification in matters of cyber and information security.

In 1994, the BSI published for the first time a document of standards for the management of information system protection in Germany and in 2001 it was officially given responsibility for the supply of information security services for the entire country. During the 2000s, with the development of the electronic passport and health card, the BSI developed protocols and technological directives for the support of these projects. It very quickly also became the main body receiving reports of cyber events and identifying gaps in cyber protection in Germany, for both state institutions and the general public. The BSI is also responsible for the CERT centers in Germany. The first CERT in Germany was established by the BSI in 1994 and in 2001 it was declared to be Germany's official CERT center. In 2006, a designated CERT center was created for the citizens of Germany, with the goal of raising awareness and providing reliable and up-to-date information on cyber dangers.

Germany's cyber strategy, which was announced in 2011, instructed the BSI to create a designated center for response to state-level cyber events. The center is called Cyber AZ and works in cooperation with the intelligence and domestic security offices and with the German police. Industry and academia also took part in the design of Cyber AZ and since then have been involved in decision making relating to cyber events. Cyber AZ assists Germany's National Security Council in making decisions on cyber issues, on both a routine basis and in the case of specific events. Essentially, it has led to the institutionalization of information and knowledge sharing between the various authorities responsible for cybersecurity in Germany.

The German Ministry of the Interior is also highly active in critical infrastructures. In 2003, Germany defined a critical infrastructure on the federal level as follows: "Organizations and institutions with high importance to the state and if harmed the result would be a major threat to public security and would lead to difficulty in meeting the country's basic needs."[125] In 2005, the state presented a national plan for the protection of information system infrastructures, which was aimed at both state institutions and industry. The sectors defined by the plan as containing critical infrastructures were energy, communication and information, transportation, health, water, food, finance and insurance, mass communication, media and culture (including television, radio, and digital and printed newspapers), symbolic national structures, and state institutions.[126] In addition, the government at that time came out with a designated program for collaboration between industry and the state in all aspects of critical infrastructure. The program included all relevant sectors defined as having critical infrastructures and related to issues connected to both physical and cyber protection of those infrastructures. In addition, the program designed simulations for the management of cyber events in critical infrastructures, promoted activities for training and instruction in this area, published studies, and defined which critical infrastructures should meet the requirements for protection of their information systems.

In 2007, the federal government issued a plan for the protection of critical infrastructures in Germany called KRITIS. The plan included crisis management and response to events, as well as the functional continuity of the infrastructures. Specifically, the plan presented guidelines for the relations and cooperation between the government and private operators of critical infrastructures and outlined the manner in which they are to respond to cyber events. In 2011, efforts began in order to anchor these principles in legislation, which eventually led to the passing of the IT Security Act in 2015, which constitutes the current legal foundation for the protection of information systems of cyber infrastructure operators in Germany. The law established that private operators must protect not only their sites but also their backend systems. The protection standards are not anchored in legislation but rather are based on the international standards of the ISO or

125 See the definition on the website of the Federal Office of Civil Protection and Disaster Assistance: http://www.bbk.bund.de.

126 See the designated website created for this subject: http://www.kritis.bund.de.

DIN. Refraining from the creation of German standards through legislation was meant to allow defensive systems to be updated over time. As a result, German industry can decide on its own standards as long as they ensure the functioning of the infrastructures. The legislation currently serves also as guidance for industries that are not formally bound by it. The passing of the Information Security Law established the status of the BSI as the main body responsible for the gathering of information on cyber events in critical infrastructures.

The KRITIS regulation went into effect in 2016. It established the criteria according to which private operators are defined as being subject to the regulation of critical infrastructures. This regulation allows the BSI to impose fines of up to €100,000 on critical infrastructure operators that do not meet the mandatory standards. The latest innovation in the cooperation between the state and industry is the call for "Security by Design" whose goal is to introduce considerations of cybersecurity in future software development.

The authorities in Germany have defined the internet as being critical infrastructure for German society. Nonetheless, some experts claim that the federal government is not doing enough in this area by pointing to the insufficient investment in cyber protection within the framework of the national programs to encourage the shift to digitally-based industry.[127] Essentially, the German cyber protection strategy published in 2016 confirmed this situation when it pointed to the lack of state institutions and bodies that can assist the general public in dealing with cyber events and described the ad hoc Mobile Incident Response Teams (MIRTs) as the ones that deal with them.

The BSI is also responsible for the protection of information in the federal networks themselves. It accomplishes this by choosing architecture with redundancy and by adopting a policy of comprehensive encryption. Furthermore, it carries out assessments of cybersecurity for the state and, in particular, it recommends practices that will improve it. Similarly, it carries out evaluations of various cyber protection products that exist in the market and certifies their quality. Thus, for example, from September 2015 to June

127 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "Germany Cyber Readiness at a Glance," (Potomac Institute for Policy Studies, October 2016), http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf.

2016, BSI approved forty-seven different protection products, twenty-seven of which were later rejected for not meeting standards.

Unlike in other countries, the BSI also is responsible for raising awareness of cybersecurity among the public.[128] To accomplish this, it has a designated website that deals with technological issues related to cyber protection, including the provision of information and recommendations on "hot" issues, such as encryption of email, security for mobile phones, and security in the social networks. The popularity of the site can be seen from the fact that between July 2015 until June 2016 it had about 173 thousand visits.

In addition to the intensive activity of the BSI, the German Ministry of the Interior operates in the domain of cybersecurity. Thus, for example, it began an initiative for information sharing between the various bodies in Germany (as part of the Alliance for Cyber Security). The initiative bore fruit and has led to cooperation between the BSI and the Federal Association for Information Management (Bitkom).

The Alliance for Cyber Security brings together all the key players in Germany in both the private and public sectors; it has created a library for cybersecurity and holds roundtables on the subject. Its goal is to support and strengthen the cybersecurity of institutional bodies. Every entity—agencies, commercial companies, and academic research institutes—can participate and use its information, according to security classification and the degree of urgency.

Another activity of the Ministry of the Interior is the development of technological capabilities to fight crime and terror. In this context, the Ministry of the Interior created the ZITiS unit, whose function is to create technological capabilities for monitoring communication networks, investigating networks, breaking codes, working with big data and issues related to espionage and cybercrime. The unit currently has about 120 employees and a budget of about €10 million.

Within the Ministry of the Interior is the Federal Office for the Protection of the Constitution, which is responsible for domestic intelligence in Germany. Its main goal is to gather information and to analyze activity that is inconsistent with the German Constitution. It is responsible for intelligence analysis of the activity of extreme nationalist groups and foreign elements in Germany, as well as counter-espionage activity. Having about 3000 employees, it also

128 The site is mostly in German: http://www.bsi-fuer-buerger.de.

operates in cyberspace, including the monitoring of fundamentalist Islamic content on the internet. In addition, it has designated teams that mobilize in the case of a cyber event linked to extremist elements or terrorists. It has also recently begun publicity campaigns in cyberspace and to oversee news sources.

The German Ministry of the Interior also includes the Federal Office of Civil Protection and Disaster Assistance, which acts as its executive arm in areas related to the protection of citizens and responding to disasters. It was created in 2004 as a result of the September 11 events in the United States and the floods in Germany in 2002. Its involvement in cyber affairs centers around critical infrastructures and includes the development of work directives and simulation exercises.

The Federal Criminal Police Agency (BKA), which is also part of the Ministry of the Interior, takes a leading role in the efforts against cybercrime. Germany has various laws relating to deterrence and the imposing of sanctions on cybercrime, including, among others, computer fraud, information theft, malicious damage, business espionage, phishing, and so forth. The BKA became involved in cyberspace already in 1998, which includes searching the internet for illegal content. It collaborates with the various authorities on a local level, carries out research on cybercrime, and deals with the underreporting of cybercrime against individuals.

Other state entities

Alongside the institutional infrastructure within the Ministry of the Interior, which, as mentioned, carries out the main cybersecurity activity in Germany, some additional bodies involved in this domain are worth naming. The National Commission for Cyber Security was created in 2011 as part of the national strategy, and it is meant to facilitate cross-domain cybersecurity activity. The ministries of the interior, defense, commerce, technology, justice, and the economy operate within this framework together with industry and academia, with the goal of formulating joint approaches to cybersecurity. The goal of the commission is to recommend changes in strategy when needed, to promote cyber legislation, encourage research, and provide assistance on cybersecurity issues, in collaboration with international organizations.

Another important player in cybersecurity in Germany is the military, whose functions include cyber protection. According to the 2011 strategy document, the Germany military is meant to protect primarily itself, but

according to the 2016 strategy, it also has a role in protecting all of the state's institutions. The more recent strategy document has clarified the army's double function, that is, to protect its own assets against cyber threats while at the same time exploiting cyberspace in order to further its goals. In this strategic document, the German Ministry of Defense also expressed its intention to provide the army with hack-back capabilities in the event that it is attacked.

Another important agency dealing with cybersecurity in Germany is the Federal Intelligence Service (BND), which was created after World War II and deals with the gathering of foreign intelligence. The BND has technological capabilities for gathering and monitoring information outside of Germany's borders, in addition to its counter-espionage activity and its activity to counter cyberattacks against Germany and its critical infrastructure. In this context, it operates a SIGINT system to assist in protecting against cyber threats, including systems to warn of such threats based on information it gathers.

In addition to the various ministries' routine activities in cybersecurity, government ministers promote specific initiatives in this domain. These initiatives can be divided into two main categories: those that strengthen German sovereignty in cyberspace and initiatives that encourage and develop education and awareness of cyber threats among the public.

The initiative to strengthen German sovereignty in cyberspace is embodied in the 2011 German cyber strategy. In particular, the state has invested in innovation and research in cyberspace, with the intention of strengthening Germany's ability to control what goes on within its territory in cyberspace. The 2016 strategy document promotes products produced in Germany in order to strengthen the German economy, which is accomplished by encouraging cyber protection among companies.

The effort to increase public awareness was also embodied in the 2011 strategy, which emphasizes the provision of incentives to create mechanisms that license products as being secure for the public's use. In 2015, the German government announced a program to promote R&D in cybersecurity and allocated about $200 million for the period up to 2020. Furthermore, the 2016 strategy document gives expression to the government's intention to promote the use of local encryption products as the desired standard. The goal in this case is to support German industry in this area and to encourage the public to use high-quality security products. The 2016 strategy also seeks to include "digital education" at all levels of the German education

system, including cooperation between the government and the various universities. In practice, this collaboration has led to the creation of three German research centers for cyber protection whose goal is to eliminate the shortage of German cybersecurity experts in industry and government. The R&D programs assist judges and law enforcement officials, among others, in order to enhance their professional skills in cyberspace.

The Ministry of Education and Research also has taken a leading role in the digitization-of-industry project. This project is mainly to do with cybersecurity in the manufacturing sector and includes an association of fourteen companies and seven R&D institutes for the development of cybersecurity solutions for industry. This program assists small and mid-sized businesses in developing and using solutions that are otherwise beyond their means.

As mentioned, Germany also relies on broad initiatives and collaborations on the international level, both within the European Union and in the international arena. There are collaborations with the UN, NATO, the G-7 countries, and the European Commission. The 2016 German strategy gives expression to this trend by emphasizing the importance of positioning Germany as a rising star in cybersecurity, both within the European Union and internationally. Essentially, already in 2011, the German Foreign Minister appointed a team for coordination and synchronization of cyber activity on the international level, indicating that it is an important component in Germany's foreign policy.

Privacy and information protection

Germany has a broad conception of privacy, with an emphasis on civil rights. As such, it plays a central role in the regulation of cyber and information security. It rests on the constitutional approach that all citizens are free to develop their own personality and aspirations and to control the use and distribution of their personal information. According to German law, personal information includes personal details on various levels and is divided into three main categories of sensitivity:

1. The internal/personal level—personal information about an individual that must remain confidential at all cost.
2. The individual level—personal data requiring a person's permission.
3. The individualistic level—the individual as a citizen in a larger collective, about whom public information can be accessed.

The German Information Security Commission was created as part of the Law for Information Protection in 1977. In 1990, the law was amended in view of the technological developments during that period. It was again amended in 2001 in order to fulfill the 1995 European Information Security Directive and to meet the uniform European standard for personal information security.

In 2005, Germany passed the Freedom of Information Law, which is concerned with the obligations of the Information Security Commission to enable access to public information. The law was amended in 2009 in order to facilitate transparency, the control of data objects, and the use of information about them for advertising purposes. The privacy legislation in Germany includes other laws that address the question of privacy in defined domains, such as media information or the activity of security organizations.

In 2016, the Information Security Commission became an independent agency that does not report to any other organization. The strengthening of its independence was the result of privacy protection legislation passed in 2014, against the background of information exposed by Edward Snowden and the scandals in the United States surrounding the right to privacy. Currently, the Information Security Commission reports only to the Parliament and the courts in Germany and its status is consistent with European information protection directives, which call for complete independence from anybody within the executive arm of the state. The commission serves public bodies as well as private ones, including communication providers and postal services. In addition, it constitutes an address for citizens who wish to submit complaints of privacy violation against private or public entities. It is also involved in individuals' access to public information and encourages government transparency. With respect to enforcement, the Information Security Commission cannot impose fines and relies on information protection agencies at the level of states within Germany (which already in the past imposed a fine of €1.1 million on a railway company).

The exposure of Edward Snowden caused a sensation in Germany and led to unprecedented public criticism of the United States by parliament members and the German cabinet. Chancellor Merkel went even further and, together with the president of Brazil, initiated a resolution in the UN Security Council in 2013 (Resolution 167/68) prohibiting illegal surveillance and gathering of information, such as that revealed in the Snowden case, and stating that such activity violates the values of a democratic state. The

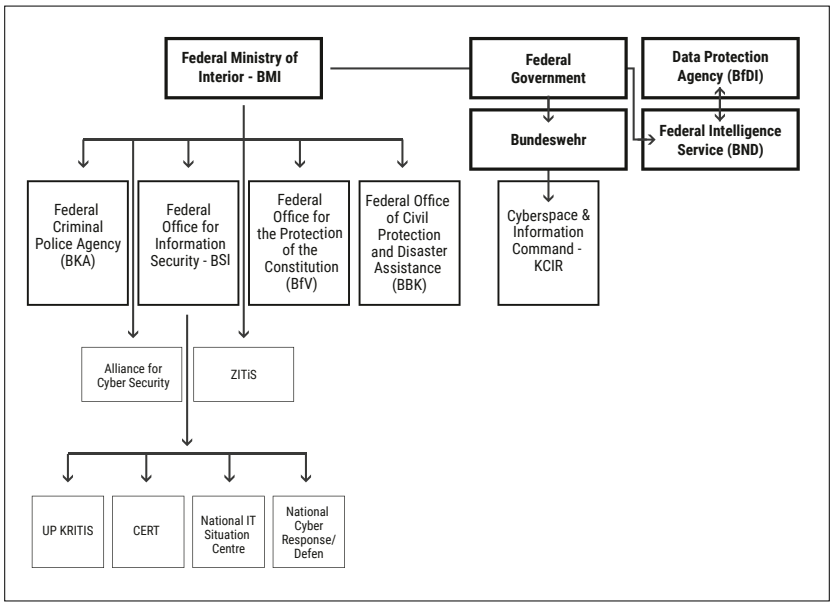

Figure 5: Agencies and institutions involved in cybersecurity in Germany

exposure of the Snowden documents also led to an audit and reform of the German security services, after it became clear that they were operating without a clear constitutional infrastructure and without suitable supervision.[129]

In 2016, after a year of negotiations with members of Parliament, the German government proposed a new constitutional foundation for the gathering of foreign intelligence. As part of the reform, approval is required before intelligence is gathered and controls are required after intelligence is collected, and the legality of the intelligence gathering can be appealed if necessary. In addition, the reform is meant to increase the transparency of intelligence collaborations between Western countries, which have been the main violators of privacy on the state level. The reform imposes restrictions on the gathering of information by German intelligence agencies and does so based on a distinction between German citizens and EU citizens and between the latter and citizens of other countries. The advantages of the reform include the creation of a clear and declared constitutional foundation

129 Thorsten Wetzlin, "Germany Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls: Policy Brief," *Stiftung Neue Verantwortung*, June 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

for the activity of German intelligence. Nonetheless, critics of the reform claim that additional procedures make it difficult to supervise intelligence activity in Germany and that they do not impose restrictions on meta-data collection. Figure 5 above presents the hierarchy and relationships between the various agencies in Germany involved in cybersecurity, as described above.

Israel

Cybersecurity governance arrangements in Israel has spanned a period of two decades, beginning in 1998 when regulation was imposed on public organizations, until the end of 2017 when the National Cyber Headquarters and the National Cyber Security Authority were consolidated into the National Cyber Directorate within the Prime Minister's Office. The Israeli approach to issuing binding cybersecurity regulations to the business sector has been a patchwork process, combining between the US and EU approaches. On the one hand, most of the private sector in Israel is not subject to any binding regulation and the state, as in the case of the United States and many countries in Europe, relies on market forces and collaboration in order to find the correct balance between suitable protection and the cost of achieving it. On the other hand, the approach to state intervention is manifested in the regulation imposed on private companies in certain sectors, such as banks, the capital market, energy, and healthcare, which are considered to be strategically important by the State of Israel, even though they are not all considered to be critical infrastructure. Over time, Israel has moved from specific regulation of entities that are critical to national security, into regulation that is largely sectoral, in which each ministry supervises according to its own needs. At a later stage, regulation came to be centralized within one body that has the powers to issue cybersecurity regulations, to institute a common methodology and language in this domain, and to create designated units within government ministries, whose employees were drawn from the staff of the National Cyber Bureau. The overall goal of the state is to adopt a single uniform approach to cybersecurity across the government.[130]

State intervention in private sector cybersecurity in Israel is manifested in two main ways: First, the infrastructures that are classified as critical, such

130 As of April 2018, designated units had been established in fifteen of the eighteen government ministries in which cybersecurity personnel are responsible for oversight and for the response to challenges specific to each ministry.

as water, electricity, and transportation, are subject to comprehensive and binding state directives issued by the General Security Services (GSS) and the National Cyber Directorate. These directives are based on the regulatory and enforcement powers of each authority or government ministry in its own jurisdiction. Thus, for example, the Ministry of Energy uses a private company to supervise the water and electricity infrastructures, which are privately owned. Other examples include the Ministry of Health, which supervises the hospitals and the Israel Securities Authority, which supervises the main financial trading systems. The second form of state intervention involves non-critical infrastructures. These are subject to government directives by way of the sectoral regulators, each of which is concerned with its own area of responsibility.

Underlying these two forms of intervention is the Privacy Protection Law, which includes elements of information security and is applied to all sectors in which there are databases of personal information that contain more than 10,000 records. In 2017, and for the first time since 1981, information security regulations based on this law were amended and they constitute an advanced constitutional infrastructure for information and privacy protection in cyberspace.

The coalescence of cyber regulation in Israel began in the late 1990s, together with the "accessible governance" initiative which led to the establishment in 1995 of Tehila, a body meant to provide government ministries and the various authorities with secure solutions for their internet connections, interministerial online activity, and online interaction with the public.[131] Nonetheless, and in spite of the attempts to provide a uniform solution to the government ministries, they continued to operate independently without any professional body to provide them with guidance.[132]

The development of cyber regulation in Israel took place over two main stages, which were done without any national strategic concept that would systematically apply to all the sectors in the economy.[133] The beginning of cybersecurity regulation in the private sector can be traced to the Law to Regulate Security in Public Bodies, which established the requirements to

131 Deborah Housen-Couriel, "Israel," NATO CCD COE Series Reports on National Organizational Models for Cyber Security, 2017.

132 Dmitry (Dima) Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy," *Washington Quarterly* 40, no. 2 (2017) 113–127.

133 Siboni and Assaf, *Guidelines for a National Strategy in Cyberspace*, p. 22.

protect information systems in organizations defined as "essential" to the state's national security. In other words, the disruption of their operations would cause damage to the state (for example, to GDP). These bodies include air transportation and water, electricity, and media infrastructures. In 2002, it was decided that the regulation of these sectors would be the responsibility of the National Authority for Information Security, which reported to the GSS. It is worth mentioning that this framework includes organizations in both the private and public sectors (the refineries, El Al, the Israel Electricity Company, Israel Railways, and so forth). In addition, it was decided that other essential organizations would be carefully chosen by a designated steering committee. Over the years, the list of essential organizations has grown. Numerous organizations that were not defined as having the potential to cause extensive damage remained without regulation and their level of security was determined primarily by economic considerations.

In 2011, Israel entered the second stage in the development of cyber regulation, in which the government changed its approach and began to consider the need to intervene in the civilian sector as well, including the transfer of powers from the intelligence agencies to the cyber organization that had just been established within the Prime Minister's Office. The decision to revise the way in which the state operates in cyberspace was not the result of a formative event or a crisis that required rethinking, but rather the insight that existing arrangements are insufficient to deal with current cyber threats.[134]

A task force that included experts from various sectors recommended the establishment of the National Cyber Headquarters within the Prime Minister's Office. Its creation was based on the desire to achieve a more successful integration within the business sector and to adopt a broad and holistic approach to cyberspace in Israel. In 2015, the government approved Decision 2444[135] to establish the National Cyber Security Authority as an independent agency within the Prime Minister's Office, whose goal is to protect civilian cyberspace. Its function is to protect critical assets, with the goal of maintaining the functional continuity of the state's critical

134 Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy."

135 For the full text of the decision, see Prime Minister's Office, "Promoting National Preparedness for Cyber Protection," http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2444.aspx [Hebrew].

infrastructures, and it would function as a regulatory body for the entire economy by means of the various regulators.[136] At the beginning of 2018, the National Cyber Security Authority was consolidated with the National Cyber Headquarters to form the National Cyber Directorate.

At the head of the pyramid (see Figure 6 below) are self-regulating bodies that are primarily sensitive security organizations, such as the GSS, the Mossad, and the IDF, which protect themselves and are not subject to external oversight. There are no binding information security regulations that obligate these sensitive organizations.

The next level consists of sensitive facilities and the defense industries, such as Israel Aircraft Industries, Rafael, and others, which are subject to the oversight of the Director of Security of the Defense Establishment (DSDE). The directives issued by the DSDE are intended to protect confidentiality and prevent harm to national security as a result of a cyber breach in these sensitive organizations.

On the next level are the essential and critical infrastructures, as defined by the steering committee. These are, as mentioned, under the comprehensive supervision of both the National Cyber Directorate (for most of the critical sectors)[137] and the GSS (for communication infrastructures). The critical infrastructures include, as mentioned, gas, energy, electricity, water, transportation, health, communication, airports, the National Insurance Institute, and so forth, in which a successful cyberattack would cause a significant disruption and damage to national security.

The Knesset Foreign Affairs and Defense Committee decided in 2016 that the National Cyber Directorate should be the entity responsible for cybersecurity in Israel and that its role is to strengthen state resilience, to meet cybersecurity needs, and to respond to cyberattacks on Israeli targets.[138] The committee recognized the fact that the creation of the National Cyber Directorate would conflict with the responsibility and powers of the GSS in this domain and therefore called for cooperation between the National Cyber Directorate—whose exclusive domain is cybersecurity and which takes into

136 National Cyber Security Authority, "Summary of the First Two Years of the National Cyber Security Authority: 2016–2017," December 31, 2017 [Hebrew].

137 The process of transferring powers from the National Cyber Security Authority to the GSS for twenty-six critical infrastructures was completed in July 2017.

138 The Foreign Affairs and Defense Committee, "Report on Examining the Division of Cyber Security Responsibilities and Powers in Israel," August 2016 [Hebrew].

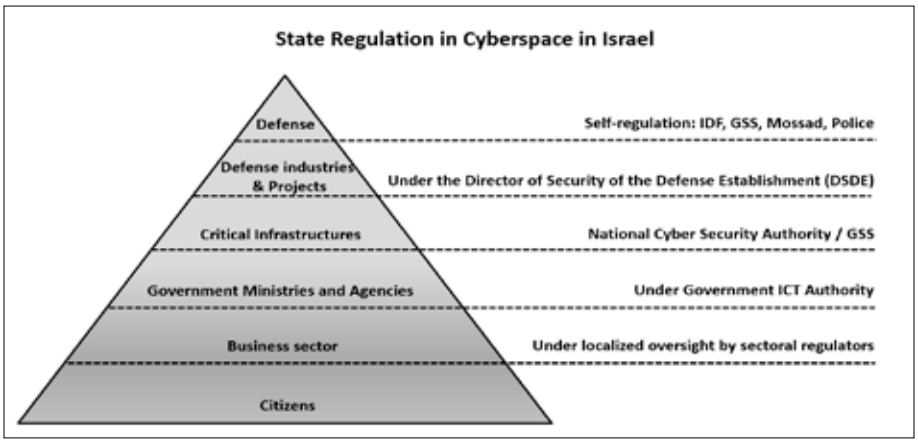

Figure 6: Areas of responsibility in the supervision of cybersecurity in Israel, 2018

account civilian-state considerations—with GSS that has the expertise in the security and intelligence elements in this domain. According to the committee, the National Cyber Directorate should not become another intelligence organization but rather should rely on the intelligence-gathering capabilities of existing intelligence organizations. The importance in formalizing the division of responsibility between the various organizations active in cyberspace is also evident in the 2016 Annual Report of the State Comptroller, which comments on the gap between the government decision to establish the National Cyber Directorate and its implementation.

On the next level are the government ministries under the oversight of the Government ICT Authority, whose function is to oversee cybersecurity in each ministry, including their independent agencies. It is essentially a reincarnation of Tehila, the original organization which, as mentioned, was created in 1997 as part of the "accessible governance" program of the government ministries.

On the next level of the pyramid is the business sector, most of which is not subject to regulation, apart from the localized supervision of the banks, the capital market, securities, energy facilities, and healthcare institutions, which have sectoral regulators. The majority of the business-civilian sector is not subject to state oversight, does not optimally share information and focuses only on minimizing damage to customers, while reporting cyber events to them according to their discretion.

It is worth describing the activity of the sectoral regulators, which extends beyond the responsibility of the government ministries and is, as mentioned,

trickling down, at least in part, to the business sector. Two such examples are the Bank of Israel and the Capital Market Branch within the Ministry of Finance. In March 2015, the Bank of Israel issued Directive 361—"Management of Cyber Security"—to the banks.[139] This directive includes instructions for the creation of a cyber risk management plan in each bank, in which the Bank of Israel delegates the decision on how to do so with the banks. An important component of this directive is the appointment of a designated information security officer who is accountable to the Bank of Israel. The supervisor of banks stated in this directive that the technological innovations and the connectivity of information systems creates fertile ground for major cyber risks to the banks. These risks include disrupting activity, preventing service to the banks' customers, exposing private information, erasing and disrupting data, losing public confidence, damaging the bank's reputation, and reducing ability to manage risks and customers. The directive describes the roles of the various position holders and the way in which they are to contribute to the bank's cybersecurity. The bank's board of directors is responsible for setting strategy and approving the framework for cyber risk management, as well as deciding on the method of supervision and reporting of major cyber events. The role of senior executives is to formulate cybersecurity policy for the bank and to implement it, to allocate the necessary resources, and to periodically examine what is being done in this domain. In addition, a designated "cybersecurity manager" is to be appointed whose function is to oversee the bank's exposure to cyber risk, to formulate methodology, and to coordinate the bank's cybersecurity efforts, including simulations to test cyber preparedness, in cooperation with all the relevant departments in the organization.

The Bank of Israel's directive requires that each bank formulate a multi-year work plan to deal with cyber threats that will be based on its strategy and analysis of exposure to cyber threats and will prioritize installing controls to reduce the bank's cyber risk. Each bank will carry out an assessment of cyber risk at least on an annual basis and will include a mapping of the business processes and the use of indexes in order to quantify the exposure to risks.

---

139 Bank of Israel, Supervisor of Banks, "Directive 361 – Cyber Security Management," March 2015, https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf [Hebrew].

This process will be carried out on a comparative basis, which will facilitate prioritization and will be documented and approved by senior management.

The Bank of Israel directive also outlines how to create an effective controls system to reduce cyber risk, based on the use of technologies, processes, procedures, and professional staff across the entire bank. To accomplish this, the bank's supply chain, including suppliers, associated companies, customers, suppliers of communication services and computer infrastructure, outsourcing, service providers, and foreign entities, is to be assessed. Each entity identified as relevant will undergo a "soundness and monitoring check" in order to ensure that it is not generating cyber risk for the bank. In addition, the banks will carry out independent investigations of threats, which will include the sharing of information and the analysis of scenarios that will help fortify their cybersecurity and their operating environment against a potential attack. This will occur in parallel to an assessment of the bank's security based on its internal and external environment.

The cyber controls in each bank are meant to reinforce the bank's ability to appropriately respond to events and to deflect and delay potential attackers; to withstand a cyberattack and to restore the bank's business activity; to investigate what has occurred; to minimize the exposure to threats by hardening systems and limiting authorizations; to implement multi-layered security at various points in the organization; and to manage relevant cyber processes for monitoring identities, assets, and the supply chain.

According to the directive, the banks are to define the responsibilities of their staff, and their practices of hiring, recruitment, and absorption of manpower in order to take into account cyber issues. The monitoring and control systems that are to be created should be manned continuously and should include identification of anomalies and integration with other systems. The reporting of cyber events will be internal, without exposure to the public. The evaluation of cybersecurity monitoring will be carried out by means of existing evaluation mechanisms, surveys of vulnerabilities, and controlled breach testing. The bank's cyber risk reports will include a status report and will be supported by risk measures and a description of any significant damage and relevant external events that are liable to affect the bank in cyberspace.

Another example of agency guidelines over the private sector is the circular on cyber risk management issued by the Capital Market Branch within the Ministry of Finance in August 2016. As in the case of banking

supervision, the Capital Market Branch reached the conclusion that the growing technological threats are liable to disrupt the operations of the entities it supervises. Therefore, it decided to establish guidelines for the protection and maintenance of information confidentiality, integrity, and access, including the security of information systems and business processes.[140] The expectation is that every institutional body in the Israeli capital market will adopt the standards in the Capital Market Branch circular. The circular also describes the role of the board of directors, the CEO, the steering committee to be established, and the designated cybersecurity manager in the organizations. In addition to the detailed risk management process, the circular describes in great detail the cyber protection measures that every supervised organization is to adopt. This includes gathering of intelligence, monitoring and control of information, preparedness for events, execution of surveys, breach testing, the security of communication and operating systems (including acquisition and development of new systems), management of users and authorizations, outsourcing, physical security, hiring procedures, and security of communication channels with internal and external entities.

Operators of electricity and energy infrastructures are another type of organization in the private sector that are subject to localized regulation. The Ministry of Energy and National Infrastructures is responsible for supervision of cybersecurity among private infrastructure operators. More specifically, the Director of Security for the Private Sector within the Ministry's Security Branch is responsible for functional continuity—and therefore also information security and physical security—of the various infrastructures. The supervision involves the following process: Each private operator in the energy sector that produces more than a certain quantity of electricity must obtain a license from the Ministry of Energy. Obtaining the license is conditional upon fulfilling the ministry's regulations, which generally takes several years. The ministry's supervision of private operators is outsourced. The objective is to ensure that an appropriate risk survey is carried out and that information security advisors are appointed who will ensure the functional continuity of every industrial enterprise.

The operating infrastructures of each operator are under the supervision of the Ministry of Energy while the hookups to the Israel Electricity Company

140 Dorit Salinger, Ministry of Finance – Capital Market, Insurance and Saving Branch, August 2016.

are supervised—as a critical state infrastructure—by the GSS or the National Cyber Directorate. The costs borne by each private operator are significant, although the supervising entity works to reduce the fees charged by security providers and does not itself charge any fee for its advice, since it is being given at the initiative of the state. In this way, the state incentivizes private electricity producers to protect themselves appropriately. The state also established the Center for Cyber Event Management for the private energy sector and has successfully encouraged competing companies to share information on cyber events.

In addition to the selective supervision of the various sectors, the State of Israel has issued *six* major directives and regulatory initiatives that apply to the business-civilian sector. The goal of the *first* directive is to strengthen the existing supervision carried out by the Branch for Supervision of Defense Exports in the Ministry of Defense and to increase the number of products under state supervision,[141] in order to control the arms race in cyberspace and maintain Israel's relative advantage in this domain.

Following a prolonged process of consultation with the various cyber industries, the state decided to refrain from invasive supervision and instead to continue adhering to international supervisory standards. The reason for this was the opposition of industry, which feared that it would not be able to compete with rival companies in countries not subject to regulation.[142] The desire to preserve Israel's status as a leading cyber exporter relative to the size of its population[143] has resulted in, among other things, the maintenance of the supervisory status quo. It indicates the mutual understanding and cooperation between the various industries and the Ministry of Defense.[144] The Ministry of Defense took the industry's needs into account on the

141 The extension primarily included products for penetration, breach analysis, and the detection of weaknesses in hardware/software.

142 For further details, see the guest writer column, "Behind the Cancelation of the New Cyber Order," *Geek Times* April 2016, http://www.geektime.co.il/the-decline-of-the-israli-cyber-law/ [Hebrew].

143 On the state's goal of making Beersheba the regional cyber capital, see Warwick Ashford, "Israel's Cyber Security Frontier," *ComputerWeekly*, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier.

144 Matthew Waxman and David Hindin, "How Does Israel Regulate Encryption?" November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

question of cyber supervision; nonetheless, it still maintains a presence in this domain and is part of the decision-making process in the case of a cyber product with clearly offensive capabilities.

The goal of the *second* initiative is to nurture human capital and to create standards for the cybersecurity professions. In December 2015, the National Cyber Headquarters published a document that attempts to regulate cybersecurity professions in Israel. The document is an official recommendation that is similar in character to regulation, in which the state specifies the training needed to work in cybersecurity at the various levels.[145] Essentially, this is a unique directive that is meant to raise the level of professionalism by establishing various training trajectories that are to be developed specifically to meet this regulation; however, it is also likely to marginalize the importance of the autodidactic process through which most of the cyber experts accumulate their knowledge.[146]

There are countries that invest in formulating a single uniform directive that specifies the knowledge that cyber professionals must acquire. Similarly, there is a visible trend in various countries to recognize existing professional and academic certificates that testify to cyber abilities and skills. In Britain, for example, there is an attempt to provide public certification to various professions in cyberspace. Furthermore, the British government will only work with cybersecurity providers that have recognized certification.

The National Cyber Directorate in Israel chose a system of personal cyber certification that requires testing every three years and to this end issued a recommendation specifying the knowledge and skills needed in this profession, based on the adoption of an accepted state standard. In addition, the state has differentiated among specific professions and positions in the cybersecurity domain, including between a "professional" and a "position holder." The former is certified in a particular field who requires specialized skills, while the latter holds an appointed position, which combines areas of specialization that are recognized as a profession. In the first stage, Israel

145 The National Cyber Headquarters, *Policy of Regulation of Cyber Security Professions in the State of Israel*, 2015, http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf [Hebrew].

146 See National Research Council, *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making* (Washington, DC, The National Academic Press, 2013), http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurityworkforce-criteria-for-decision-making.

chose to regulate the definition of a "professional" but not that of a "position holder."[147] "Professionals" were divided into five main categories:

1. Cybersecurity implementer—an individual who implements cybersecurity in the organization;
2. Certified for breach testing; ability to identify weaknesses in the systems;
3. Certified for cyber investigation; ability to investigate cyber events;
4. Certified in cyber methodologies;
5. Certified in cyber technologies.

Each of these professions has two levels of certification—basic and advanced. In order to implement the regulation, the National Cyber Directorate decided to create a designated unit that would oversee all aspects of the regulation, including validation of professions and fields of study, preparation of exams to test for the required knowledge, the definition of conditions and criteria for partial exemptions from the exams, the processes to renew a certificate, levels of certification for each profession, criteria for professional abilities, and the promotion of relevant primary/secondary legislation. The goal of the regulation is to advance the public interest and protect it from poorly skilled professionals who are likely to cause damage as well as to ensure that professionals—whose activity will likely have implications that go beyond the employers themselves—have a sufficient level of professional skills.

The *third* initiative is the amendment of information security regulations for the protection of database privacy, as approved in March 2017 by the minister of justice. The amendment includes the expansion of powers of the director of the Authority for Law and Technology and also a long list of information security regulations that apply to database operators. The new regulations include an obligation to report to the Authority for Law and Technology (and sometimes also to the individuals themselves) in the event of a database breach; a reduction in the amount of personal information held by others; a requirement to appoint an individual responsible for information security; and the training of an organization's employees in the area of information security and privacy.

The new regulations also deal with outsourcing, encryption, monitoring, breach testing, documentation, and backup of information. The regulations

147 The Prime Minister's Office, National Cyber Headquarters, *Policy of Regulation of Cyber Security Professions*.

are modular and include requirements whose stringency varies with the level of database sensitivity. To the extent that the information is more sensitive and exposed to more people, the regulations are more stringent. The regulations determine a database's sensitivity ranking.[148] Databases defined as having "regular" sensitivity ranking (up to 100,000 records and ten managers) are required to maintain a basic level of security. Databases of up to 100,000 records and to which about 100 people have access are defined as "intermediate" and are required to have a higher level of security. Databases with more than 100,000 records and to which more than 100 people have access require a "high" level of security. The Bank of Israel and the Capital Market Branch within the Ministry of Finance have requested that some of these regulations not apply to their sectors in order to avoid duplication with the directives they themselves have issued in the past.

The new regulations initiated by the minister of justice have two motivations: First, the European Union threatened to withdraw Israel's status as a "country that protects privacy" according to EU standards. This would have had far-reaching consequences on Israel's economy, since Israeli companies would not have been able to gather and analyze information on EU citizens. Second, small and mid-sized companies seek a clear standard for information security. The bar set by the new regulations is viewed as being the lowest possible and they went into effect on May 8, 2018.[149]

The *fourth* initiative is the National Cyber Bureau's Cyber Security Doctrine for an Organization,[150] which was published by the National Cyber Directorate in April 2017. The document applies to organizations in the business-civilian sector and provides tools for the management and improvement of cybersecurity in organizations, including the creation of formalized work plans. The document views organizations in the economy as important components in the effort to increase Israel's national resilience and divides

148 Omer Tene, "Israel Enacts Landmark Data Security Notification Regulations," May 2017, https://iapp.org/news/a/israel-enacts-landmark-data-security-notification-regulations.

149 Ilan Shahar, "After a Delay of Seven Years: Small Companies will also be Obligated by the Information Security Regulations," *Calcalist*, March 13, 2017 [Hebrew].

150 Prime Minister's Office, National Cyber Directorate, *Cyber Security Doctrine for an Organization – Version 1.0*, April 2018, https://www.gov.il/BlobFolder/policy/cyber_security_ methodology_for_organizations/he/Cyber1.0_418_A4.pdf [Hebrew].

them into two categories: organizations whose potential damage as the result of a cyber event is insignificant and organizations with a potential to cause major damage as the result of a cyber event.[151] The document is not binding and is essentially a work plan for reducing cyber risk for organizations that are not directly regulated by the National Cyber Directorate. The document focuses on multi-layered protection of the organizations and relates to the "people, technology, and processes" needed to raise organizational resilience. It is based on the directives of the US National Institute of Standards and Technology (NIST), which include protection of organizations against attack, in addition to the strengthening of detection capabilities and recovery abilities.

The National Cyber Directorate has adopted this document and has adapted it to the characteristics of the Israeli economy according to five main stages: identification of the potential damage; protection against risk; identification of an event; response; and recovery. Every organization undergoes a stage of asset mapping and a listing of security needs, based on its primary controls: encryption, information protection, network security, cloud computing, and so forth. Organizations with a high potential for damage must evaluate the level of protection needed for each mapped asset and must also assign a probability for realizing the risk, according to the responses to questions related to the organization's information security procedures.

The National Cyber Directorate was also actively involved in the *fifth* initiative as well, which include the formulation of the first Israeli cybersecurity strategy.[152] The strategy describes the operational approach of the National Cyber Directorate, including the resilience of the economy, systemic resilience, and national defense. The strategy's innovation is that it assigns a prominent role to the development and encouragement of technological innovation in the business sector, universities, and pre-academic education and treats innovation as a power multiplier in cybersecurity efforts. The efforts to create resilience in the economy relate directly to the business-civilian sector and are manifested in direct and indirect supervision of organizations in the economy, usually by means of existing sectoral regulators, as well as the development of expertise in the field. The strategy is composed of early

151 The criteria for differentiating between the two categories is whether the cost of dealing with a cyber event exceeds NIS 100,000. If it does, then the potential damage from a cyber event is considered significant.

152 Prime Minister's Office, National Cyber Directorate, *Israel's Cyber Security Strategy*, 2017 [Hebrew].

protection (prevention), which includes the evaluation of risk management processes; planning of the organizations' architectures; and procedures for system use, including the risk of human error and the way in which technological solutions can be implemented. Another component of the strategy is real-time defense by means of state intervention and assistance in the containment of attacks. The state's professionalism in this area, which includes the assistance of technological teams and experience in working with critical sectors, is relevant to the economy as a whole and can provide valuable assistance in dealing with localized attacks.

The *sixth* and last initiative is the draft of the "Cyber Law," which is being discussed by decision makers in the National Cyber Directorate and other circles. The proposed law anchors the powers of the new National Cyber Directorate and gives it authority in all aspects of cybersecurity in the economy. The law establishes a legal framework to deal with cyber events in real time and facilitates the granting of incentives to the economy in this domain, including an exemption from responsibility for internal organizational cybersecurity activity and permission from the director of the Antitrust Authority for the sharing of cyber information among competitors in the economy. The law also establishes a single sovereign for cybersecurity in Israel—the National Cyber Directorate—and attempts to establish clear boundaries between the various regulatory bodies in cyberspace. The decision as to who will be the main regulator directly responsible for cybersecurity in every instance requires a precise mapping of the market and a comprehensive evaluation. Thus, for example, in the case of hospitals many regulators are involved, and there are cyber elements even within the hospitals' environmental protection efforts and in its day-to-day activities. Therefore, one of the principles of this law is to organize the domain and to resolve authority conflicts over regulation that affect the entire economy.

The main issue that the Cyber Law is meant to address is the question of who in the economy will be subject to binding regulation. To this end, the law divides the economy into three categories: of about 600,000 organizations in the economy, about one thousand will be defined as Level A, or critical organizations that are obligated by the state to protect themselves; the rest will be divided into Level B organizations, to which will apply the currently existing regulations and additional supervision from above, and Level C organizations whose potential to cause damage does not justify binding regulation and who will operate on the basis of incentives only.

The law proposes that the National Cyber Directorate be the exclusive and principal regulator of high-risk organizations, while in the case of the other organizations, the existing decentralization on the basis of international standards will be maintained.

In order to meet the challenge of regulation in cyberspace in a comprehensive manner, the National Cyber Directorate assigns staff members to serve in each of the government ministries, in order to provide support and professional solutions to cyber-related challenges that the ministries encounter. Thus, the National Cyber Directorate enables the sectoral regulator to focus on cybersecurity within their own area of responsibility, while maintaining a presence and oversight over cyber activity in each ministry. The benefits of the new law will include mitigating potential harm to organizations and the public interest on the one hand, and allowing for the growth of the Israeli cyber market, with increased confidence in the digital domain on the other.

Cybersecurity regulation in an emergency, that is, during a cyber event in real time, and its regulation on a routine basis—dealing with risks before they are realized—need to be differentiated. Israel has adopted an advanced approach to cybersecurity during an emergency incidents; it has created spheres of cooperation between organizations with competing interests, and it is working to achieve common goals also in the international arena.[153] In contrast, the directives issued to the economy on how to operate on a day-to-day basis are more complicated and their structuring has led to numerous power struggles between regulators and private stakeholders, including those that are meant to protect the public interest.

In conclusion, a broad view of the State of Israel's cyber strategy indicates that in spite of the innovation and uniqueness of the state's integration within the effort to protect the economy, the state still pays insufficient attention to the business-civilian sector. Although the Cyber Law goes a long way toward the goal of closing this gap, the economy as a whole lacks a systematic solution that will encompass all the sectors and will deal with every existing

153 For example, the creation of the national CERT in Beersheba, which has been in operation since October 2016, or the creation of the CERT center for the financial domain, which is meant to serve as an institutional mechanism for cooperation between the relevant players in order to prevent cyber events in the financial system. A designated center for the management of events has also been created in the energy sector, and it is facilitating the accumulation of sectoral expertise in this domain.

and future project that has the potential to cause damage to national security as the result of a cyberattack. Despite the precise mapping of the market, as described above, major organizations not subject to supervision, despite their substantial impact on Israel's national resilience in cyberspace. Companies like Matrix and Malam, for example, provide digital services to many companies in the economy, but there is no regulator that verifies the quality of their work or the security of their practices. Although the state regulation of the business-civilian sector in cyberspace has developed considerably during the last two years, an overall approach to the supervision of the private sector—according to which every organization is supervised independently by its sectoral regulator and according to the size of its databases—is lacking, as described above.

Other Regulatory Issues

Two other regulatory areas of interest are the Internet of Things and cyber insurance. Both these subjects have the potential to influence the structure of the regulatory regime in cyberspace, although they are still being discussed by decision makers, who have yet to decide on how to regulate them. The survey that follows describes the existing gaps on these two fronts and the issues being discussed. The proposed regulatory model in the following chapters considers some of the recent developments in each of these areas.

The Internet of Things

The 2010s has been the era of mass connection to the internet of devices and smart sensors. In the past, commercial computers were initially hooked up to the internet, followed by personal computers and finally cellular phones. Today, numerous types of devices are connected, with the purpose of sharing information and creating communication channels that will improve the devices' performance. Examples are remotely controlled cameras, pieces of clothing worn by athletes that measure pulse and signs of stress, smart cars, thermostats, refrigerators, dryers, and light bulbs. Simple devices that previously had only a localized effect have been transformed into smart devices, becoming thus more efficient and money-saving for the consumer. These devices, however, have also become vulnerable to attacks on the internet and are liable to become a tool of the attackers.

Recently, the US secretary of homeland security stated that "securing the Internet of Things has become a matter of homeland security."[154] The state of Illinois, which is trying to become the first smart state in the United States, has invested in online services and has been exploiting the advantages of the Internet of Things in order to achieve greater efficiency. According to Gartner, a technological research center, the number of smart devices is expected to reach 20 billion before 2020.[155] The market for smart devices has recently been estimated by the Cisco company at about $19 trillion. Siemens, a company that specializes in smart devices, calls this phenomenon the "fourth industrial revolution," after the invention of steam, electricity, and the computer. According to the Department of Homeland Security, the expansion of the Internet of Things means that the window of opportunity to secure it is rapidly closing.

The term "Internet of Things" is ambiguously defined and can be interpreted in many ways. In its broadest sense, the concept relates to the connectivity of physical objects to the internet in order to identify other objects and manage data and information structures without human involvement. The Federal Trade Commission published its definition of the Internet of Things in 2015 as "devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information from one to the other by way of the Internet."[156]

Despite the obvious advantages implicit in connectivity and in data structures for physical objects, there are also risks to the objects themselves, as well to the network on which they operate and the homes and structures in their vicinity. A number of breaches of smart devices have occurred, revealing their potential to cause damage. The McAfee security company

154 Eliza Chapman and Tom Uren, "Issues Paper: The Internet of Insecure Things," *ASPI International Cyber Policy Center*, 2018, https://www.aspi.org.au/report/InternetOfInsecureThings.

155 "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," *Gartner*, February 7, 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

156 FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commissionstaff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

demonstrated in 2012 how it could cause an Android telephone to heat up to the point of self-destruction. In that same year, Chrysler automobile systems was successfully breached. In 2014, the Proofpoint security company identified a cyberattack carried out using smart devices, such as televisions, speakers, refrigerators and communication routers, which sent infected emails to expanding circles of targets. In 2015 and 2016, at the largest conference of hackers in the world (called DefCon), 113 weaknesses were revealed in smart devices of various types, including doors, thermostats, refrigerators, wheel chairs, and solar panels. In October 2016, researchers discovered a way to attack smart light bulbs and to create a chain reaction from one to the next.

The most famous attack so far was carried out in October 2016, when a vulnerability in smart security cameras was exploited in order to turn them into a botnet.[157] It was caused by weak passwords used by the manufacturer and as a result, damage was caused to the Dyn company, which provides domain name system (DNS) services on the internet. As a result of the attack, eighty-five sites became unavailable for a day, including some of the most popular ones, such as Netflix, Twitter, PayPal, and Sony. The owners of the smart devices did not know that their products were involved in an attack, since the devices continued to operate normally.

These events reinforced the understanding that smart devices lack security on the most basic level. The vulnerable products are not only devices for personal use but also include industrial controls used in transportation, electricity, gas, and food production. This situation is liable to create numerous risks to both national security and organizations that integrate smart devices within their service. Medical devices also are life threatening as a result of the insufficient cyber protection of the connectivity they facilitate.

The US federal government recognizes the importance of smart devices to the economy and to society and is trying to promote their security, although without much success to date. At the beginning of 2015, the US Senate published a declaration supporting the formulation of a national policy for smart devices. The Senate viewed the continued development of such devices as playing a significant role in promoting economic innovation,

157 See the official blog of the Dyn company, which analyzes the attack on its systems: Scott Hilton "Dyn Analysis Summary of Friday October 21 Attack," October 26, 2016, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

but it also recognized the need to prevent fraud and malicious use of these devices.[158] The Senate's declaration marked the beginning of the effort by the US Congress to better understand the challenges in this domain, which includes the convening of expert committees and promotion of relevant legislation; nonetheless, the parliamentary activity in this domain has been insignificant.

The executive arm of the US government has also tried to promote the use of smart devices, while maintaining their security. Thus, the National Telecommunications and Information Administration (NTIA) published a position paper at the beginning of 2017, identifying the need for government agencies to encourage the installation of security updates.[159] The American National Standards Institute (ANSI), which is highly involved in cybersecurity in the United States, has also organized conferences and brainstorming groups on the subject. Overall, the US administration has made a major financial investment in the Internet of Things: $250 million in research on smart cities, in addition to cities that receive financial assistance also from sectoral agencies, such as transportation and the environment, as well as from the National Science Fund. At the same time, the progress of this effort is being delayed by the inaction of the Congress, which has yet to adopt any major legislation or policy on the subject due to its fear of harming industry, growth, or innovation, thus blocking the introduction of binding regulation.

The Federal Trade Commission (FTC), as the main regulator dealing with information protection, is trying to take action in this domain by means of, among other methods, filing suits in the courts against organizations that supply smart devices without meeting basic security requirements. In 2014, the FTC filed a suit against the TRENDnet company, which sells video cameras but does not secure them sufficiently—despite its obligation to do so—thus enabling anyone with the internet address of the camera to watch and listen to what the camera films. As a result of the suit, the company arrived at an understanding with the FTC to formulate a plan to raise the security level of its products and to inform consumers of their possible vulnerabilities.

158 US Senate, "A Resolution Expressing the Sense of the Senate about a Strategy for the Internet of Things to Promote Economic Growth and Consumer Empowerment," Res, 110m 114th Congress, March 2015.

159 The Department of Commerce Internet Policy Task Force and Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017.

In another instance, the FTC brought a suit against the ASUSTek company, which produces routers for home networks. The company supplied routers with major security weaknesses, which in early 2014 gave attackers unauthorized access to about 13,000 computers. In addition, the company did not sufficiently encourage their customers to install security updates on their routers and left them exposed to breaches. As a result of the lawsuit, the ASUSTek company paid fines, upgraded its security programs, and notified users on how to protect themselves.

The FTC filed another lawsuit in January 2017 against the D-Link company. This suit was somewhat of an exception since it did not follow a clear breach or damage but rather was the result of the FTC's diagnosis that the company, which mainly produces smart cameras and routers, had not sufficiently protected their products. The company was accused of not testing software sufficiently, not providing enough security for control of access and product definitions, and not using encryption in sensitive segments. In addition, in this case, the problems were exposed despite the company's assurances that its products were secured using the most up-to-date methods.

Another government agency that has become a player in the efforts to protect smart devices is the Federal Communications Commission (FCC). Although it does not have a clear mandate to regulate the security of smart products, it exploits its power to approve the use of a frequency range by such products in order to intervene and raise their level of security. The leader of the cybersecurity lobby in the US Congress has even recommended in this context to reconsider the approval process of communication devices by the FCC with the goal of adapting it for the purpose of supervising the security of smart devices. This process was halted after the 2016 presidential elections and the shift of power, and as a result the FCC does not currently have an up-to-date solution for smart devices.

The vacuum created by the lack of any significant state intervention has been filled by private third-party organizations that function as regulators. The main organization in the domain of smart devices in the United States is Underwriters Laboratories (UL), which works to promote "safe science" and in April 2016 created a designated program for the testing and approval of security in smart devices. The organization claims that industry in this domain needs basic indexes and processes that will enable the evaluation and measurement of security in smart devices. The standards proposed by UL were developed in collaboration with government agencies, such as

the Department of Homeland Security, the National Security Agency and the FCC, together with industry and academia. UL also declared that it is working on all aspects of smart devices on the basis of ANSI standards. The rationale behind UL's program is to provide producers and investors with security and confidence in the cyber protection of their smart devices.

There has been widespread criticism in the United States of these regulatory efforts and many have expressed doubt of the technological expertise of UL. Furthermore, the fact that a private entity is meant to guide industry in how to implement certain standards raises conflict of interest questions. Another concern relates to the lack of monitoring and control after the security of a smart device has been approved, even though cybersecurity—being dynamic—requires feedback and testing that is up to date with the latest developments in the field.

In conclusion, ensuring the security of smart devices is a complex task. The technology is continually changing, and usually includes critical components that originate from all parts of the world, which increase the probability of threats. The development of appropriate standards is an important step but only the first one. Thought should be given to the ways in which the standards should be implemented and how the market should be incentivized to adopt them. Further details are presented as part of the proposed regulatory model described in the next chapters.

Cyber insurance

The growing risks in the cyber world have intensified the need for the state to adopt various risk management strategies. Israel has taken the route of risk prevention by means of binding cybersecurity directives issued to sectors that are defined as having critical infrastructures or to supervised private sectors. Other countries are working to facilitate risk mitigation by means of national and sectoral CERT centers. What is lacking is a strategy for risk spreading, a process by which an insurance mechanism and premium payments distribute risks of a particular actor over all other policy holders. The free market has not managed so far to develop efficient risk-spreading mechanisms in cyberspace and the two main challenges are the achievement of standardization and a common language for the quantification and coverage of first- and third-party cyber damages, and the creation of an actuarial database for the calculation of premiums.

Despite these difficulties, the cyber insurance market in the United States has been in existence since 2005, and in 2014 it had a turnover of $2.5 billion. Nonetheless, the state has remained on the sidelines in this market. The cyber insurance market focuses on third-party damage only, and there is plenty of room to optimize its activity due to three main factors: Each policy currently requires a great deal of resources and is determined separately for each insured organization; the insurance policies do not raise the insured organization's level of resilience; and the policies leave ample room for differences in interpretation in the event of a successful attack.

The dynamic environment and the high costs in the case of a successful breach have led many companies to show interest in cyber insurance policies. These companies want to insure themselves against unexpected costs, whether due to the infringement of their customers' privacy or as a result of cyber damage to their operations. The companies also wish to protect themselves from damage to their functional continuity, loss of business information, loss of revenue, and damage to the stability of the organizational network. As mentioned, the spectrum of threats and the potential damage, together with the variation across companies, have led to the purchase of designated insurance policies that are tailored specifically to each company. The Marsh and AIG insurance companies report an uptrend in the purchase of such policies.

The cyber insurance market is flooded from the demand side, but there is no appropriate regulatory supervision and small and mid-sized businesses find it difficult to bear the cost of these expensive policies. In 2015, the Department of Financial Services of the State of New York issued a report on the security situation in the financial sector and announced a search for ways to develop the insurance market in this sector.[160] In 2016, a representative from South Dakota testified before the US Congress about ways in which the state is trying to promote this market.[161]

Several cases discussed in the US courts have highlighted the need for regulatory intervention in the structuring of the cyber insurance market. In

160 For the official report of the Department of Financial Services of the State of New York, see https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_insurance_report_022015.pdf.

161 See the testimony of Adam W. Hamm to the US Congress, March 2016, http://www.naic.org/documents/government_relations_160322_testimony_hamm_cyber_insurancer_risk_managment.pdf.

June 2016, judges ruled in favor of the Federal Insurance Company, which had sold a policy to protect against cyber damage to the P.F. Chang company. The Federal Insurance Company did not cover the damage caused by a successful breach of Chang's systems, because the breach had occurred as a result of its relationship with a third-party vendor, an issue that was not specifically covered by the policy. The legal interpretation of this case, as mentioned, highlighted the importance of creating regulatory standards and directives in the cyber insurance market.

The development of the cyber insurance market is dependent, first and foremost, on the state's manner of intervention, which raises the issue of exactly how the state should intervene—through regulation that mandates the acquisition of a policy or by requiring that any company that wishes to work with the state must acquire a policy. Another issue in this context is encouraging transparency and the obligation to report theft of information and breaches of commercial companies, as an incentive to acquire an insurance policy (as in the United States at the state level). In this context, the question arises of what the requirement of reporting cyber events should include in order to create an effective incentive for purchasing insurance policies: What should be reported (for example, major cyber events with damage beyond a certain minimum)? To whom should cyber events be reported? How soon should they be reported? Who can provide advice before reporting? What compensation should there be in order to encourage the early purchase of policies and protection? What happens in the case of encrypted information? Are all organizations to be treated equally? What levels of risk should be determined for cyber protection?

Another function of the state, as already mentioned, is to assist in the creation of actuarial information to be used by insurance companies for the purpose of determining premiums. In the United States, for example, the Department of Homeland Security monitors all suits filed by insurance companies in the context of cyber damage and encourages businesses—by means of a law passed at the end of 2015—to share information on existing threats to their networks. Another traditional means of intervention by the state is the limiting of the insurance companies' liability in the case of a "cyber disaster" in order to prevent bankruptcies, which is accomplished by making financing available in emergency situations.

Another question that arises is whether to encourage policies for first-party damage (the networks and the companies themselves) and/or third-party

damage (the customers whose personal information was stolen). Furthermore, consideration should be given to the design of an effective insurance policy and the guidelines for such a policy—whether by requiring a specific type of product protection or by adopting guidelines set by the American National Standards Institute—and whether the actual configuration is important.[162] Other questions facing the state include: Which sectors will make most extensive use of the insurance market—retailing, finance, marketing, consulting companies, or manufacturers? How acquainted should the insurance agent be with the applicant seeking a policy? Should a policy meet the specific needs and work procedures of each organization or can a general model be developed and then adapted to the different organizations, according to declining marginal cost? In this context, account should be taken of issues such as the preparedness of the organization for cyber events, protection products that it uses, the employees' level of awareness, the frequency of security updates, and so forth.

The cyber insurance market in Israel is directed at small and mid-sized businesses. In contrast, large businesses go to the global market for insurance. For example, the Menorah company sold about one thousand first-party and third-party cyber insurance policies during the period 2014–2016. Migdal offers three types of coverage: cyber insurance as part of the third-party segment of its business insurance policies; cyber insurance as part of professional liability insurance; and stand-alone cyber insurance for companies that are looking for a specific solution. The insurance companies that sell policies to customers manage the entire event, rather than just compensating for damage. At the same time, customers have a low level of awareness of their risk level. An attack on cyber infrastructure that is not a service provider in the United States—that is, one that does not have a very large number of customers in the digital domain—is considered to be a low-to-mid-sized cyber risk.

Overall Insights from the Literature Review

A review of the literature reveals similarities and differences in cyber regulation throughout the world. Various countries became involved in cyberspace

162 The configuration has significance in determining the type of insurance policy. For example, the Linux operating system, which is viewed as more secure than the more common Windows operating system, can also be defined as not secure.

at different points in time and while some have concentrated on critical infrastructures and national security, others have focused on protection against cybercrime. All the countries have invested major resources in cybersecurity in order to create a state and institutional supervisory capability, as well as the ability to influence the cyber domain in the economy and in the various threatened domains. In most of the countries (except for the United States and Germany), a central body in the form of an agency or institution deals with cyber threats, which creates the standards for cyber protection and facilitates an organized decision-making process in this domain, despite the complexity and multidimensionality of the cyber problem.

At the same time, and despite the investment of resources and the creation of state capability in this domain, the inclusion of the business-civilian sector in the cybersecurity effort is lacking worldwide. Not one country systematically regulates the business-civilian sector and relates to the national security threats from cyberattacks on that sector. The European Union has recently decided that the legislation mandating cyber protection will also apply to providers of digital services, such as search engines and cloud services, which have not traditionally been included in the state regulatory realm. Nonetheless, not even the European Union provides a comprehensive solution to cyber threats. In the United States, most of the business-civilian sector is not subject to binding regulation, apart from a few exceptions such as finance, health, and energy. In Britain and France, the business-civilian sector is almost completely ignored by regulation. In Germany, attempts have been made at collaboration between the state and the business-civilian sector in order to formulate standards for cybersecurity; however, this has not occurred systematically and encompasses only specific sectors.

The Israeli approach to the business-civilian sector is a complex one. The responsibility for cyber regulation of this sector is divided between the various sectoral regulators and is sometimes supervised directly by the relevant government ministry (such as in the healthcare sector), the state regulatory authority (such as the supervisor of banks), or a private organization with specific expertise that is employed by the state as a regulatory intermediary (such as in the energy sector). Despite the initiative of the National Cyber Directorate to impose binding cyber regulation on the entire economy, a systematic and organized process of identifying the potential damage to national security as a result of a cyberattack still lacks. This lacuna is even more evident given the growth of the Internet of Things, which creates new

cyber risks in sectors that have not yet been defined as a potential threat to cyberspace and national security.

In addition to the lack of binding regulation, the incentives provided to the business-civilian sector in the various countries are insufficient. In the United States, these incentives focus on information sharing and exemptions from liability when appropriate. In contrast, the European Union is developing a regulatory infrastructure to provide certificates for security products in a way that will incentivize the market to willingly adopt binding standards. The subject of standards is prominent also in the various European countries. In Britain, for example, a stamp of approval was introduced for the level of protection of a product or organization and tax breaks are awarded to organizations that assimilate cybersecurity measures. France is using the power of the state as a major employer to set minimal conditions for cyber protection among service providers interested in working with the government and participating in its tenders. Germany has established minimal conditions for encryption for organizations interested in working with the state, and in addition it is actively developing standards and regulations in cyberspace.

The lack of a suitable solution for the business-civilian sector is particularly evident given the development of the Internet of Things and the activity in the cyber insurance market. The checkered history of security in the Internet of Things around the world gives an indication of the scope of the new reference threat that originates in the private sector and that is not being met by adequate state response. The threat has intensified in view of the difficulties in developing a cyber insurance market and encouraging the widespread purchase of policies. The state will have to address major gaps and concrete questions in developing the cyber insurance market.

In conclusion, major investment has been made in protecting against cyber threats and states have developed significant capabilities in this field. Nonetheless, the provision of localized incentives to the economy and the lack of a comprehensive solution for the business-civilian sector, given the growing threats, has created a major gap in this domain. Companies that are not subject to regulation and that have neglected risk management in their cyber operations are liable to cause damage to national security. In addition, economic activity in recent years shows that a competitive market rewards companies for innovative technological products but not for having adequate security. As a result, it can be assumed that companies will not

invest sufficiently in order to protect themselves. In the absence of organized state regulation, a vacuum has been created that needs to be filled.

In order to understand the way in which to deal successfully with cyber threats in the business-civilian sector, there is a need to examine other domains. Next section's examination and analysis of what is being done in the domains of environmental protection and nuclear energy, in which private players account for much of the activity—and in most cases constitute the state's "frontline defense" against risk—will help in developing a regulatory model for cybersecurity that includes the business-civilian sector.

The Development of Regulation in the West—A Comparative Summary

The following table presents a comparative summary of the development of cyber regulation in the countries surveyed above. It describes the point in time when each country began dealing with cyber regulation, the differences in investment of resources, the degree of the regulatory regime's concentration, the part played by intelligence organizations, the sectors that are subject to regulation, and the incentives provided to the business-civilian sector.

Table 1: A Comparative Summary of the Development of Cyber Regulation in the Countries Surveyed

	Beginning of the cybersecurity regulatory regime	Annual budget of main agencies	Degree of regime centralization	Situation of the business-civilian sector	Influence of intelligence organizations	Sectors subject to binding regulation	Incentives provided to the business-civilian sector
United States	1965—Passing of the Brooks Act for the classification of information on federal networks; it empowered the National Institute of Standards and Technology (NIST) to protect government information.	US cyber budget is dispersed to many agencies. The proposed budget of the DHS in 2018 was $1.5 billion, although this figure also includes other security domains and not only cyber.	Decentralized structure—Many agencies are involved, without a single central agency, although in the domain of critical infrastructures the DHS operates as a meta-regulator.	Most of the sector is not subject to binding regulation, except for in the domains of infra-structure, health, and finance.	Major—intelligence organizations have maintained their status as influential agents, sometimes in opposition to the positions taken by legislators.	Critical infra-structures, health, and finance.	Sharing of information on cyber threats with the state makes possible exemption from responsibility in the case of damage as a result of shared information (through the Cyber Information Sharing Act).
European Union	2001—First regulation in the areas of cybersecurity and information protection by the Council.	ENISA—the agency responsible for most of the regulatory efforts in cyberspace in the European Union, had a 2017 budget of €11.1 million.	Cyber protection is the direct responsibility of member states but also addressed by the European Commission, with four Directorate Generals under it. The institutional structure includes four main institutions that divide up responsibility between them.	The business sector is supervised by means of binding regulation for the protection of personal information and communi-cation networks. This includes search engines and cloud services, which for the first time were included under information protection regulation.	The influence of the intelligence organizations on the level of the European Union is marginal. The European Union mainly emphasizes privacy and public interests. Nonetheless, the influence of the intelligence organizations is greater on the level of member states.	Sensitive sectors and service providers in cyberspace, which include the following sectors: finance, energy, water, transpor-tation, banks, health and providers of digital infra-structure, with emphasis on search engines, cloud services, and online stores.	The European Union primarily operates in the areas of deterrence and imposition of fines. At the end of 2017, ENISA began an initiative to introduce standards for industry by means of supervision of the certification of products and organizations related to cybersecurity.
Britain	1997—Founding of the program for protection of government ministries.	£400 million	Centralized structure headed by the NCSC with a leading role played by the GCHQ intelligence agency.	Most of the business sector is subject to non-binding regulation.	They have a major impact. The GCHQ intelligence agency plays a leading role in the efforts to protect all sectors.	Government ministries and critical infra-structures.	Tax breaks, minimal conditions for government tenders, state protection program that provides certification for the protection provided by products and organizations.

	Beginning of the cybersecurity regulatory regime	Annual budget of main agencies	Degree of regime centralization	Situation of the business-civilian sector	Influence of intelligence organizations	Sectors subject to binding regulation	Incentives provided to the business-civilian sector
France	1988—Law for Prevention of Computer and Cyber Crime.	€84 million	Centralized structure on the agency level, headed by ANSSI.	Most of the sector is not subject to binding supervision and regulation.	Intelligence organizations do not lead protection efforts but do set the tone and receive priority over any other agency in state cyber policy, by means of the National Security Protection Law.	Sectors within the definition "critical infrastructure operator."	Licensing of products as proof of adequate security and to establish a minimal level of protection for service providers that want to work with the state.
Germany	1991—establishment of the Federal Office for Information Security (BSI).	BSI budget in 2014 was €88 million. The government program for encouraging cybersecurity is budgeted at €40 million annually.[163]	Mostly decentralized, but BSI has numerous powers to act in various sectors of the economy.	Strategy documents indicate cooperation with the private sector. Implementation of ISO/DIN standards is dynamic.	Partial influence. The intelligence agencies are part of the configuration of agencies in Germany. The agencies for the protection of information and privacy also play a significant part in the domain of cybersecurity.	Critical infrastructures in various domains. Fines are imposed if these infrastructures do not meet official standards.	Standards for the quality of products on the market; an encryption standard that is mandatory for organizations wishing to work with the state.
Israel	1998—Creation of steering committee for the mapping of critical infrastructures.	The National Cyber Directorate has an annual budget of about NIS 200 million.[164]	In the past it was decentralized — each sectoral regulator was responsible for cybersecurity in its area of responsibility. During the past two years, there has been a trend toward centralization under one roof.	Subject to sectoral regulatory directives. Most sectors are regulated by a state authority.	Major influence. Power struggles between the National Cyber Directorate and traditional intelligence organizations.	Critical infrastructures, banks, certain institutions in the capital market, private bodies with large databases. Recently, an attempt was made to bring more entities under binding regulation.	Occurs through publication of cybersecurity strategy and dissemination of professional knowledge as needed by the National Cyber Directorate. Cooperation with the state in management of events in real time.

163 ISACA, "A Guide for the Implementation of Cyber Security Checks in Companies and Government Agencies," 2014, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/Materialien/leitfaden_EN.pdf.

164 Meir Orbach, "The Government Approves the Creation of the National Cyber Directorate," *Calcalist*, February 2015, https://www.calcalist.co.il/internet/articles/0,7340,L-3652448,00.html [Hebrew].

Chapter 3
Regulatory Models in Other Domains

In order to identify the optimal model for the development of regulation in cyberspace, it is worthwhile understanding how regulation of the economy developed in other domains. Environmental protection and nuclear energy were chosen for analysis since they involve significant risks to public and private authorities. In the market, every factory has the potential to pollute and damage the environment, and the production and use of nuclear energy constitute a major risk. These two domains have been around longer than cyberspace and their regulation by the state began much earlier.

The goal of this chapter is to describe the regulation in the domains of environmental protection and nuclear energy and to understand the regulatory principles that can be borrowed and applied in the proposed regulatory model for cyberspace.

The Regulatory Model in the Domain of Environmental Protection

The challenges of environmental protection and those of cybersecurity are greatly symmetric. The difficulties of environmental protection come not only from the multiplicity of threats and their complexity but also from regulatory barriers and the relations between the state and industry, given state desire to manage environmental risks in all sectors of the economy. The parallel between the regulatory challenges in environmental protection and those in cyberspace makes it possible to generate insights that can provide direction for the model proposed in the next chapter.

Several points of tangency between the two domains are apparent. First, both are developing and dynamic domains whose growth has accelerated during the last forty years. Moreover, the management of environmental protection risk involves various fields of knowledge, such as science, engineering, economics, law, politics, health, and communication. The domain of cyber is also complex and includes challenges from the spheres of technology,

law, defense, law enforcement, civil rights, and economic development. In addition, the two domains have no clear territorial boundaries and are subject to threats from a wide variety of sources. In both, there is a gap between the needs of companies in an industrialized nation and the desire to protect the public interest and maintain a clean space. Regulation of both environmental protection and cyberspace is perceived as lagging behind technological developments and is viewed by business as being rigid and unrelated to its needs. The two domains involve cross-sectoral regulatory challenges and create conflict between the business sector on the one hand and the desire of the state to protect the public interest and national security on the other.

Environmental regulation in Israel

Economic development and modern industry have brought with them undesirable environmental byproducts, which include pollution, the depletion of energy resources, and the production of waste. The developing nations are trying to deal with these phenomena through "traditional" regulation that includes emission quotas, fines, licensing, and prohibitions against pollution. Similarly, there are regulatory programs based on incentives, such as the encouragement of factories to develop and install green technologies, the creation of emission trading mechanisms and the initiation of voluntary regulation programs that provide a competitive advantage in the market.

The "integrative" approach to environmental protection is the most common among the more advanced nations. It is a holistic approach to environmental protection that avoids focusing on a particular type of pollution or specific environmental hazard. In contrast, environmental regulation in Israel has not adopted such an integrative approach with respect to industrial pollution.[165] The principle that guides the environmental regulatory efforts in Israel is that each type of pollution is to be dealt with by a separate set of regulations, by means of primary or secondary legislation and under the authority of the various regulators. A large number of laws require that businesses acquire permits for various types of pollution. In Israel, there are more than 350 pieces of legislation and regulation, including laws, orders, and directives, which are directly or indirectly related to the protection of the environment.[166]

---

165 Yadin, "Policy for Integrative Environmental Regulation of Industry."

166 According to the data of the Ministry of Environmental Protection: http://www.sviva.gov.il/InfoServices/ReservoirInfo/Legislation.

Anyone who is defined as a polluter must acquire permits and licenses, such as an air emission permit, an ocean dumping permit, a poisons permit, or a business license. These regulatory approvals require long and expensive processes that involve a number of regulatory authorities simultaneously: the Ministry of Environmental Protection (permits for emissions, waste, and poisons), local authorities (business license and hazard prevention), the Ministry of the Economy (safety and hygiene), the Water and Sewage Authority (wastewater flow), the Water Authority and the Ministry of Infrastructures (pollution of a water source), the Supervisor of Transport in the Ministry of Transportation (transport of dangerous materials), and the planning and building committees.[167]

Many government ministries are involved in environmental protection: The Ministry of Energy and Water is responsible for comprehensive legislation related to energy conservation and management of the water and sewage systems; the Ministry of Health is responsible for the public's health with respect to drinking water, the quality of discharges into the water and the production and sale of food; the Ministry of Agriculture is responsible for the protection of wildlife and plants; the Ministry of the Economy is responsible for safety and hygiene in the workplace; and the Ministry of Transportation is responsible for the transport of hazardous materials. It is worth mentioning that none of these ministries have enforcement powers, which are allocated exclusively to the Ministry of Environmental Protection.[168] Despite the multiplicity of authorities and their decentralization, enforcement of environmental protection is lacking and has become part of the undesirable culture of not implementing government decisions. For example, the 2002 government decision to produce electricity from renewable resources and the reduction in the emissions of greenhouse gasses has not achieved even one of its interim targets and no one has been held responsible.

Environmental impact assessment

One of the cornerstones of environmental regulation in Israel and worldwide is the system of environmental impact assessments. Apart from the labyrinth of laws and permits described above, environmental impact assessments

167 Yadin, "Policy for Integrative Environmental Regulation of Industry."

168 Tsvi Levinson and Gil Dror, "Environmental Regulation is Advancing . . . Backwards," *Water and Irrigation*, July 3, 2016 [Hebrew].

allow for environmental considerations to become a decisive factor in the decision-making process for new projects in Israel.[169] Following is a description of the environmental impact assessment's purpose and how it integrates within the decision-making process, with a comparison of the situation in Israel to that in the United States, Britain, and Holland.

The environmental impact assessment process is a way of ascertaining the expected effect of development projects on the environment, in a way that makes it possible to take steps ahead of time to prevent or mitigate negative environmental effects. The purpose of the assessment is to combine the needs of environmental protection and economic development and to ensure that projects will consider environmental factors already in the planning stage. The rationale behind this process states that it is more effective to integrate solutions within the planning stage than to look for solutions after the project has been completed and begun operation.

In Israel, the environmental impact assessment is part of the planning and building process, based on the view that environmental considerations should be integrated within the decision-making process as an integral part of the considerations of the planning and building institutions. The environmental impact assessment was created by Israeli legislation in 1982, when regulations were approved which specify the documents for assessing the effect of a development plan on the environment. There have been instances in which the assessment presented risks that were so large that there was no choice but to recommend the rejection of the proposed plans.

In the United States, environmental impact assessments have been required by law since 1970. Other countries, such as Canada, Japan, Australia, Austria, Switzerland, and Holland, followed suit. In 1985, the European Council adopted the use of environmental assessments and in 1988 the idea was implemented in practice in the EU countries.

An environmental impact assessment is essentially meant to ensure that all the essential information is gathered in order to understand and analyze the proposed project and the expected impact of building it and operating it and also to suggest the measures to prevent or mitigate harm to the environment. The assessment is important on four main levels: as a tool to be used by

169 Valerie Brachiay and Uri Marinov, "The Environmental Impact Assessment – Collection of Articles," Ministry of Environmental Protection – Planning Branch, Jerusalem, 1997 [Hebrew].

the planning authorities in order to decide whether to approve the project; as a guide in deciding what is required of the project in order to protect the public interest; as a means of clarifying the project's implications with regard to environmental quality and to provide the public with information on the project's effect on the environment, which it can use in order to voice its opposition; and as a framework to include environmental safety experts within the planning and building decision-making process.

Prior to an environmental impact assessment, instructions for carrying out the assessment are formulated by the Ministry of Environmental Protection at the request of the planning authority. The instructions for the assessment include a description of the project's expected environmental impact; the existing situation prior to the expected environmental impact; the presentation of alternatives and the reasons for the location of the project, including the factors that guided the developer in choosing the proposed alternative; a description of the plan itself and the activities derived from its implementation, including their environmental effects; an evaluation of the expected environmental impact and measures that need to be taken in order to prevent or mitigate the negative effects (which is the core of the assessment); and finally, conclusions and recommendations in the format of practical steps to fulfill the plan's instructions.

Carrying out an assessment is required in cases where the proposed projects have a significant impact on environmental quality. In some cases, it is mandated by law while in others it is left to the discretion of the planning authorities. The regulations require the submission of an assessment in the case of airports, power plants, ports, and sites for the disposal of hazardous waste. The planning institutions decide in many cases to submit an environmental impact assessment even when it is not required by law. These include plans for the construction of landing sites, marinas, water pipelines, dams and water reservoirs, sewage treatment plants, mines and quarries, sites for the disposal of solid waste, and the building of factories outside an industrial zone. The obligation to carry out an assessment also applies to a large number of national, district, and local zoning plans, as well as a plan that is viewed as environmentally problematic by the planning authorities or the relevant minister.

Following are the main participants in an environmental impact assessment:

1. The project developer: Whether public or private, the developer is responsible for the submission of the assessment to the planning authority.

To do so, it may utilize consultants who are experts in environmental impact.
2. The planning authority: It has the responsibility to provide instructions to the developer for the preparation of an assessment, to evaluate the submitted assessment, and to publish its opinion of it, with the assistance of the Ministry of Environmental Protection.
3. The Planning Branch of the Ministry of Environmental Protection: It is responsible for environmental impact assessments. It prepares the instructions and evaluates the submitted assessment, with the help of experts in each environmental domain.
4. An environmental consultant: A consultant provides advice to the Ministry of Environmental Protection in the evaluation of a submitted assessment and also to the project developer who is responsible for submitting the assessment. The environmental consultant may originate from a variety of government ministries that have a connection to the environment or be an external consultant working on their behalf.

The process for carrying out an environmental impact assessment consists of eight stages:
1. The project developer submits a plan to the planning authority and it decides whether there is a need to prepare an assessment.
2. If there is indeed a need for an assessment, the planning authority will contact an environmental consultant in order to prepare the proposed instructions for submitting the assessment.
3. The environmental consultant submits the instructions to the Ministry of Environmental Protection and they are presented to the planning authority after the approval of the director general of the Ministry of Environmental Protection.
4. The planning authority discusses the instructions and submits them to the project developer.
5. The project developer prepares (with the help of external consultants, if necessary) and submits the assessment to the planning authority.
6. The planning authority evaluates the assessment with the help of the Ministry of Environmental Protection and verifies, within a period of three months, that all the environmental implications included in the instructions for the assessment have indeed been given consideration.

7. The Ministry for Environmental Protection provides its opinion of the submitted assessment to the planning authority.
8. The planning authority decides whether or not to approve the plan. If it is approved, then the assessment and the opinion are made available to the public, which then is given the opportunity to voice its opposition.

The system for environmental impact assessments in Israel is modeled on the US system, in which the public has the right to know about the environmental impact of proposed projects. The US system assumes that the exposure of the project developer to public scrutiny and to lawsuits will induce it to take measures to prevent environmental hazards. In the United States, the preparation of an assessment is a condition for being allocated federal funding; however, the authority that decides whether to approve projects is not obligated to take the assessment's findings into account. The situation is different in Israel, where from the start there is the possibility of including the assessment within the decision-making process of the planning authorities.

The comparison of the environmental impact assessment between the United States, Britain, and Holland reveals a different approach in each country. In the United States, the preparation of a review is mandated by a law that applies to all federal activity with an impact on environmental quality (and not just construction and land usage). As mentioned, American law does not state that the findings of an environmental impact assessment must be considered in the decision-making process and does not provide a specific definition of the project types that require an assessment. The formal responsibility for preparing an environmental impact assessment is imposed on the federal Environment Protection Agency (EPA), where the project developer is responsible for its preparation and the state institution is responsible for its content.

One of the most important components of the environmental impact assessment in the United States is the description of possible alternatives. In this context, the assessment must relate to all the reasonable alternatives, including non-implementation of the project. The EPA evaluates all assessments, examining their completeness and their professional level. The influence of the EPA on the decision regarding a specific project depends upon the working relations between it and the government department responsible for the assessment.

An important part of the process in the United States is to provide information to the public. A public hearing is a built-in part of the evaluation process. However, if the EPA decides that a particular project does not have a significant impact on the environment, the assessment does not receive a public hearing and the public has no opportunity to voice its opinion.

The environmental impact assessment system in Britain is part of the physical planning process. The planning authorities are required to use the findings of the assessment in their decision making, except for decisions related to agriculture, forestry, security, sewage, and protection of the coasts. Nonetheless, the status of the assessment in decision making is limited. Thus, an incomplete assessment does not justify delaying a plan submitted for discussion. A project developer has the right to appeal the demand for an assessment and the secretary of state for environment, food, and rural affairs has the final word on the issue. The project developer who submits an environmental impact assessment is not required to include alternatives but rather only explanations of how to eliminate the risks that arise in the proposed project. In Britain, there is no stage in which a government authority provides instructions on how to carry out the assessment and neither is there any professional system for evaluating assessments.

The environmental impact assessment in Holland is obligatory to a greater extent and is part of the general environmental legislation. The legislation makes it possible to require an assessment for any activity that requires approval or a license. The Dutch legislation describes in detail the project types and the regions that are sensitive to environmental damage, as well as standards for examining their effect and the obligation for carrying out an assessment. The project developer is required to present the various alternatives in an environmental impact assessment, including the advantages and disadvantages of each, with one of them being the alternative of not implementing the project. Every assessment is presented to an independent body of environmental protection experts who are appointed by the government. This body submits its opinion to the deciding authority, which includes recommendations whether to approve the project. A public hearing is a formal part of the process and the public has the right to turn to the courts if it believes that the process was deficient.

In sum, the environmental impact assessment is not intended to solve existing environmental problems. It is also ineffective when the environmental effects are well known and there is no need to verify them or when the level

of planning is not sufficiently detailed in order to assess environmental impact. It serves as an efficient tool in deciding whether to approve proposed projects, and its unique location in this process makes it possible to include environmental protection considerations within projects of many sectors of the economy. In this way, it is possible to map and manage risk at an early stage. The findings of the assessment allow decision makers to approve projects, to place limitations or reservations on their implementation, to make changes in them, to delay their implementation, or even to cancel them altogether.[170]

From environmental protection to cyber protection

From a broad historical perspective, it is possible to find numerous similarities between the development of regulation in environmental protection and in cyberspace. Historically, environmental regulation preceded cyber regulation by several decades. In both domains, regulation began with the imposition of sanctions. The first sanctions in environmental protection were imposed on polluters that did not meet government standards, while sanctions in cyberspace were imposed for computer crimes, as defined in the first cyber laws in the various countries. At a later stage, regulation was based on supervision and regulation of the key players, in both environmental protection and cybersecurity. In the former, these were large polluters while in the latter, they were information system infrastructures defined as critical to national security. Currently, regulation in both domains is expanding and is being applied to an increasing number of sectors and is gradually being viewed as a binding standard for a growing number of businesses and organizations.

In both domains, the initial ethos did not accomplish what it had meant to. The desire to maintain the ethos of nature or a digital domain free of intervention, which would benefit all to the same extent, was inconsistent with the developments in industry and technology and the negative byproducts that accompanied them. Phenomena of polluted water resources, unequal consumption of natural resources, and sea and air pollution became common. Cyberspace experienced a similar process and became subject to threats from both state and non-state players who sought to exploit its weaknesses, to steal sensitive information, and to cause harm.

---

170 Brachiay and Marinov, "The Environmental Impact Assessment – Collection of Articles."

In Israel, the first sanctions for environmental protection were imposed on those harming wildlife, vegetation, and water sources. The first sanctions in cyberspace were imposed on computer criminals—the classic hackers—which the state sought to deter. The next stage of regulation in both domains was based on the understanding that damage to the environment or in cyberspace has an impact on other domains that are related to the economy, security, and society's functioning. New threats became part of the discourse and it became clearer that the environment and cyberspace have major ramifications in other domains as well. Therefore, the new threats called for an across-the-board—as opposed to localized—response by the state.

As a result, regulatory authorities were created in Israel whose function is to supervise what was previously defined as "critical." The most urgent problems in the environment led to the establishment of non-profit organizations such as Adam Teva ve'Din and other environmental organizations, which later grew into a large civil society movements.[171] The change in the discourse led to a flood of laws and regulations, such as the Hazard Prevention Law (which led to the establishment of an enforcement body in the form of the Public Council for Noise and Air Pollution), a law to protect the quality of drinking water, a directive regarding oil pollution in the sea, the Prevention of Sea Pollution Law, the Anti-Litter Law, the Freshwater Sources Pollution Law, the Hazardous Materials Law, and the Law for Collection and Disposal of Waste for Recycling. These laws led to regulation that established standards and norms for the implementation of timely measures meant to prevent pollution, hazards, and inappropriate use of natural resources. Similarly, the perspective in cyberspace is sectoral, where each regulator protects cyberspace within its realm of responsibility.

Despite the many points of similarity, the regulation of cyberspace lags behind that of environmental protection in the degree of intervention by effective mechanisms and by civil society organizations. The effective institutional mechanisms for the supervision and management of environmental protection include the Local Authorities Law, which assigns responsibility for municipal sewage to the municipalities; the National Parks Law, which established

171 More than one hundred organizations are registered as members of the umbrella organization Life and Environment. See additional information in Alon Tal, Shira Leon Zechut, Liat Frankel Ashuri, Etai Greenspan, and Shira Akov, "The Environmental Movement in Israel – Trends, Needs and Potential," Ben Gurion University of the Negev, June 2011 [Hebrew].

the National Parks and Nature Reserves Authority whose function is to protect sites with historical and national value; the Rivers Authority whose function is to protect the country's rivers; the Planning and Construction Law which established the planning and building committees; and the Business Licensing Law whose goal is to prevent environmental hazards. The growing influence of globalization processes and the privatization of environmental risk management in the twenty-first century have raised the awareness of civil society environmental organizations and reinforced their public standing. These organizations exploited the momentum created and promoted additional laws, such as the Bottle Deposit Recycling Law, the Coastal Environment Protection Law, the Clean Air Law, and the Packaging Regulation Law. In addition, the Supreme Court has been sympathetic toward the protection of the environment and the role of environmental organizations in its rulings.

When Israel joined the OECD, it began to adopt economic tools to further environmental goals, such as fees and levies on emissions as part of the Clear Air Law, the deposit mechanism in the Bottle Deposit Law, the levy on dumping waste into the ocean, economic enforcement mechanisms, and compulsory reporting and registration to achieve transparency of information on environmental risks. During this period, mechanisms for self-regulation that are based on the desire of companies to protect the environment took on a larger role within the context of existing standards, such as ISO 14001, the Green Stamp, and the Maaleh index. These mechanisms are supervised by the companies themselves or by independent third parties.

Cyberspace has not yet undergone a similar stage of development. Apart from the protection of critical infrastructures and the regulation by specific authorities, such as the Bank of Israel and the Israel Securities Authority, there is no supervision over mechanisms of self-regulation and there is no protection of the business-civilian sector as a whole. The regulatory model proposed below attempts to bridge this gap.

Adoption of environmental protection regulatory models in cyberspace

The survey of regulatory models in environmental protection yields several insights that will be useful in developing a regulatory model for cyberspace. First, it is proposed that a holistic approach be adopted in this domain. Just as an environmental hazard can have an impact across sectors, so also damage to information systems can lead to a chain reaction that will endanger Israel's national security. Holistic regulation in environmental protection

does not consider pollution from a one-dimensional perspective but rather endeavors to relate to cross-sectoral effects. The prevention of air pollution from a factory that is polluting the water in a nearby lake will improve the quality of both the air and the water.[172] The environmental regulator is meant to take these two effects into account when examining the cost-benefit of the proposed regulations. Accordingly, the proposed model for cyberspace should relate to the broader implications of a cyberattack as a result of deficiencies in cyber protection.

Second, as in environmental protection, we are witnessing a shift from "traditional" regulation involving levies and rigid standards to regulation based on incentives and market mechanisms and therefore mechanisms should be created in cyberspace that will incentivize industry to protect itself, particularly when the current market model in cyberspace does not sufficiently incentivize the development of secure products and creates a preference for innovation over security and protection. The importance of the way in which industry behaves has led decision makers in environmental protection to create incentives for the private sector. The encouragement of initiatives to develop and install technologies for the reduction of pollution in exchange for benefits, the introduction of emission trade mechanisms, and even the creation of "green" factories under state auspices are only some of the ways in which the state encourages environmental protection in the private sector. Regulation of industry in cyberspace should involve similar mechanisms, which will change the equilibrium in the current market model and in a way that will provide rewards for appropriate levels of protection, rather than only for initiative and innovation in product development.

Another important principle is to avoid a multiplicity of authorities and decision makers in cyberspace. Based on what is happening in environmental protection and the involvement of more than five government ministries that lack appropriate enforcement powers, it can be concluded that the business-civilian sector will benefit from working with a single body that will provide direction to the sectoral regulators as needed. The institutional infrastructure for such a body in cyberspace was put into place with the establishment of the National Cyber Directorate in recent years. Furthermore, the power struggles described in state comptroller reports and in the discussions of Knesset committees indicate that changing the institutional structure has been

172 Yadin, "Policy for Integrative Environmental Regulation of Industry."

beset with problems. Based on what has been accomplished in environmental protection, such consolidation is important in achieving efficient regulation. Indeed, since the end of 2017, it appears that regulation in cyberspace is progressing in the right direction under the guidance of the National Cyber Directorate.

Environmental protection is an important case study of the problematic culture of compliance among supervised entities and the phenomenon in which supervisory bodies in Israel avoid taking responsibility. The situation of insufficient enforcement of the Business Licensing Law—which is the basis for environmental protection, among other things, in the private sector—and the fact that government decisions on environmental protection are often not carried out and do not specify the party responsible for enforcement provide a lesson as to how regulation in cyberspace should not be developed. The proposed model for cyber regulation will need to consider the culture of noncompliance among supervised entities and determine a scale for imposing sanctions that will make noncompliance worthless. In addition, external monitoring mechanisms should be put into place for the implementation of government decisions in cyberspace in order to verify implementation.

Finally, the adoption of the environmental impact assessment framework in the decision-making process of organizations and companies in cyberspace and its integration within the proposed model will provide solutions in the form of regulatory tools in a wide variety of sectors. Just as the environmental impact assessment is meant to provide an understanding of how natural resources (land, air, and water) are being exploited or of the population's exposure to pollution (air pollution, noise pollution, and so forth) and to determine whether they are reasonable relative to the contribution of each project, an assessment of the cyber impact of each project will make it possible to avoid or mitigate harm to Israel's national security that originates from cyberspace. At the same time, the adoption of the environmental assessment model will help in dispelling fears of cyber threats originating from new projects and as a result will encourage industrial and economic development.

The Regulatory Model in the Nuclear Energy Sector

Regulation in the nuclear energy sector, like in environmental protection, can provide insights into the regulatory model to be adopted in cyberspace. The nuclear energy sector came into being with the scientific discoveries in Germany in 1938, which for the first time made possible the theoretical

development of an atomic bomb.[173] In response, the United States accelerated its nuclear research program and began to enrich its stock of uranium, with the goal of overtaking the Germans in the development of nuclear capability.[174] In 1941, President Roosevelt signed an executive order to create the Office of Scientific Research and Development and to develop applied projects in parallel to the existing research. Meanwhile, researchers at the University of Birmingham in Britain made some major discoveries in nuclear research, which put them ahead of their American allies with whom they shared knowledge. The cooperation between the two countries led President Roosevelt to approve the development of a nuclear bomb and assigned the US Army the leading role in the project, which became known as the Manhattan Project.[175]

During the 1940s, the United States ceased sharing knowledge with its allies and established a culture of concealment regarding the development of its nuclear capabilities. This strategy accelerated the nuclear arms race. In 1952, Britain produced its own nuclear bomb. President Eisenhower decided to change the policy of concealment and in a speech to the UN declared the Atoms for Peace program among the Western allies as part of the International Atomic Energy Agency. This led to information-sharing agreements between nations, which involved the exploitation of the American advantage in knowledge for political and economic purposes.[176] In this framework, the United States agreed to provide knowledge on enriched uranium, heavy water, and nuclear bomb development, as long as the partner country promised to use nuclear energy for peaceful purposes. The enforcement of how the nuclear energy was to be used was carried out by American inspectors.

The 1950s saw the privatization of nuclear energy development in the United States. American companies became dominant in the international

---

173 Tom Sharpe, "Explore the Making of the Atomic Bomb: Guide Details Manhattan Project Sites in N.M.," *McClatchy - Tribune Business News*, June 15, 2010.

174 L.R. Walton, W.A. Orenstein, and L.K. Pickering, "The History of the United States Advisory Committee on Immunization Practices (ACIP)," *Vaccine* 33, no. 3 (2015): 405–414.

175 William Lanouette, "Book Review – Nuclear Rivals: Anglo-American Atomic Relations 1941–1952 by Septimus H. Paul," *Isis* 93, no. 1 (2002): 128–129.

176 Yateen R. Pargaonkar, "Leveraging Patent Landscape Analysis and IP Competitive Intelligence for Competitive Advantage," *World Patent Information* 45 (2016): 10–20.

nuclear energy sector. The Nuclear Regulatory Commission (NRC) became the regulator of the private nuclear industry in the United States and was responsible for meeting the challenges of supervision and enforcement of safety in this sector. Still today, most of the nuclear energy infrastructure in the United States is owned by private companies, although the state is deeply involved in the activity of these companies and in the financing of their research. The private sector does not particularly welcome this involvement, due to the complexity, among other things, that it introduces. Thus, for example, the state's process of approving a new nuclear power plant takes between three and five years and the financing of scientists working in this field comes primarily from national laboratories and universities that work in collaboration with industry.

Two main risks are managed by the state regulation of nuclear energy. The first is the risk to workers in nuclear facilities. Regulation in this area relates to the operation of nuclear facilities and their safety standards, including the prevention of exposure to radiation and environmental damage. The second concerns the production of weapons of mass destruction. The regulation in this area attempts to prevent the use of nuclear energy as a weapon and does so by means of licensing, restrictions on exports and monitoring of the use of materials in nuclear facilities. Alongside the importance attributed by nuclear regulators to the production of nuclear weapons, safety in the operation of nuclear power plants also became a greater priority following accidents at these facilities.

The monitoring of the safety of nuclear facilities in the United States is assigned to the NRC, which is responsible for the safety and security of all aspects of nuclear energy. The NRC supervises the various nuclear facilities, is responsible for the licensing of their operations and for renewing licenses, and manages the environmental risks in their operations.[177] In addition to the NRC, the nuclear industry in the United States set up another designated body, the Institute for Nuclear Power Operations (INPO), which proposes and assimilates safety standards in nuclear facilities. The INPO model has been adopted all over the world and has become the global model implemented by the World Association of Nuclear Operations (WANO), an

177 US Nuclear Regulatory Commission, "Information Technology/Information Management Strategic Plan," US Nuclear Regulatory Commission Strategic Plan, vol. 1 (2008).

umbrella organization of nuclear facilities around the world, which shares information and develops expertise, with the goal of maintaining safety in nuclear facilities.[178] The motivation to share information grew following the Three Mile Island nuclear accident in Pennsylvania in 1979, which made clear the priority of transparency over commercial secrecy in the operation of private nuclear reactors. In this case, there was no economic incentive for sharing information but rather a desire among various companies to do everything possible to prevent the next nuclear disaster.

With respect to the safety of nuclear facilities, there are reciprocal guarantee agreements between the European countries in the case of a nuclear accident.[179] This guarantee makes it possible for the nuclear industry to develop, as in the case of the 1957 Price-Anderson Act in the United States that promised state compensation to private businesses in the case of a nuclear safety accident at their facilities.

The encouragement of the nuclear industry, the provision of financial guarantees by the state, and the existence of mechanisms for cooperation also made possible the creation of an insurance market in the nuclear domain. The various insurance companies rely on the universal standards for civilian facilities that were established by the INPO, in a way that makes the insurance policies profitable for them. The NRC requires expensive insurance policies as a condition for granting an operating license to nuclear facilities and in this way verifies that the applicant for a license has the economic resilience needed to address a nuclear accident.

The second type of risk—the production of weapons of mass destruction—is primarily the responsibility of the International Atomic Energy Agency (IAEA). The IAEA uses monitoring measures and sophisticated capabilities for identifying nuclear traces and the use of materials that are prohibited by signed agreements. In the case of a violation of these agreements, the IAEA can report to the UN Security Council, which has the power to impose military and economic sanctions on countries that are developing weapons of mass destruction in violation of what has been agreed upon. The IAEA has signed agreements with WANO for the advancement of safety in nuclear facilities

178 Ramon Revuelta, "Operational Experience Feedback in the World Association of Nuclear Operators (WANO)," *Journal of Hazardous Materials* 111, no. 1 (2004): 67–71.

179 John Braithwaite and Peter Drahos, *Global Business Regulation* (Cambridge, Cambridge University Press, 2000), pp. 297–319.

in order to avoid a conflict of interest and to promote a joint effort to ensure the safety of nuclear facilities all over the world. Essentially, the IAEA has a double role, namely the management of safety risks at nuclear facilities and the prevention of the proliferation of weapons of mass destruction, a situation that reduces the effectiveness of its activities. One of the criticisms of the IAEA, which became particularly vocal after the disaster at the Fukushima nuclear power plant in 2011,[180] is its inability to establish binding standards for the civilian nuclear industry.

The adoption of nuclear energy regulatory models in cyberspace

The challenges of safety and security in the nuclear energy sector are unique to that environment. Nonetheless, much can be learned from the industrial and international cooperation to promote safety and prevent the proliferation of weapons of mass destruction throughout the world, as well as the widespread practice of state compensation in the event of a nuclear accident. This intervention has facilitated the development of the industry and the insurance market in a way that has increased the number of stakeholders in the regulation of nuclear energy.

The cooperation in nuclear energy led to the creation of national and international centers of knowledge, on both the public and private levels, which help to preserve the safety of nuclear facilities. The creation of such centers for knowledge sharing between players in cyberspace will significantly advance the development of knowledge and protection in this domain. Although there are private initiatives for the sharing of knowledge related to cyber threats, they do not cut across sectors and do not benefit from any state-provided incentives; on the contrary, there is a clear lack of trust between industry and the state, particularly in the United States, on issues of cybersecurity. A possible reason is that there has not yet been a disaster on the scale of a nuclear accident, such as that which occurred in Japan in 2011, in the former Soviet Union in 1986, and in the United States in 1979. This has led to a lack of urgency to create large-scale collaborations in cyberspace.

---

180 The nuclear disaster occurred as a result of damage from an earthquake and a subsequent tsunami. During the accident, a significant amount of radioactive material was released into the atmosphere, the ground, and the Pacific Ocean. Several of the plant's employees were seriously injured and more than 300 absorbed serious amounts of radiation. The cleanup activity around the plant is expected to continue for decades.

From the viewpoint of state intervention, the state is currently involved in almost every aspect of the nuclear facilities within its borders. In the United States, this is carried out by a designated authority that brings together under one roof the powers and expertise in this sector. Such centralization of authority still does not exist in cyberspace, although it has, in fact, begun to develop in Israel since 2015 in the form of the National Cyber Directorate. Moreover, the standards on which cyber regulation rests are, for the most part, viewed by private companies as ineffective given the fast pace of technological development.

The practice of issuing an operating license for nuclear energy activity also in cyberspace is worthy of adopting. In order to obtain a license, a nuclear facility must subject itself to systematic examination and supervision and this is a regulatory tool that can also help eliminate cyber risks in the private sector. Cyberspace should also adopt the idea of collaboration between the various entities, as in the domain of nuclear energy, which will facilitate the development of appropriate standards.

On the international level, the IAEA oversees the nuclear energy sector. It has monitoring and enforcement powers and establishes norms that are adhered to by member states. In contrast, there is currently no international cooperation within the framework of a single organization in cyberspace. The creation of such an organization will facilitate the establishment of international norms for handling cyberattacks, will have an impact on the domain of cyber threats and will help to introduce ethical considerations in the use of offensive measures.

With respect to incentives, the state currently provides a guarantee of generous compensation in the event of a nuclear accident. This compensation mechanism creates the stability needed by the industry to develop and for the insurance market to spread risk among policy holders. The fact that insurance companies know that in the event of large-scale damage the state will provide economic guarantees incentivizes these companies to offer policies and to assist in advancing the public interest in the safety of nuclear facilities. Similar state involvement can support cybersecurity efforts. The establishment of a functioning insurance market under state guarantee will make it possible to raise the level of cybersecurity and will serve as an incentive to lower the cost of policies to organizations and companies. Finally, it will introduce another major player, namely the insurance companies, into cyberspace, which will have an interest in protecting this domain also in the business sector.

Chapter 4
Proposed Regulatory Model for Cyberspace in Israel

The previous chapters surveyed the challenges in managing cyber risk by means of regulatory regimes, presented a comparison of what is being done in key countries with regard to cyber regulation, and provided insights based on regulation in the domains of environmental protection and nuclear energy. The emerging threats in cyberspace call for wise state intervention, which, on the one hand, will mandate appropriate and proportionate security measures and, on the other hand, will encourage the market to protect itself by means of incentives, including identifying primary intervention objectives, for which the benefits of protection outweigh the cost.

The proposed regulatory model for Israeli cyberspace focuses on the regulation of day-to-day operations. The model is based on what already exists but also innovates and extends it, and it differentiates between three types of regulation—self-regulation, binding state regulation, and voluntary incentive-based regulation—as follows:

1. **Self-regulation.** Security organizations such as the IDF, the GSS, the Mossad, and the Israel Police will be subject exclusively to internal directives, which will be periodically validated by the risk management mechanisms in each organization and will be subject to external oversight.
2. **Binding regulation**. The state will impose binding regulation on organizations should damage to their cyber infrastructure threaten Israel's national security. These bodies will be divided into sectors according to five categories:
   a. *Defense industries and facilities*, whether under private or public ownership, as well as highly sensitive projects will be overseen by the director of security of the defense establishment (DSDE).
   b. *Critical infrastructures* will be subject to the directives of the GSS and the National Cyber Directorate. The GSS will require operators

of communication infrastructure, such as Bezeq, to accept binding regulation, which will include standards, periodic breach testing, and responses to emerging threats, while the National Cyber Directorate will oversee and assist critical infrastructure operators in the rest of the sectors, such as transportation, energy, water, ports, and air transport, in meeting stringent standards of cybersecurity.

c. *Economic sectors that are essential to the continuity of functioning in Israel* will be overseen by the specific sectoral regulator in each government ministry, in cooperation with the National Cyber Directorate and under its supervision. For example, the supervisor of banks will impose cybersecurity regulations on the banking system; the Israel Securities Authority will impose binding regulations on the infrastructures for trading in the capital market; the Ministry of Health will require hospitals to meet cyber regulation standards; and the Ministry of Energy will require private energy infrastructures to operate under cybersecurity regulation.
d. *Private businesses* that require a business license or permit from the various planning authorities will be subject to regulation that applies in the business-civilian sector, based on the cyber resilience review questionnaire that each business will be required to fill in. The goal of this regulation is to reduce the potential harm to the public in the event of a localized cyber event in a company or private organization.
e. *In key resiliency points for cyberspace*, binding regulation will be imposed in order to reinforce cyber resilience. For example, providers of services that constitute a critical component in the chain of supply of many organizations such as payment industry methods; companies that host internet web sites; installers of various information security products in the market; and so forth.

3. **Incentive-based regulation**. The role of state incentives is to encourage cybersecurity practices within organizations. These include, for example, the encouragement and creation of a cyber insurance market; the provision of tax breaks for the acquisition of cyber protection; and the provision of incentives for the sharing of information on cyber threats among organizations.

Following is a description of the three regulatory frameworks that together compose the proposed model for the regulation of cyberspace in Israel.

Self-Regulation

As mentioned, security organizations such as the IDF, the GSS, the Mossad, and the Israel Police will be subject to internal directives only. In this domain, the proposed model leaves the current situation unchanged. Nonetheless, all organizations included in this category should develop self-monitoring abilities in order to apply developments in cybersecurity knowledge and report to an external body, such as the state comptroller, about their activity in cyberspace. For example, these organizations should carry out risk management processes on a scheduled basis—annually or biannually—with the assistance of external bodies that are authorized to operate in these organizations' sensitive environment.

The danger in self-regulation for such sensitive organizations is that the existing organizational barriers, which may prevent attaining optimal protection, will remain in place. This is a risk that should be managed by periodic external audits in coordination with the organizations themselves.

Binding Regulation

Binding state regulation will be imposed on an organization if it faces a cyber threat that represents a threat to Israel's national security. This type of regulation will be imposed by various state authorities with expertise in the operations of the regulated organizations, as will be described below.

Supervision by the DSDE of the defense industries and sensitive facilities

The supervision and regulation of the defense industries and sensitive facilities by the DSDE will preserve the secrecy of their operations. Regulation by the DSDE includes both defense-related directives in cyberspace and regulatory governance. This is based on the desire to protect national security and the functional continuity of the supervised organizations.

The regulation of organizations by the DSDE includes the provision of intelligence information if necessary, the issuing of directives for cyber protection, and the creation of criteria for position holders in the domain of cybersecurity. The supervised organization is meant to provide the resources and to implement what is requested by the supervising entity. According to the proposed format, the DSDE will in most cases decide on the guidelines for cyber protection and the supervised organizations will choose how to implement them. In any case, the directives must be implemented with the cooperation of both sides.

Binding regulation of critical infrastructures

Binding regulation will also apply to organizations defined as essential/critical infrastructures. Both the National Cyber Directorate and the GSS will carry out the supervision, as is currently the practice. The National Cyber Directorate will develop knowledge and expertise, in collaboration with the GSS, in order to protect critical infrastructure organizations. A designated steering committee will examine and redefine the list of entities in this category, if necessary, and those on the list will need to meet stringent standards, including periodic breach tests.

The steering committee will be composed of representative of the GSS, the National Cyber Directorate, the Ministry of Infrastructures, and private companies that are involved in the protection of critical infrastructures. The committee will periodically consider the possibility of adding new organizations to the binding regulatory framework or to remove organizations already in it.

Binding regulation in the government sector

In addition to the organizations defined as critical infrastructures, numerous systems and organizations are highly important to national security but are not yet defined as critical infrastructures by the state. These include, for example, hospitals, the traffic light system, the electoral system, banks, and the food industry. Therefore, it is recommended that the regulator in each of these sectors accumulate expertise in their operations and supervise them with the goal of preventing harm to national security.

The proposed model recommends that sectoral regulators, which oversee organizations with a potential to cause harm to Israel's national security, will continue to fulfill that function. Similarly, the model is in favor of the sectoral regulator relying on professional experts, under the guidance provided by the National Cyber Directorate. This will make it possible, on the one hand, to provide professional guidance to organizations that are important to national security and on the other hand will maintain the role of the sectoral regulator in implementing binding regulation. The sectoral regulator will operate by issuing detailed directives in the area of its supervision, as in the case of the Bank of Israel and the Israel Securities Authority, and also by means of regulatory intermediaries that will develop expertise in the area, as in the case of the Ministry of Energy (which has authorized an external

professional body to act as a regulatory intermediary for cybersecurity in the private energy infrastructure sector).

Binding regulation of licensed businesses

Up until this point, the proposed model has, for the most part, adopted the existing situation. What follows is a detailed description of the proposed model's innovative aspects, which seek to impose various levels of cyber regulation on the entire economy, in accordance with the criteria met by each organization. The goal is to find a balance between deepening cybersecurity at the national level on the one hand and the continued development of business organizations' ability to operate and to advance the Israeli economy on the other.

The proposed model is based on the existing regulatory model for cybersecurity, which requires that each business organization requesting or renewing a business license will evaluate the potential harm that could be caused to national security as the result of a successful cyberattack.

The following discusses the existing gap in the decision-making process regarding the imposition of binding cybersecurity regulations and describes the relevant state regulator in the domain and the proposed process.

Decision making in Israel regarding protection in cyberspace

The reinforcement of cyberspace's resilience on the national level requires that every organization operating in the domain understands and systematically maps the potential damage it faces in every type of cyberattack. While various countries have developed ways to protect the infrastructures that are critical to their functioning,[181] the decision-making process in Israel, which relates to the question of what to protect and how, is not transparent and systematic, does not ensure appropriate protection at an early stage, and is not able to prevent harm to national security.

The quantification of the potential damage originating from information systems is a complex task that requires in-depth familiarity with the organizational processes in each organization. The damage is measured not

181 In 2002, the National Authority for Information Security was established in Israel. It has the power and responsibility for information systems, on the basis of the decisions of the designated steering committee of the National Security Council, whose job is to examine the information security risks implicit in every system in the domain.

only in financial terms or according to the effect on the country's GDP but also by the damage to assets that have national and symbolic importance. In the United States, for example, there are plans to protect heritage and memorial sites.[182] The range and scope of the damage in cyberspace is too broad in order to carry out an unequivocal ranking, according to which mandatory protection would be imposed. The model proposes a possible mechanism for quantifying the damage and imposing designated "protective suits" to reinforce the resilience of cyberspace and to prevent harm to national security.

The US Department of Homeland Security uses a methodology called cyber resiliency review.[183] It relates to the main elements of an organization's operations and provides a picture of the critical assets to be protected, the management of the organization's communication infrastructure, the factors that affect its functional continuity, its technological management, the scope of its dependency on external factors, the management of emergencies and accidents, its ability to identify and manage weaknesses, and its ability to carry out an objective evaluation. A review of these elements makes it possible for decision makers in each organization to obtain an overall cyber picture and to formulate a work plan for improving its cyber resiliency; however, the process is not sufficiently systematic, nor is it mandatory and therefore does not ensure resiliency in practice.

The situation in Israel is quite similar. The steering committee meets from time to time and examines the list of organizations defined as critical infrastructures. Their inclusion on the list requires that they upgrade their cyber protection and that they meet the cybersecurity directives of the GSS (in the case of communication providers) or of the National Cyber Directorate (in any other case). However, there is currently no systematic and binding statutory process with clear criteria that enables early identification of these groups.[184] When an organization or body is defined as subject to cybersecurity regulation, the actual process of supervision begins, whether carried out by

182 Patrick Beggs, "Securing the Nation's Critical Cyber Infrastructure," US Department of Homeland Security, February 25, 2010.

183 These sectors include, among others, water, energy, communication, transportation, the chemical industry, agriculture and the food industry, information systems, banking, financial and commercial services, health services, and also assets with importance to national identity (memorial sites, heritage sites, and so forth).

184 The criteria used by the steering committee are not public knowledge and the how they defined critical infrastructure in Israel remains confidential.

the GSS or by the National Cyber Directorate. This supervision includes the gathering of information on the potential threats to the organization; warnings of possible cyber failures in the organization; direction on how to protect its assets; and inspections and surprise simulations as part of enforcement.

The main question is how to identify organizations that are potentially critical infrastructures before any harm occurs. This a complex task, given that almost every business or government industry has an interface with sectors that are defined as critical infrastructures. For example, the protection of water supply infrastructures and water quality in Israel is not just related to processes at the Mekorot company but also to dozens of other entities, such as other water suppliers, the water corporations, desalinization and conveyance facilities, sewage treatment facilities, facilities for treating and conveyance of waste water, and so forth. A large number of these facilities are operated as private businesses and cybersecurity is not always their first priority. Another example is the suppliers and subcontractors used by systems that are defined as critical infrastructures by the state. For example, an industrial plant that has been designated as critical infrastructure and operates under the binding supervision of the National Cyber Directorate may be dependent on other producers (smaller "satellite producers") that provide inputs (sometimes critical ones) for the plant's production process. In many cases, some of these satellite producers are not included in the category of critical infrastructures and therefore their level of protection is less than optimal. Any cyberattack on them could significantly damage the critical infrastructure.

It is therefore essential to map potential damage to the business-civilian sector. As the use of information technologies is widespread in Israel, in both the public and private sectors, Israel presents a large range of targets to potential cyberattackers interested in harming Israel's resilience and national security. Therefore, identifying additional entities whose operations call for supervision by the National Cyber Directorate or a sectoral regulator is necessary in order to achieve an optimal level of protection.

Surveys carried out from time to time and information provided by the various government ministries confirm this need, but there is still no overall response. A structured process should be initiated that will lead to significantly improving the protection of projects in the private sector that are exposed to cyberattacks, which could potentially affect the national level.

The regulator in cyberspace

The process of mapping the business sector and the state's involvement in order to protect cyberspace already at the stage of issuing a business license will require cross-sectoral analysis since the development of knowledge in cybersecurity is common to all sectors. Therefore, the cyber regulation of licensed businesses will be based on both the National Cyber Directorate, whose function is to develop knowledge, tools, and methods that can raise their level of cyber protection, and the sectoral regulators, which develop expertise according to the needs of the specific sector and make any necessary modifications to the general directives of the National Cyber Directorate. These two bodies must achieve synergy, based on the working assumption that most of the regulation in cyberspace does not vary across sectors; nonetheless, existing directives should be modified according to the nature of the supervised entity.

An example of such integration can already be seen in the cooperation between the government ICT Authority and the Ministry of Health. The role of the government ICT Authority is to supervise the protection efforts of all government ministries while the Ministry of Health makes the necessary modifications to its directives when applying them in the hospitals under its responsibility. A process should be created—which the National Cyber Directorate has already begun—that will define the relevant regulator for cyber protection in a particular organization, with the aim of avoiding a situation (that already exists to some extent) in which a number of regulators are supervising the same organization and in the same context.

The proposed process: Use of existing statutory tools

As described in the review of the literature, organizations in Israel that have been defined as critical infrastructures are subject to binding supervision by the GSS (in the case of data communication organizations) or by the National Cyber Directorate (in the case of all other critical infrastructure organizations). The regulation of government ministries and authorities and the organizations under them is the responsibility of the government ICT Authority. It also supervises other sectors, which, according to their level of criticality, are supervised by additional state cyber regulatory bodies (for example, the Electricity Authority). The various government ministries supervise bodies within their sphere of responsibility that are perceived as

important. Thus, for example, the Ministry of the Interior supervises the local authorities and the companies that operate within their frameworks.

Most of the business-civilian sector in Israel is not currently regulated. In order to improve this situation, it is proposed that cybersecurity be introduced as a structured component of the existing statutory process in the business sector, both in the stage of creating a project (approval by the various planning committees) and when it is already operational (the Business Licensing Law). We propose that for every project submitted for the approval of the state's planning committees, a questionnaire should be filled out in order to assess the potential damage from a cyberattack. The questionnaire will constitute the main statutory tool for identifying and assessing a project's exposure to the possibility of cyberattack and for implementing protective measures against such attacks. The questionnaire will also provide the National Cyber Directorate with a tool for identifying and managing critical infrastructures in Israel that require protection. In addition, the relevant authority responsible for licensing the project will be able to evaluate the entity's long-term ability to fulfill cybersecurity directives.

At this point, a more in-depth explanation of the proposal is necessary. The creation of any enterprise in Israel, including national infrastructure projects, requires that it go through the existing statutory planning processes. Thus, projects that involve the construction of facilities and structures are required to obtain the approval of the various planning committees, according to the circumstances: local, district, and national. The assessment of the planning documents that are submitted for the approval of the relevant planning authority is one of the main tools for supervising these projects. Among the documents submitted for the evaluation of the planning committees are those related to fire safety, various aspects of public health, environmental considerations, handling of hazardous materials, protection of the home front, and so forth. These documents define the steps to be taken by the project developer in order to meet the requirements in each of these domains. These steps are subject to the oversight of the authorized regulatory authorities, which utilize experts in order to ensure that the project does not threaten the public interest or national security.

Dozens of projects are considered each year in Israel and any threat to them is also liable to be a threat to national security. Examples include infrastructure facilities, water and sewage treatment plants, transmission systems, transportation projects, and energy and communication facilities.

In addition, the construction or expansion of industrial facilities is discussed. A cyber threat to some or all of these projects and initiatives is likely to cause not only direct economic damage to the country, such as the inability to provide an essential service, but also harm, such as Israeli companies being unable to supply their products for some given period.

One example that can illustrate the proposed process is the requirement to submit an environmental impact assessment. Its goal is to identify and assess the environmental hazards that could result from implementing the project and the ways of minimizing the harm to an acceptable level. Submitting an environmental impact assessment is anchored in the planning and building regulations (issued in 1982 and updated in 2003). As mentioned, the environmental impact assessment was the result of the increase in public awareness of environmental issues in the United States, and in 1970, it led to the passing of legislation that made it part of the planning process.

Alongside the planning component of new projects, it is possible, as mentioned, to also take advantage of the business licensing process, which require license renewal, in order to verify that the project over time continues to meet the criteria to which it is obligated in the various domains, including protecting against cyberattacks. Mishael Cheshin, a former Supreme Court judge, stated in one of his rulings that "the goal of this law [business licensing] is to preserve and protect various values that are perceived in our society as important . . . including protecting the public, maintaining public health and safety, protecting environmental quality and quality of life . . . in order to meet the goals of society."[185] Accordingly, the tool provided by the Business Licensing Law can be used for the purpose of cyber protection. Thus, it creates another legal regulatory tool to be used by the National Cyber Directorate, which can verify that existing enterprises meet the binding regulations that apply to them. In certain cases, it can even require private businesses to submit a cyber resilience review and to fulfil cyber protection directives.

Questionnaire to determine potential cyber threat damage

As part of the process for receiving or renewing a business license, project developers will contact the National Cyber Directorate, which will provide them with a questionnaire to understand the extent of exposure to the public in the event of a cyberattack on their organization. The questionnaire will

185 Criminal Appeal Authority 4270/03, State of Israel vs. Tnuva [Hebrew].

seek to ascertain the organization's level of network activity, the degree of its exposure to the public in the event of a successful cyberattack, and the importance of the organization to the country's functional continuity and its national security. The questionnaire will make it possible to determine a cyber ranking for the project and the content of the cyber resilience review that it must carry out. The more important the project to national security, the more detailed the cyber resilience review will be. The costs of closing any gaps found in the organization's cyber protection will probably also be higher.

The National Cyber Directorate will determine the criteria to be included in the questionnaire, which will be used to define the projects that must carry out a cyber resilience review. These can include a number of components, such as the size of the project, its exposure to the internet, its exposure to cyber risk factors, the sector to which it belongs, the project's interfaces with entities that are already under the supervision of the National Cyber Directorate or the GSS, and also various aspects related to any expected damage from a cyberattack.

It should be made clear that the need to implement cyber protection measures, based on the diagnosis of the organization, will be determined solely according to the estimated extent of damage to national security that could result from an attack on its cyber infrastructures. The state is not concerned about any economic damage caused to the organization itself as a result of a cyberattack, as it is an internal matter to be dealt by the company's executives and shareholders. Nonetheless, if the economic damage is on a large scale and is liable to have affect the Israeli economy as a whole, state intervention should be considered.

The cyber resilience review

As mentioned, projects in the process of approval and, in certain cases, projects that are already in operation will be required to submit a cyber resilience review to the National Cyber Directorate, based on the questionnaire on potential cyber damage. Several guidelines can be proposed for the content of the cyber resilience review, as well as for the entities authorized to conduct and submit the review, such as external consultants, and the entities that will examine and approve it. From a statutory viewpoint, the contents of the cyber resilience review must be comprehensive and should apply to all requests for new projects, unless an exemption is granted by the relevant authority.

Once it is decided that an organization must submit a cyber resilience review, the process will be carried out according to the following milestones:

1. **Directions for the cyber resilience review.** The National Cyber Directorate will be responsible for preparing the instructions for implementing the review. These directions must be specifically tailored to the project or organization. The instructions should include a number of components, such as a mapping of the potential damage due to a cyberattack, mapping the weak spots of the project or plan, and means of minimizing the exposure and the damage.
2. **Preparation of the cyber resilience review.** The organization requesting the license will be responsible for preparing the review and for financing it. Reviews will be prepared using consultants chosen from a designated list of consultants who have been trained and authorized by the National Cyber Directorate. These consultants will work according to the instructions for preparing the review.
3. **Evaluation of the quality of the cyber resilience review.** The National Cyber Directorate will be responsible for evaluating the review. It can make use of external consultants who will be trained and authorized to evaluate cyber resilience reviews. The project developer will bear the cost of the evaluation. During this process, the National Cyber Directorate and the project developer may engage in several rounds of comments and responses to them.
4. **Approval of the cyber resilience review.** Authorized staff members from the National Cyber Directorate will evaluate and approve a cyber resilience review and will also issue further instructions to the organization that submitted the review. The approval may also set conditions for the granting of the business license, as well as instructions that will apply to the project developer's plans.

As mentioned, the Business Licensing Law constitutes a convenient platform for the regulation and implementation of directives for protecting against cyberattacks among existing organizations. However, the current extent of compliance with the law is insufficient and this issue is discussed below as part of the recommendations for implementation. In addition, due to the restrictions of information security and the leaking of information, this process should be defined as compartmentalized and not transparent to the public but rather limited to the purview of the authorized entities.

The stages of the proposed model are described in schematic form in Figure 7:

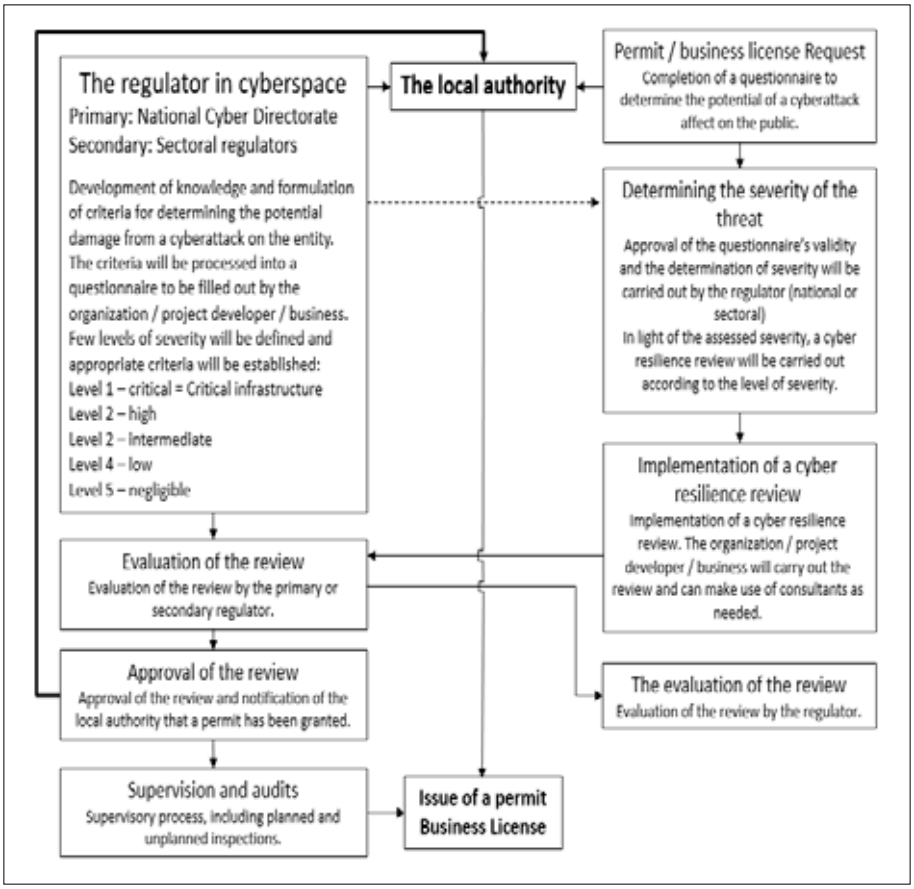

Figure 7: The proposed regulatory model for the business sector

According to Figure 7, the first stage is the request by the project developer or business owner to obtain a business license, during which a cyber vulnerability questionnaire will be filled out. Then, according to the decision of the cyber regulator (the primary national regulator, i.e., the National Cyber Directorate, which will operate in coordination with the secondary sectoral regulator or the government ministry for the relevant project to be licensed), the level of severity of a potential cyber threat will be determined and instructions will be issued for implementing a cyber resilience review. The review will be evaluated and approved at the end of the process by the sectoral regulator

in coordination with the National Cyber Directorate. This approval will constitute one of the conditions for obtaining the requested business license.

The advantages of the model rest first and foremost on the balance created between the need for deepening cyber protection and the desire for economic growth. The model uses the methodology of an environmental impact assessment, which has proven to be effective in dealing with polluters and provides a comprehensive and detailed mapping of potential risk. In addition, it involves a statutory, systematic, and mandatory process that will generate a comprehensive understanding of the potential threats to the organization. Israel's business sector is an inviting target for a potential cyberattack and therefore the systematic identification of business organizations is an important task. According to the proposed process, the assessment of businesses will cut across sectors, increasing the awareness of the dangers in cyberspace among business owners and the public in general.

The most significant disadvantage of the model is the reliance on the business licensing process, which is enforced at the level of the local authority. Since the directives issued by the local authorities are not state-level and not rigidly enforced, many businesses decide not to go through this regulatory process. Moreover, the business licensing process is dispersed among many regulatory agencies and requires significant time investment.[186] In order to deal with this situation, reforms have been instituted over the years and mechanisms for "temporary permits" and "fast-track permits" have been created in order to allow operations to continue until the completion of the process to obtain a full license.

As part of the attempt to impose cyber protection efforts on the economy in general, the proposed model calls for greater enforcement of the Business Licensing Law in Israel and for simplifying the process to obtain a business license. Regulation should be concentrated in one body within the Ministry of the Economy, which will operate efficiently and in coordination with the relevant regulators to provide approval for opening a business. At the same time, the experience in recent years shows that about 40 percent of businesses in Israel operate without a license,[187] a situation in which the

186 Levinson and Dror, "Environmental Regulation is Advancing . . . Backwards."

187 Shimon Ifergan, "40% of businesses in Israel operate without a Business License," *Mako*, December 27, 2012, http://www.mako.co.il/special-mako-news/Article-a434351304cdb31006.htm [Hebrew].

proposed model will be ineffective. Therefore, the regulatory process should be simplified and the Ministry of the Economy should be given the power to enforce the closing of businesses that do not meet the minimal conditions to receive a license.

Regulation of the chain of supply and its critical points

Binding regulation according to the proposed model will also include state intervention to protect important cyberspace resiliency points, which will yield significant benefit at low cost. An in-depth study of the primary and critical infrastructures in the economy will identify the important resiliency points upon which a critical mass of players in the economy relies. The rationale behind this is finding key critical points for which supervision will be beneficial for ensuring the national security. It is important to emphasize that the state will not intervene to protect these points; rather its role will be limited to identifying them and cooperating with the relevant suppliers in order to encourage them to acquire protection, based on the need and the desire to increase the resilience of cyberspace in Israel.

Examples of these points include principal suppliers in the supply chain, such as hosting services, which provide the infrastructure for a large number of internet services in Israel; application software and centralized information systems that manage the settlement of credit card activity, upon which most private businesses rely; integration companies (such as Teldor and Malam), which provide support for the information systems in most of the economy; the cash register systems of the Retalix company used by most food outlets; the Brinks company for the transportation of cash and on which the various banks rely; various applications for the management of bank accounts that are in use by the banks; and internet providers that provide access to global cyberspace.

After identifying these points, the state will need to employ third-party providers that will be responsible for the quality assurance of these critical service providers. The following sections will describe the principles on which this model rests, the way in which such points in the economy will be identified, and how the state should intervene in the model's implementation.

Identifying resiliency points in the economy: supply chains and other examples

In the world of information security, a vulnerability known as a "class break" can damage not just one system but all the systems that contain the weakness. Examples include a vulnerability in a widely used operating system or damage to a certain kind of camera through which it is possible to crash a large number of sites (as occurred in the attack on the US domain name service provider, Dyn, in October 2016).

A class break is not a new concept in the domain of risk management. Floods and earthquakes are examples of risks from the physical world that damage infrastructures and harm many individuals indiscriminately. These risks are usually handled through exclusions in insurance policies, since insurance companies are not interested in dealing with multidimensional damage that occurs simultaneously among many systems. Cyberattackers look for vulnerabilities in security in order to exploit them again and again, particularly when the attack targets one weak spot and uses a device through which it is possible to attack a wide variety of systems. It is important therefore to identify the class breaks at an early stage also in the domain of cyber regulation.

One of the clearest examples of weak spots with a potential to affect the entire economy involves the supply chains of service providers. The supply chains are a group of resources and processes that are connected to the suppliers, purchasers, and subcontractors needed in the process of developing, producing, handling, and delivering goods and services to various purchasers.[188] The system can be attacked through the supply chain at any stage in its life cycle and protecting against this eventuality has become increasingly complex. Numerous organizations rely on their various suppliers as being able to maintain the continuity of their operations although the suppliers may not be able to meet the security requirements required by the organizations that use their services. Furthermore, an organization may not consider the suppliers when planning its risk management.

188 Ram Levi and Ami Rojkes Dombe, "The Chain of Supply – the Quiet Cyber Threat," *Israel Defense*, February 19, 2014 [Hebrew].

According to an OECD report from 2013,[189] more than half of the products in the world are used for the production of other products. This figure manifests the widespread fragmentation of the production chains worldwide as a result of technological progress and the globalization of markets, resulting in risk to service providers all over the world. The characteristics of the supply chains make protection very difficult and constitute an advantage for the attacker: They are long, complex, interconnected, dispersed throughout the world, and have many logistic links. Their configuration is not static and they include various levels of outsourcing. From the perspective of the potential victim, the implication of these characteristics is the difficulty in understanding the components of each system and sub-system—together and each on its own. Furthermore, in the current global labor market, the various components of the same product could be produced in a number of countries and assembled at various locations, a situation that increases the number of weak points in the supply chain, rendering cyberattacks on them particularly worthwhile. For example, Microsoft uncovered an attack in 2017 that used the supply chain in order to attack targets in the financial sector. The attackers used an update of a third-party program whose update configuration was breached in order to obtain access to the target computers.[190]

The reliance on supply chains leads to two main threats. The first is a reduction in functionality due to the difficulty in verifying the quality of suppliers of services, hardware, and software. The second is an undesirable functionality; that is, the penetration of malicious code into hardware or software during production, which will be exploited when the hardware or software reaches its destination. Another possibility is the use of software developed at a low level, whose vulnerabilities can easily be exploited. Because of the high degree of complexity in analyzing the supply chain, discovering or exploiting its vulnerabilities is a lengthy process. Therefore, under the auspices of the state, an early mapping should be done of the major service providers and subcontractors, including classifying them according to the level of security to which they can commit. This model can be found

189 OECD, "Interconnected Economies: Benefiting From Global Value Chains – Synthesis Report," OECD, 2013, https://www.oecd.org/sti/ind/interconnected-economies-GVCs-synthesis.pdf.

190 For details on the attack, see the report of the National Cyber Directorate dated May 9, 2017, https://www.gov.il/he/departments/publications/reports/micro_finance [Hebrew].

in the requirements imposed by the state on building contractors, whereby the state gave every contractor a classification approved by the Registrar of the Ministry of Housing.[191] Such a classification should be established for service providers and links in an organization's supply chain, according to the potential damage that the supervised organization could cause to national security. The establishment of such a stamp of quality will lead to classifying the major service providers in the economy according to their level of security, which will assist service recipients in managing the cyber risk that results from the relationship with them. The creation of three or four rankings for suppliers will enable every organization to choose the appropriate subcontractors with whom to work. In addition, the creation of a ranking will obligate organizations to employ subcontractors according to the organization's field of activity.

Besides the regulation of the various services in the economy according to their level of cybersecurity, the state can intervene in other important areas in order to reinforce national resilience. One example is information security integrators whose job is to install information technologies and information protection in large organizations, and thus dominate the information security in most of the economy. Failure to implement an organization's security policy or install a security device in a non-optimal manner will lead to a "rolling" security failure and could cause major harm to Israeli cyberspace. The model proposes state intervention in order to verify the quality of integrators, based on the assumption that strengthening their status will increase security in Israeli cyberspace as a whole.

Another example is internet service providers serving as the conduit through which all users surf the internet. Most of the traffic in cyberspace flows through these providers and they are the gateway for both cyberattacks and attempts to protect against those attacks. Israel has advanced protection capabilities that are not used by the internet service providers market. The setting of rules for suitable protection of these providers—in a way that does not infringe on the privacy of their customers—would be an important step in reinforcing Israel's cyberspace.

Providers of web hosting suppliers constitute another important resiliency point in Israel's cyberspace. These companies provide hosting farms, and

191 See State of Israel, "Regulations for the Registration of Engineering Construction Contractors (Classification of Registered Contractors)," 1988 [Hebrew].

their servers host the numerous internet sites that service the citizens of the state. The server farms contain a massive number of internet sites and a failure of their security would likely cause a security failure in a large number of sites. Despite their importance, these server farms are currently secured according to the discretion of the hosting companies. There is a lack of transparency in the way that these farms are secured and there is no ranking that classifies the various levels of security that they provide to their customers; furthermore, this weakness is poorly dealt with—if at all—despite its importance. Introducing standards for the hosting of internet sites will significantly increase their resilience and will reduce the ability of hostile elements to exploit vulnerabilities in order to harm Israel's citizens.

State intervention at the economy's important resiliency points

After identifying the critical resiliency points that affect the entire economy, the state needs to classify them into categories and to verify the support and quality control of the services they provide. The state's intervention should be carried out by international cooperation with relevant standards organizations, by the sectoral regulator, and by third-party suppliers that have the capability of verifying the quality of the service offered. Thus, for example, integrators and information system supporters will need to undergo periodic training and certification tests under state supervision in order to remain up-to-date on the evolving threats and the latest security products. Training and certification tests can be carried out according to the existing ISO or ISACA standards, which are revised from time to time.

Critical systems that dominate a particular sector are another example of where the state needs to intervene. Examples include the ATMs, bank account management systems, and payment settlement systems. These systems will be examined according to the most advanced international standards, such as those of the American National Standards Institute, and according to the accumulated knowledge gained from previous cyberattacks on such systems.

The sectoral regulator will also play a part in this effort. Thus, for example, in the case of systems for information sharing in the insurance domain, systems for the trading of securities, or salary systems, the sectoral regulator will examine parallel systems in other countries and will employ third-party suppliers as needed in order to verify the security of the Israeli systems. This way the state will choose the sensitive locations in the various sectors

where it needs to ensure that the level of cybersecurity is sufficient, while avoiding the sweeping regulation of all the sectors in the economy.

One of the main disadvantages of this model is the creation of a class of "winners." According to the model, the state selectively chooses to ensure the quality of the systems that already have a strong presence in the economy, while it discriminates against their competitors. Nonetheless, the value of competition should be secondary in importance to functional continuity and to endangering national security as a result of damage to the systems chosen by the state. Therefore, the advantages of the proposed model outweigh its disadvantages on this count.

Incentive-Based Regulation

Cyber insurance based on mandatory reporting

The entry of insurance companies into the cybersecurity market will be an incentive for companies in the market to protect themselves and for insurance companies to reduce the prices of their insurance policies. A flourishing insurance market, however, must be based on statistical models that are fed by actual data on cyber events and actual risks. Therefore, the creation of such an insurance market requires binding regulation that will ensure transparency in a cyber event or at least the creation of an actuarial database that will meet the needs of the insurance companies. Currently no such transparency regulations exist, thus preventing the development of a cyber insurance market that would be beneficial to the entire economy.

There is no obligation to report cyber events in Israel, except for breaches of databases. Theft of user names, spying, or demands for ransom do not require any reporting. Compared to other countries, the low frequency in which Israeli companies report cyberattacks suggests that most cyber events in Israel are not reported and remain within the confines of the targeted organization. Documents of the National Cyber Security Authority[192] indicate that in 2017 there were one hundred breaches of organizations in Israel each month. These numbers are inconsistent with what is reported to the public and indicate a lack of transparency in this area. Furthermore, even if the National Cyber Directorate receives information about a cyber breach

192 The National Cyber Security Authority, "Summary of the Founding Years 2016–2017," 2018, https://www.gov.il/he/Departments/news/summary [Hebrew].

from a specific company, it is not authorized to force an investigation on the company nor does it have any enforcement powers, as does the Israel Police.[193]

The lack of public transparency has significant implications for the resilience of cyberspace in Israel. Companies and organizations that are not required to report choose to maintain secrecy in the case of a cyber event and believe that their reputation will not be harmed as a result. As mentioned, the lack of public transparency also makes it difficult for insurance companies to accumulate actuarial information that can be used to price cyber protection insurance policies. The existence of a cyber insurance market would allow heavyweight players, i.e., insurance companies, to join existing stakeholders with an interest in the protection of the various organizations. As in the auto market, where insurance companies have encouraged the installation of safety measures, organizations that want to insure themselves against cyber events will be required to adopt measures to improve their cyber protection, which they would not have adopted otherwise.

The proposed model seeks to achieve public transparency for medium to large-scale cyber events and in this way to encourage the creation of a cyber insurance market. The reporting need not be simultaneous with the response to the event, but once the event has been addressed to a reasonable degree, the media should report it to the public. Such reporting should include details about the channel of penetration and the harm caused (if any) to customers' privacy. Mandatory reporting should be accompanied by appropriate compensation for the loss of information or the damage to privacy as a result of the cyber event. At the same time, the supervisor of insurance and the capital market should design a uniform cyber insurance policy for the various insurance companies, which will enable small and medium-sized businesses to also acquire a policy that will cover the compensation of their customers in the case of a cyber event.

Mandatory reporting and the creation of an active insurance market that will also include small and medium-sized businesses will significantly increase the incentive of organizations to protect themselves in cyberspace. When a business' reputation is on the line and companies with a solid financial base, such as the insurance companies, are interested in protecting against

193 Rafael Kahan, "Hacker? We'll Manage on our Own: Industry in Israel does not Believe in the Cyber Regulation System," *Calcalist*, June 28, 2017, https://www.calcalist.co.il/internet/articles/0,7340,L-3716104,00.html [Hebrew].

cyberattacks, the resilience of Israel's cyberspace is expected to strengthen. In this context, it is worth mentioning that the National Cyber Directorate is considering ways to bridge the gaps in the realm of cyber insurance and to facilitate the creation of a cyber insurance market in Israel.

Tax breaks for cyber protection

The acquisition of cyber protection products is an expensive prospect. Companies choose certain protection products over others in no small part due to cost considerations. The state and the Tax Authority should encourage the purchase of cyber protection products by providing tax breaks and reducing the price of the products for organizations. The tax breaks will be provided according to the protection measures that are already in place in the various organizations, enabling them to create multi-layered protection. For example, organizations that already possess products for network protection but do not have a solution for end stations will receive tax breaks for purchasing end products; however, they will not be eligible for tax breaks on products for network protection. In other words, organizations' cybersecurity posture will be reported to the tax authorities in order to determine the type of incentive to be provided.

Sharing of information within a sector and between sectors for the purpose of cyber protection

The sharing of information in cyberspace is becoming an increasingly common practice in Israel. The National Cyber Directorate, together with the various government ministries, is working to establish sectoral event monitoring and management centers that will improve operational and decision-making mechanisms and will thus reinforce national resilience. However, information sharing on a day-to-day basis occurs for the most part via a third party, i.e., the sectoral regulator, rather than directly between the various organizations that belong to the same sector and compete with one another.

Information sharing is highly important in cybersecurity. It is one of the strategic foundations of cybersecurity and its objective is to reinforce overall resilience in cyberspace.[194] Information sharing for the purpose of cyber

194 Gabi Siboni and Hadas Klein, "Challenges of Information Sharing in the Intra-Sectoral Environment," *Military and Strategic Affairs* 8, no. 1 (July 2016) [Hebrew].

protection includes information on existing cyber weaknesses, methods of attack and concrete threats in the domain, identification of attackers, and attempts to ascertain the motive behind the attacks. The goal of sharing is first and foremost to prevent the threat from spreading and therefore it usually occurs on an intra-sectoral basis, although inter-sectoral sharing can also play an important part in strengthening protection in cyberspace. The advantages of information-sharing practices are that they shed light on the entire life cycle of a cyberattack—from the early stages of intelligence gathering to the practical stage of employing active defense measures. Information sharing makes it possible to update and enhance deterrent mechanisms in order to enrich prevention efforts, improve efforts to detect attacks, and create better responses, including learning from others' experiences. Nonetheless, information sharing is not a widely accepted practice among commercial companies and states. Competing companies are afraid to cooperate in order not to harm their business interests while states are not enthusiastic about sharing valuable intelligence information, based on, among other motives, the desire to preserve their relative advantage.

Studies show that companies are afraid of receiving low-quality information and of harming their reputation should they reveal that they were attacked, as well as not wanting to aid their competitors. As a result, companies refrain from consistently sharing information. Inherent problems in the sharing of information among many players include the lack of reciprocity and the competitors' using information they received for their own benefit while they themselves do not share information.

Every model of information sharing includes information producers and information consumers. As part of the proposed model, effective information sharing in cyberspace will depend upon a central authority that will manage the distribution of information to the other consumers. The creation of an information-sharing center will make it possible to centralize decision making, which will go beyond the narrow business interests in each sector, and thus will advance cybersecurity as a top priority. One example is the activity of companies that provide cyber protection services at various levels—from protection of end stations and networks to the installation of monitoring and control products. These companies rely on databases that constitute the raw material at the core of their products. Information sharing between these companies will significantly improve all cyber protection products, although it is liable to strengthen one player at the expense of another.

Another barrier to information sharing in the private sector and even more so in the public sector is the desire to possess knowledge and therefore to become or remain a significant player in the decision-making processes. Issues of sovereignty over information, the entrenchment of a particular organizational culture, asymmetry between information sharers, and the lack of incentives to share discourage organizations in both the private and public sectors from sharing information related to cyber threats.

The United States has sought to encourage information sharing between the various sectors and is increasing its efforts in this direction. The Department of Homeland Security created forums called Information Sharing and Analysis Centers (ISACs) in the various sectors following the September 11 attacks. Organizations decided to join them based on the understanding that information sharing is an essential component of national security. These forums are supported technologically and economically by the state, and they enable the sharing of knowledge with relative convenience, particularly when a company's line of business is not related to cyberspace.

The National Cyber Directorate in Israel is working to eliminate bottlenecks in this domain and especially seeks to raise the level of knowledge sharing between the various players. The vision is to create a forum, headed by the Director of the National Cyber Directorate, that will deal with significant cyber events and will decide on issues raised in other knowledge-sharing forums. Another project of the National Cyber Directorate is the creation of mechanisms for cooperation in the financial sector and in the energy sector, by means of cooperation and involvement of all the relevant players. In order to encourage information sharing of this type, the model proposes incentives that will make it possible to expand upon what already exists.

Chapter 5
Recommendations for Implementing the Proposed Model

There are numerous challenges in implementing the proposed regulatory model, due to the difficulty in changing existing systems and arrangements, the conflicts between the various interests in designing a public policy in this realm, and the existing institutional structures that oppose change and reform. Each body is interested in controlling the means of supervision, since the regulation of cyberspace translates into economic power and influence. It can be assumed that existing bodies will find it difficult to accept the new rules of the game.

In addition, each supervisory body has different interests and each would like to have the decision-making authority on cybersecurity issues. These interests, in most cases, create power struggles and, as a result, they are pressured to design public policy in a certain direction. The institutions and arrangements in the model, such as the Business Licensing Law, have existed for a long time but are not sufficiently effective. Implementing the model proposed here will provide them with additional power and authority that they do not currently possess.

This chapter presents recommendations for implementing the model proposed here for cyber regulation. The recommendations are divided according to the various layers of the model: self-regulation, binding regulation, and incentive-based regulation, with the intention of outlining concrete steps that will allow decision makers to successfully introduce the new regulations. It should be noted that all the recommendations are new and not currently implemented in the Israeli economy.

The Self-Regulation Model

Recommendation: To consider the need to develop a professional and independent supervisory body within the National Cyber Directorate, which will operate among the organizations that are currently within the framework of self-regulation (organizations in the defense establishment, the IDF, the Israel Police, and so forth).

These organizations should be exposed to knowledge that is being developed in the National Cyber Directorate and in the civilian market. It is recommended that a designated body be created that will facilitate knowledge sharing and the assimilation of advanced approaches to cyber protection among these organizations. This designated body will employ top experts and will constitute the knowledge-sharing arm of the National Cyber Directorate, which will operate discretely among sensitive organizations and will assist them in verifying the quality of cybersecurity in their systems. This recommendation also applies to the DSDE, which will benefit from the development of knowledge in the National Cyber Directorate and in the civilian sector.

The Binding Regulation Model

The binding regulation model is divided into several components and concrete and specific recommendations are presented for each of them.

Binding regulation by way of sectoral regulators

Recommendation: The creation of a forum within the National Cyber Directorate that will help to create an overall picture of the regulatory techniques used by the government ministries and authorities to supervise cybersecurity in the sectors under their responsibility.

The review of the literature revealed a variety of techniques used by the government ministries and authorities in the regulation and supervision of various sectors in the economy. The regulation and supervision will be carried out by means of circulars by the director general and binding directives (as in the case of the Bank of Israel and the Capital Market Authority); by means of regulatory intermediaries in the form of private companies (as in the energy domain); or the creation of a designated branch to provide solutions to supervised organizations (as in the Ministry of Health). While these are all worthwhile regulatory techniques, it is recommended that a designated body in the Government ICT Authority take a leading role in

monitoring their quality and relevance, in order to create cross-pollination and advance the overall regulatory effort.

Binding regulation in the granting of a business license

This is one of the main components in the development of cybersecurity regulation in Israel. Its implementation does not require special legislation, but it can be applied as part of the existing Business Licensing Law (in line with the ruling of Judge Cheshin in the lawsuit brought by the state against the Tnuva company).[195] It may be sufficient to apply a government decision that pertains to the Business Licensing Law also to the cybersecurity domain, in accordance with the model proposed in this essay. In this context, a number of concrete recommendations are suggested:

Recommendation: Increased enforcement by the Ministry of the Economy and the Ministry of the Interior in order to improve compliance with the Business Licensing Law in Israel.

The proposed model, which is based on the Business Licensing Law as a binding statutory mechanism, will be effective only if its enforcement is strengthened and its compliance is improved. To this end, a single entity should be authorized to enforce the law and it should do so with greater determination, in order to create deterrence among companies and private businesses that operate without a license. Once the Business Licensing Law is enforced in the entire economy equally, the proposed systematic process can reach its maximal potential.

Recommendation: Creation of an executive arm in the National Cyber Directorate that will supervise cyber resilience reviews for the entire economy.

The National Cyber Directorate will develop knowledge on how to complete a questionnaire and a cyber resilience review, based on the accumulated knowledge in Israel and around the world. The review will need to include a solution for all the evolving threats in cyberspace so that it will remain relevant for new businesses and so not to become a burden on industry.

Recommendation: Standardization of cyber professions.

Since the use of the questionnaire and the cyber resilience review will increase the demand for cyber experts and consultants, it is recommended that the various cyber professions be standardized. It is especially important that consultants be able to provide a solution in the form of a cyber resilience

195 State of Israel vs. Tnuva.

review and encompass all the cyber risks resulting from the organization's activity and its interfaces. A cyber consultant will receive official certification from the state and it should be validated annually so the consultant can remain up-to-date on threats and the methods for carrying out reviews in other countries.

Regulation of critical resilience points in order to improve national resilience in cyberspace

Recommendation: The creation of a forum that includes the National Cyber Directorate, the Government ICT Authority, and technological leaders in the economy in order to identify, analyze, and protect critical points and thus strengthen national resilience.

State intervention at critical points in order to improve the resilience of cyberspace requires a clear mapping of all major infrastructures in the economy and the way in which localized intervention can be beneficial or detrimental to economic activity. Such a mapping requires technological knowledge and familiarity with the technological landscape of the Israeli economy across sectors. A joint forum of the National Cyber Directorate, the Government ICT Authority, and the private sector will provide technological knowledge on the one hand, and an intimate familiarity with the government ministries, the supervised sectors, and the economy in general on the other. After identifying the anchors in the industries, a survey should be conducted of developments in parallel industries in other countries, including what can be learned from them and how to better protect the anchors in these industries.

Incentive-Based Regulation

Encouragement of cyber insurance on the basis of mandatory reporting

Recommendation: Promoting a law that requires all entities in the economy to report a major cyberattack.

The proposed law will provide clear criteria for defining a "major" cyberattack, which will be based on the amount of information stolen and its sensitivity and on the question of whether and to what extent it was encrypted. The law will require reporting to the National Cyber Directorate, the provision of compensation to customers who were harmed, and notification to the public once the organization is out of danger. Such a law will incentivize organizations to protect themselves at an early stage since their reputation

will be on the line and also will generate a flow of actuarial information to the insurance companies, which will help them price cyber insurance policies.
Recommendation: Allocation of a designated government budget to the Capital Market, Insurance and Saving Authority in order to provide a state guarantee to insurance companies in the case of a large-scale cyber event.

The government needs to provide a guarantee to the insurance companies in the case of a large-scale cyber event in order to encourage them to provide policies against cyberattacks at competitive prices. The allocation of a designated budget will make it possible to establish clear criteria for a cyber event, which will allow insurance companies to rely on the government guarantee in order to provide compensation to organizations that suffer damage in such an event. The state guarantee will reduce the risk in issuing cyber insurance policies and is expected to incentivize the insurance companies to enter this market.

Tax breaks for cyber protection

Recommendation: The government will weigh the possibility of providing tax breaks for the installation of sufficient cyber protection.

The Ministry of Finance will consider introducing tax breaks for companies in the economy that achieve a sufficient level of cyber protection. It will define the criteria for granting the tax breaks according to the organization's level of protection and its scope of activity in the economy. A wider scope of activity and a higher level of protection will lead to a higher tax break.
Recommendation: Creation of a designated cyber unit in the Tax Authority.

The cyber unit to be established in the Tax Authority will be able to examine and rank the level of protection of an organization requesting a tax break for the installation of cyber protection measures. The development of expertise in the cyber domain within the Tax Authority is expected to create healthy competition between the various companies over eligibility for tax breaks in exchange for cyber protection and will thus strengthen national resilience in this domain.

Intra-sectoral and inter-sectoral sharing of information for purposes of cybersecurity

Recommendation: Promotion of legislation to provide an exemption from responsibility in the event of a cyberattack and an exemption from antitrust

regulation in the case of inter-organizational sharing of information on threats in cyberspace.

Legislation like that passed in the United States in December 2015 will encourage information sharing in order to facilitate pro-active defense against cyber threats. In addition to the current efforts to establish sectoral information-sharing centers, legislation will make it possible to obtain an overall picture of the cyber threat in the Israeli economy at any given moment. Companies will have an interest in sharing as much information as possible so that they will be exempt from responsibility should a cyber event occur after having adopted protective measures as a result of analyzing the threats that were shared.

Conclusion

The survey and analysis of developments in Israel and worldwide regarding the effort to strengthen cyber protection indicates that the regulation of this domain is expanding and developing rapidly. The centrality of cyberspace in modern society, together with the security challenges it creates, have led many Western countries, including Israel, to expand their activity in this domain, to allocate significant resources to it, and to update institutional structures in order to handle new challenges. At the same time, the business-civilian sector remains largely unregulated and the incentives for it to strengthen its cyber protection are neither comprehensive nor sufficiently attractive. Market forces prefer innovation and technological development over information security and data protection and states' regulatory systems have not managed to change this status quo.

In recent decades, state systems have been involved in managing and eliminating risks to society in numerous facets of life, such as transportation, environmental protection, finance, and safety. In contrast, an effective strategy has not yet emerged to significantly reduce cyber risks and prevent threats to national security. The regulatory model proposed in this essay seeks to address this challenge by taking an interactive approach to cyber risks. The model relates to Israel's cyberspace in its entirety by suggesting a formal methodology for managing cyber risks across the various sectors of society, including by applying a variety of regulatory types—self-regulation, binding regulation, and incentive-based regulation. The three categories of regulation are meant to provide a multi-layered solution to the regulatory challenge that cyber poses.

Self-regulation, according to which sensitive security organizations regulate themselves, will be under the periodic oversight of an external entity, established within the National Cyber Directorate as a professional and independent oversight body. A designated government decision will require self-regulated organizations to undergo a periodic external audit and

will facilitate supervision of how the most sensitive security organizations protect themselves. The challenge in achieving this supervision is the potential opposition of the organizations themselves, which are not used to being subject to external oversight. Such opposition is liable to intensify institutional friction and to weaken the oversight activity.

Binding regulation, which primarily involves the regulation of critical infrastructures and government ministries as well as the business sector, will be implemented in three ways:

1. Reliance on the sectoral regulator that implements the regulation and supervision of the activity under its responsibility, including the creation of a forum across sectors that will oversee the ways in which government ministries regulate the private sector and the various regulatory techniques they employ. The main challenge implicit in the horizontal view taken by sectoral regulators is the complexity of each regulator's activity. Each government ministry has accumulated expertise in its own jurisdiction; the desire to create an oversight group that will supervise and direct the work of the sectoral regulators is liable to encounter resistance in the existing authorities and will also face the challenge of recruiting human capital with appropriate expertise.
2. The creation of a new statutory process, by means of the Business Licensing Law, in order to identify potential threats to national security as a result of a cyberattack on the business sector. In this context, a cyber resilience review will be carried out in the private sector, using a questionnaire that describes the potential damage implicit in the activity of each business organization. The executive arm of the National Cyber Directorate will supervise the implementation of the review as well as consultants who will operate according to professional standards and will undergo periodic certification. These consultants will assist organizations in filling out the reviews, including the description of all potential threats. The challenge in using the Business Licensing Law lies in the weakness of the law within the Israeli regulatory culture. Thus, compliance with the law has eroded significantly over the years and in order for it to be effective, the responsibility for its implementation needs to be concentrated in one ministry (the Ministry of the Economy), which will also be responsible for achieving greater enforcement.
3. Mapping of critical points in the Israeli economy, which have a decisive influence on cyber national resilience, in order to create state intervention

to raise the level of protection at these points. A double challenge arises in such an undertaking: First, identification of critical points is liable to be a complex task and will require an in-depth horizontal perspective of the Israeli economy; and second, the manner of intervention is liable to be such that it will prioritize players with a dominant status in the economy and will thus hinder competition from other players that are seeking to challenge their position. State intervention will, in this case, need to be implemented with sensitivity, while considering all the existing interests and will need to adopt complete transparency vis-à-vis the method of intervention and the relative advantage that it provides to dominant players.

Incentive-based regulation is intended to encourage market forces to invest more in cybersecurity. This type of guidance is based on the following components:

1. There is a need to create a cyber insurance market, which will require legislation for mandatory reporting and transparency regarding cyberattacks on organizations and the allocation of a government budget to the Capital Market Authority in order to provide guarantees to insurance companies in the event of a mass cyber event. The challenge that arises here is the reluctance of companies to fulfill the requirement of mandatory reporting, partly due to the fear of harming the company's reputation. Not revealing that a cyberattack has occurred enables a company to conceal the very existence of any resulting damage. The exposure of cyberattacks is liable to constitute a fatal blow to the activity of small and medium-sized businesses. Insurance policies with a state guarantee should be created for these cases, which will allow small and medium-sized companies to endure the damage.
2. Tax breaks should be instituted for expenditure on cyber protection. This is to be accomplished by means of a designated unit to be created within the Tax Authority, which will examine organizations' requests for tax breaks in the case that they prioritize cybersecurity and provide a high level of protection to their customers. The challenge in providing tax breaks for cyber protection is the need to develop technological knowledge within the Tax Authority, which will allow it to evaluate the requests and to rank companies requesting a tax break. Determining whether a particular cyber infrastructure is secure will be a difficult task. The Tax Authority will

have to set clear criteria and will need to rely on international standards in order to create a cyber performance model for the various companies.

3. Exemption from responsibility should be provided in the case of intra- or inter-sectoral sharing of information on organizational cyber threats, in order to allow pro-active defense in this domain. The challenge in this case is to maintain the privacy of the companies' customers. Encouraging information sharing between the business sector and the public sector is liable to generate a flow of information that will allow the state to become intimately familiar with the activity of the companies' customers, such as in the internet service providers (ISPs) market. The state must fully anonymize the information that it receives. This is a complex challenge, but the benefit of doing so outweighs the cost and will enable pro-active defense in cyberspace.

At the beginning of this study, we asked four research questions. The first concerned the laws and institutions on which the State of Israel currently bases its efforts to protect cyberspace. In practice, since the 1990s, the State of Israel has invested in protecting critical state infrastructures. Since the beginning of the 2000s, government ministries and authorities of sensitive sectors of the economy, such as health and finance, have engaged in localized and sectoral regulation. In the current decade, Israel has been centralizing the decision-making process and has chosen to manage the cyber challenge through a single sovereign entity, namely the National Cyber Directorate. Israel has emphasized the resilience of the economy, cyberspace, and national security. Even after Israel has taken these steps, it still lacks an overall and formally-stated strategy for protecting the civilian-business sector, despite steps in this direction.

The second question was how other countries implemented cyber regulation in the business-civilian sector. The survey of the literature indicated that other countries took various approaches to cybersecurity and that their regulation of cyberspace has been usually a patchwork affair. Critical infrastructures are still considered as the main sector at risk and attention to cybercrime prevails, in parallel to building institutions and decision-making processes increasingly centered around a single government agency. Furthermore, in the countries surveyed, a lack of attention is paid to the business sector, except for localized entities that provide incentives by means of labels and certification.

The third question focused on what could be learned from the regulation of other domains, such as environmental protection and nuclear energy, vis-à-vis the cyber regulation of the business-civilian sector. The survey of environmental protection suggested a holistic approach that considers the short- and long-term effects of the potential risks. Similarly, it indicated the importance of incentives as a factor in encouraging the assimilation of standards in order to eliminate risks to the private sector. Centralizing the decision-making process in a single entity will also positively affect the working relations with the private sector and reviewing the risks to the economy will assist in assessing and mitigating risk at an early stage.

The regulation of nuclear energy sheds light on cooperation between industry and the state in creating knowledge centers that help promote security. In addition, the existence of comprehensive compensation mechanisms in the case of a major attack indicates the potential for developing a cyber insurance market, in which the sale of cyber insurance policies will incentivize the business sector to protect itself. Finally, like in the nuclear energy sector, the granting of licenses in cyberspace can be used to encourage organizations to protect themselves.

The fourth and final question sought to identify a possible model for the regulation of cybersecurity in the business-civilian sector in the State of Israel. Based on the gaps in the literature and the insights gained from regulation in other domains, we have proposed a multi-layered model of cybersecurity regulation in Israel. The proposed model seeks to combine the need for economic development and the increasing activity in cyberspace on the one hand and the maintenance of national security on the other, based on regulatory tools borrowed from the field of environmental protection, particularly the cyber resilience review. Similarly, the identification of the main anchors that significantly influence the economy as a whole, as proposed by the model, will directly reinforce the resilience of cyberspace in Israel and will strengthen Israel's national security. The proposed incentives, some borrowed from the fields of environmental protection and nuclear energy and some innovations of this model, seek to encourage transparency regarding cyber events and to create an efficient cyber insurance market in order to distribute the risk in this domain. Similarly, the model advocates tax breaks for sufficient cyber protection to bring about changes in the current situation in which the market forces operate.

The regulation of cyberspace, like the organizational practices of cyber protection, is a multi-layered effort that relates to a variety of sectors and requires that attention be given to the uniqueness of each sector on the one hand and the need to systematically consider the potential risks facing all sectors on the other. This is a model that, for the first time, gives high priority to the business-civilian sector and the structure of joint work processes. This is likely to reinforce the resilience of cyberspace and significantly differs from the current regulatory regimes.

The proposed model becomes even more important given the calls for active self-defense in the business sector. In a situation of insufficient protection, growing threats, and high costs of protection, voices are calling on the state to allow private companies to hack back when it is possible to identify the source of an attack. Moreover, the lack of regulation in this domain creates a vacuum that allows companies to accelerate the arms race in cyberspace. The advantages of the proposed model include a change in the balance of incentives that is currently perceived as overly rewarding for attackers; a reduction in the government's burden of response; and a decrease in attacks and the minimization of potential damage to the business sector. At the same time, such an approach is liable to create friction and escalation between various organizations due to the built-in asymmetry in their capabilities for active defense and may lead to the hiring of "mercenaries," who will make cyberspace even less secure than it is today.

The dilemmas in this domain include where to draw the boundaries of this activity (if they are to be drawn at all), particularly when the lack of a regulatory solution leads companies to adopt initiatives involving active defense, even without explicit authorization.[196] A balance is needed between the benefit and damage from such activity, as well as an analysis of its short- and long-term consequences. The goals of active defense are to deter low-level hackers, to assist in the investigation of events (including the introduction of tokens monitored for theft), and more generally to encourage more active steps, beyond simply an in-depth investigation following an attack. The fact that companies are seriously considering adopting such a practice indicates the gap that has emerged in regulating the business-civilian

196 Wyatt Hoffman and Ariel Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?" Carnegie Endowment for International Peace, 2017.

sector in cyberspace and the need to come up with other solutions, beyond the conventional regulatory efforts.

In conclusion, with the creation of the National Cyber Security Authority in 2015 and the consolidation of all the agencies involved in cyber in Israel within the framework of the National Cyber Directorate in 2018, as well as the accumulation of expertise on cyber issues across numerous sectors, the conditions are ripe for adopting a new regulatory model that will take an in-depth look at the players in the economy and will make it possible to identify and eliminate cyber risks. The challenges to the model proposed in this document are strengthening the Business Licensing Law and increasing compliance with it, as well as adapting the model to the new regulatory challenges.

Artificial intelligence and the self-learning abilities of interconnected systems in the Internet of Things era create challenges for decision makers. In order to deal with these challenges, a regulatory model is needed that provides effective cyber protection. As the decision-making processes and the state's infrastructures gradually become entirely digital, any regulatory model will have to promote the public interest in cyberspace more intensively, even at the price of conflict between various stakeholders. The public interest includes the preservation of information security, functional continuity, national security, commercial secrecy, and the privacy of users across all strata of the information society.

INSS Memoranda, June 2018–Present

No. 190, April 2019, Gabi Siboni and Ido Sivan-Sevilla, *Regulation in Cyberspace.*

No. 189, March 2019, Carmit Padan and Vera Michlin-Shapir, *National Security in a "Liquid" World* [Hebrew].

No. 188, February 2019, Carmit Padan and Meir Elran, *The "Gaza Envelope" Communities: A Case Study of Societal Resilience in Israel (2006–2016).*

No. 187, February 2019, Dan Meridor and Ron Eldadi, *Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later*.

No. 186, December 2018, Udi Dekel and Kobi Michael, eds., *Scenarios in the Israeli-Palestinian Arena: Strategic Challenges and Possible Responses.*

No. 185, December 2018, Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges* [Hebrew].

No. 184, November 2018, Gabi Siboni, Kobi Michael, and Anat Kurz, eds., *Six Days, Fifty Years: The June 1967 War and Its Aftermath*.

No. 183, October 2018, Meir Elran, Carmit Padan, Roni Tiargan-Orr, and Hoshea Friedman Ben Shalom, eds., *The Israeli Military Reserves: What Lies Ahead?* [Hebrew].

No. 182, August 2018, Dan Meridor and Ron Eldadi, *Israel's Security Concept, The Committee Report on Formulation of the Security Concept* (Meridor Committee), Ten Years Later [Hebrew].

No. 181, August 2018, Avner Golov, *The Israeli Community in the United States: A Public-Diplomacy Asset for Israel*.

No. 180, August 2018, Gabi Siboni and Ido Sivan Sevilla, *Cyber Regulation* [Hebrew].

Special publication, July 2018, Udi Dekel and Kim Lavie, eds., *A Strategic Framework for the Israeli-Palestinian Arena* [Hebrew].

No. 178, July 2018, Carmit Padan and Meir Elran, *Communities in the Gaza Envelope – Case Study of Social Resilience in Israel* (2006-2016) [Hebrew].

No. 177, June 2018, Yotam Rosner and Adi Kantor, eds., *The European Union in Turbulent Times: Challenges, Trends, and Significance for Israel.*

No. 176, June 2018, Udi Dekel and Kobi Michael, eds., *Scenarios in the Israeli-Palestinian Arena: Strategic Challenges and Possible Responses* [Hebrew].

The resilience of the private sector in the world of cyber has a decisive impact on national security. This sector is usually the weakest link through which cyberattacks develop and serves as a springboard for attackers who are interested in harming state targets. In addition, built-in market failures lead to a lack of sufficient organizational investment in proper cybersecurity.

Negative externalization of cyber damage in organizations, the difficulty in quantifying the benefit of investing in cybersecurity, the lack of responsibility of software and hardware providers for their products' security vulnerabilities, and a competitive market that rewards innovation and progress over proper cyber protection create a gap that requires state intervention.

A review of cyber protection regulation regimes in the Western world reveals a lack of systematic solutions for the business sector and a gap in mapping out national security threats that could result from potential cyber damage in this sector.

This memorandum, which is based on world events in the field of cyber and in other areas of regulation, offers a multi-layer regulatory model for cybersecurity in the private sector. The memorandum suggests an integrated model for a state regulatory alternative that includes mandatory regulations, the creation of monitoring mechanisms for supervising self-regulation, and providing incentives for encouraging organizations to protect themselves. In an era of widespread use of linked devices, the entry of artificial intelligence into all aspects of life, and the creation of an insurance market for cybersecurity, regulating the business sector is a vital national interest.

Gabi Siboni is the director of the Military and Strategic Affairs research program, director of the Cyber Security research program, and editor of the journal *Cyber, Intelligence, and Security* at the Institute for National Security Studies, which he joined in 2005. During his military service, he served as a combat soldier and commander in the Golani Brigade, and in a variety of positions in the reserves, including deputy commander of a logistics regiment and head of staff of a division. As part of his work in the IDF, Dr. Siboni is the chief methodologist of the center for directing the buildup of military force—the conceptual lab. Dr. Siboni has a BA and MA in mechanical engineering from Tel Aviv University and a PhD in geographical information systems (GIS) from Ben-Gurion University. Dr. Siboni serves as an adviser in a variety of areas, including military technology, water and environmental engineering, cyber threat management, and computer systems.

Ido Sivan-Sevilla is a former Neubauer research fellow in the Cyber Security program at the Institute for National Security Studies where he implemented research methodologies based on big data. He has a BA in computer science from the Technion and is a doctoral student in public policy at the Hebrew University and carries out comparative research of government structures for managing cyber risks. Mr. Sivan-Sevilla has extensive experience in cybersecurity from the Prime Minister's Office, the Air Force, and the private sector. He was a Fulbright Scholar and served as a legislative researcher at the US Congress in Washington, DC.

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב