Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations

Gabi Siboni and Ido Sivan-Sevilla

The cybersecurity challenge cuts across fields, sectors, and approaches. This essay presents the fundamentals of the problem, embraces a risk-based approach that perceives the state as society's risk manager, and overviews the development of regulatory processes in modern societies. The essay then compares how the United States, European Union, and Israel have chosen to confront the cybersecurity challenge and stresses the importance and difficulties of imposing cybersecurity regulation on the civil sector. Finally, the essay explores some possible avenues for progress and suggests some solutions for increasing the resilience of cyberspace in the civic sector.

Keywords: regulation, risks, cybersecurity, civic sector

Introduction

Cyberspace poses various challenges on decision makers. These challenges stem primarily from the heavy dependence of states and societies on such a vulnerable sphere. While cyberspace enables the flow of information, which, in most cases, leads to economic prosperity, efficiency, and social benefits, it is also a target for national security, criminal, and commercial

Dr. Gabi Siboni is the director of the Cyber Security Program at the Institute for National Security Studies. Ido Sivan-Sevilla is a research fellow in the Cyber Security Program at the Institute for National Security Studies.

threats. The challenges to the resilience of cyberspace[1] are rooted in several key factors. First, there is an obvious asymmetry between the minimal obstacles of hackers to penetrate cyberspace and the high costs of defending it. While a successful attack needs only a single vector to advance, defense efforts aspire to cover all possible vulnerabilities. Second, cyberspace relies on outdated communications protocols, allowing attackers a great deal of anonymity and making it difficult for law enforcement agencies to identify the source of the attacks.[2] Third, cyberspace allows potential attackers to exploit the numerous hardware and software weaknesses and to use existing attack tools that succeeded in previous attacks; this phenomenon accelerates the race to defend oneself, further eroding the security level. The existence of a flourishing market to exploit zero-day weaknesses only stresses this point.[3] Furthermore, recently it transpired that commercial entities have shared software weaknesses and attacks tools with governments to facilitate spying on citizens and "regime opponents."[4]

Fourth, the lack of mechanisms to share information about cyberspace threats and the means of defense employed by commercial companies make it difficult to formulate a collective, proactive effort to prevent cyberattacks. This stems primarily from only partial information sharing and limited transparency of commercial companies in the civic sector,[5] while both the military and the state sectors fail to do their part. Fifth, there is a lack of economic incentives and technological tools to develop appropriate defense. While cyberspace damage—currently estimated in the billions of dollars—incentivizes market forces to defend themselves, most of the civic sector is not required to report data breaches and cyber threats to the state. Therefore, the cost of damage resulting from a successful breach to the reputation of a targeted company is not enough to motivate companies to protect themselves before anything happens. Alongside the growing awareness of shareholders and the customer base in the private sector, there is no inclusive or binding directive instructing companies to publish data breaches or report on the damage caused. Furthermore, the capabilities of technological tools currently available on the market are insufficient to create hermetic defenses.[6] Finally, most cyberspace users are unaware of the dangers, and provide cyberspace with sensitive, critical information that is not sufficiently protected. Many users also fall victim to social engineering attempts, choose weak passwords,

and in most cases, represent the weakest link through which systems are breached.[7]

It is therefore not surprising that we are inundated daily with reports from all over the world about newly discovered weaknesses, database breaches, sensitive information theft, and computer systems that have been maliciously damaged.[8] The ease at which commercial institutions and states collect and store critical information undercuts the efficacy of the efforts expended to protect cyberspace; thus, we find ourselves dependent on the proper functioning of a vulnerable sphere. For its part, the state tries to partially fix this market failure and intervene to either prevent cyberspace dangers from being realized or mitigate their impact after they already have occurred.

The risks posed by cyberspace are the natural progression of the risks facing the modern state, as described in 1986 by sociologist Ulrich Beck in his groundbreaking book, *Risk Society.*[9] According to Beck, modern life and its technological developments offer many opportunities, but also create new dangers to humanity and the environment. In 2002, economist David Moss referred to the complexity of risk management by governments.[10] Moss showed how the US administration, as the risk manager of the American society, went through three successive developmental stages in its risk management strategy. The process began in the nineteenth century when the United States intervened aggressively in financial risk management to encourage investments and economic growth (by legislation, such as the limited incorporation law that reduced investor risk and the early voluntary bankruptcy law that protected investors from losing everything they owned). Later, the state transitioned to risk management on behalf of workers' safety and job market stability (workers' compensation, social security, and the birth of the welfare state). Finally, in the current stage, the state manages risks for the entire society—environmental dangers, food and drug safety, and now cyberspace risks—arising from modern developments.[11]

The risk strategies that states use range from risk reduction to their distribution throughout society. On the one hand, reducing risks consists mainly of both preventing them in the first place (e.g., safety regulations, traffic signs warning to slow down, information security requirements to prevent hacking, and so forth) and mitigating the damage from a risk that has already occurred (e.g., firefighting regulations for dealing with fires,

steps to reduce the damage resulting from cyberattacks,[12] and notifying the public and state entities of a security breach so that they can protect themselves before being targeted). On the other hand, redistributing the risks consists of transferring the responsibility for the risk to a range of entities; for example, product liability laws shift the responsibility from the consumer to the manufacturer. A contemporary example is the 2015 Cyber Information Sharing Act that limits the liability for a data breach in commercial companies that choose to share information on cyber threats with the government. Risk redistribution can also occur by spreading the risks among various parties via insurance companies, for example. Every insured entity pays a certain premium to cover the damage from a risk being realized with some other party ensured under the same umbrella. In cyberspace, the private sector manages risk distribution mainly for third-party risks,[13] so far without any state intervention.

Despite the many risk strategies available, the state has not yet determined the right way to intervene—especially in the civic sector—to ensure the continuous functioning, resilience, and stability of cyberspace. In terms of the resilience of cyberspace, the civic sector has tremendous importance. Because this sector represents the lion's share of activity in cyberspace, it is exposed to most of the risks; therefore, damage to the civic sector has major economic and security implications for the resilience of the entire society, as this essay demonstrates.

State Regulation: Background and Development

At its most basic, regulation consists of control, supervision, and enforcement carried out by the state or through independent state-sponsored agencies to legally enforce binding codes of conduct.[14] It applies to those entities that the regulatory body wishes to regulate. The concept of regulation emerged in the United States at the end of the nineteenth century as a political and management method to control the economy. Regulation became the government's central tool and was a natural reaction to market failures, absence of supervision, and the emergence of so-called natural monopolies. By contrast, Europe tended to nationalize the market. Supervision through nationalization delayed the development of a regulatory tradition in Europe in tandem with the United States.[15] From the end of the 1970s and into the 1980s, the United States began expanding the use of regulation and

established independent regulatory agencies, while Europe started to use regulatory tools to accelerate its economic unity.[16]

When Margaret Thatcher was elected prime minister of the United Kingdom in 1979 and Reagan became the US president in 1981, neo-liberalism and privatization of government services were on the rise. This led to independent regulatory agencies widening the scope of their activities to regulate the market, thus giving rise to the nickname "the regulatory state."[17] The state's function has gradually shifted; from subsidizing services and helping to reduce gaps, the state now seeks to bring greater efficiency to the market by means of increased regulation (or by deregulation).[18] In practice, regulation is usually understood as legislation or sub-legislation by the state or independent regulatory agencies, expressed in binding directives, decrees, and guidelines. Its function is to control market activity, while the state sets the overall policy. In the regulatory state, experts play a key role; the demand for high expertise across issues is the initial motivation for the establishment of independent agencies.[19]

Justification for state regulation can be explained in several ways. First, regulation strives to protect the values and liberties of citizens who are liable to suffer at the hands of the powerful or from external threats. This justification explains the need for the army and security forces on the one hand, and for authorities that check and balance them on the other. Second, the economic justification for regulation is to fix market failures resulting from free market practices that do not serve the public interest,[20] e.g., the creation of a monopoly or a cartel that prices and provides products as it sees fit, making supervision necessary. Third, regulation can be justified by lack of information or asymmetry of information, which causes consumers, companies, and even states to behave in a manner inconsistent with the public good. In this case, the job of the regulatory body is to allow transparency and the free flow of information. Finally, regulation can be explained as the desire to ensure the continued existence of dwindling essential public resources that one cannot avoid using, from the quality of the air to the number of fish in the ocean. The regulatory body must ensure that these resources continue to exist, despite market forces that would—when left to their own devices—completely consume them.

The literature explains how the regulatory bodies work as part of public policy procedures and the creation of regulation in the first place using

many approaches. The theory of the public interest, also known as the functionalist theory, asserts that regulation operates to promote the common good and increase social welfare.[21] By contrast, the private interest theory maintains that private interests motivate regulatory bodies to increase the gains of centralized interest groups, usually representing a small slice of the population. In that sense, redundant regulation is a product of interest groups' relations with the state and amongst one another.[22] Furthermore, an institutional explanation for regulatory regimes can be given. An institution's capacity[23] or its historical location in the public policy process[24] explains the structuring of the regulation in the way in which it was created. In the last twenty years or so, another school of thought has emerged, which explains regulation based on ideas. According to this school of thought, paradigms play a central role in the shaping of public policy.[25] A certain idea will be perceived as "right" and as "a window of opportunity," causing decision makers to establish regulation in the spirit of the paradigm and its attendant interests.[26] In other words, in many cases, ideas and interests are intertwined to the degree that an idea can provide legitimacy and expression for interests groups, which are capable of generating regulation to serve their objectives.[27]

Regulatory Approaches in Cyberspace: Israel, the United States, and the European Union

Regulation, thus, is expanding in modern societies, and its justifications and explanations are rich and varied. Nevertheless, the literature has yet to explore the regulatory process in cyberspace. The paragraphs below describe the challenges for regulation of cyberspace, the ways in which regulatory bodies deal with cybersecurity, and how the United States and the European Union[28] have structured their regulation regimes of cyberspace compared to Israel. Finally, the essay focuses on Israeli regulation of cyberspace and highlights the largest gap in that regime—the civic sector.

Regulation in cyberspace does not refer only to defense in the classical sense; rather, it consists of many aspects directly related to national security, defense of assets and intellectual property, crime prevention, information security, and the right to privacy. Such regulatory objectives challenge regulatory bodies for three primary reasons. First, the costs involved for requiring protection are high and create vehement resistance among the private sector, which represents the largest proportion of cyberspace.[29] Second, there

is no state-issued guideline demanding that companies be transparent about their level of security and the severity of attacks in practice. Both attackers and defenders share information,[30] but generally defensive efforts do no benefit from extensive collective organizing. When commercial secrets and company reputations are at stake, it is hardly surprising that the civic sector would be unhappy to share information about the goings-on in its digital sphere. Third, regulation in cyberspace—as anywhere else—involves a conflict of interests. Most prominent are the struggles between statism[31] and liberalism, and the right to privacy versus the right to security.[32] Furthermore, struggles in the context of national security interests versus the desire for economic development (as reflected in supervision of exports of sensitive goods), as well as obstacles of information sharing among companies in light of the stringent directives issued by the director general of the Israel Antitrust Authority, serve as a partial reflection of the difficulties in instituting regulation in the field. These conflicts let loose contradicting interests and power struggles, which impede the implementation of regulation in cyberspace.

Given these challenges, regulation of cyberspace usually involves four ways of dealing with the problem of cybersecurity.[33] The most common one is to create standards and requirements in information security, including encryption, monitoring, backups, strong authentication, and so forth. In addition, regulation—especially in the United States—seeks to encourage and create mechanisms for information sharing between commercial companies and the state, based on the mutual desire to confront the problem of the lack of information and thereby protect against attacks before they occur, as well as mitigate the damage by attacks that have already occurred. The regulatory field is also notable for creating regulatory agencies and bestowing authority on state institutions to enforce defensive cybersecurity standards and practices.[34] Finally, regulatory regimes include steps to mitigate third-party hacking damage, including notifying the national CERT[35] and customers whose personal information was stolen. This is consistent with the "full circle of defense,"[36] which includes preventive steps, information sharing, and damage mitigation after an attack; together they create a coherent protective shell for organizations operating in cyberspace.

The regulatory tools used to confront cybersecurity risks generally involve legislation, binding state guidelines issued by the regulatory agencies,[37] and self-regulation by conforming to recommended standards, such as the ISO

information security standards,[38] the PCI standards for online companies providing clearing services,[39] or by internal organizational expertise, which provides guidelines for protecting the organization's computer networks, although this is not always publicly known. In addition, the state also issues standards and guidelines on the recommended way to defend the organization and/or the strategies that ought to be used. In the United States, for example, the National Institute of Standards and Technology is punctilious in issuing standards for defending and encrypting information systems,[40] while the Financial Industry Regulatory Authority assesses the best defensive cyberspace strategies for financial companies.[41]

In the Western world, there are two main approaches for states to confront cyberspace risks. While regulation in the United States is based primarily on multiple voluntary, sector-based agencies with considerable weight given to market forces,[42] the European Union presents a different, hierarchic model. Lateral institutions have strong enforcement powers, in which the state is at the center and large segments of the private sector are subject to regulation. While the United States believes that business interests will lead companies to defend themselves, the European Union takes a more interventionist approach, in which the state institution makes sure to defend the various sectors for the good of the citizens. Both the United States and the European Union enforce transparency on data breaches. In the United States, transparency is carried out at the state level (there are 47 versions of data breach notification rules),[43] whereas the European Union recently issued an upgraded General Data Protection Regulation (GDPR) Directive —effective in May 2016 and fully applied starting in May 2018—that ensures a uniform standard for notification and compensation for security breaches. The rationale of the European decision makers was to create incentives for the market to protect itself ahead of time so as not to have to bear the rigid burdens of notification and compensation.[44]

Finally, it seems that the United States is on the verge of expanding the risk strategies used, not only by preventing and mitigating damage due to cyberattacks, but also by shifting liability away from commercial companies in order to encourage information sharing. By contrast, this approach has not been adopted by the European Union and it is doubtful that it will be, given the possible infringement of the right to privacy, which the European Union views as a fundamental civil right that the state is obligated to protect. This

kind of information sharing gives legitimacy to commercial companies to increase their collecting of information and forwarding it to the state; without appropriate responsibility and transparency, it is difficult to believe this will ever be considered seriously in the European Union.

Both approaches provide only a partial solution; they do not include regulation of the state's security sector (the army, intelligence agencies, and so on), which is normally exempt from government regulation and mostly applies a self-regulation model. They also do not provide a comprehensive response for the civic sector and its multiple layers, including commercial companies, industrial institutions, and the civilians themselves.

Israel presents a hybrid model. On the one hand, the civic sector is, for the most part, not subject to any binding regulation, and, like the United States, the state relies on market forces to find the right balance between protection and economic investment. On the other hand, the statist approach is manifested in private companies, including the country's banks, in which the state dictates the information security practice because of their strategic importance. The state even imposes sanctions on such companies should they fail to meeting the necessary threshold conditions. There is an exception expressed in the Protection of Privacy Law, 1981, which includes aspects of information protection and is applied to all sectors against anyone possessing personal information; this law, however, dates from 1981, and its information protection aspects have yet to be updated.

See below the comparative chart highlighting the similarities and differences among the United States, Israel, and the European Union:

	United States	**Israel**	**European Union**
Type of regulatory regime	A liberal regulatory regime; reliance on market forces and mostly voluntary	Hybrid between liberalism and statism; critical infrastructures under state supervision; the market is driven by its own forces	A statist regulatory regime; centralized and binding
State presence	Only in critical sectors: energy, healthcare, electricity, water, etc.	Only in critical sectors: energy, healthcare, electricity, water, etc.	In critical sectors and online service providers

	United States	Israel	European Union
Risk management strategies	Progressive strategy: Prevention of cyberattacks and redistribution of liability for risks in civic sector	Solely focus on the prevention of risks. Israel has no limited liability laws with regards to cyber-security or one that requires cyber damage mitigation for companies and their customers in case of a data breach	Prevention/Mitigation of risks. Strategy of preventing attacks and mitigating damage, without redistribution of liability for company risks
Transparency towards consumers during a data breach	Exists at the state level in a non-uniform manner; 47 states, each with a different version	Non-existent	Exists in a coherent, uniform manner under Directives approved in 2016 that will be implemented by 2018
Conflict with the right to privacy	Privacy is a commodity—mostly managed by market forces, except for specific sectors (health records, information about minors, etc.)	Mostly managed by market forces, with relatively strict requirements not fully enforced by the Israeli Law, Information, and Technology Authority	Managed by the state with binding laws, institutions with power, and motivated by the interest of safeguarding privacy as a human right overriding economic interests. At the member-states level, the right to privacy is weaker vis-à-vis local intelligence agencies

Figure 1: Comparison of Cyberspace Regulatory Regimes in Israel, the United States, and the European Union

The process whereby cyberspace regulation is formulated in Israel consists of two major stages, but they too, as noted, lack a national strategy for all market sectors.[45] Israel's cyberspace regime started in 1998 with the law regulating security in public institutions. The law listed all the requirements for protecting information systems of institutions defined as "critical" to the state. These included aerospace, water, electricity, and communications bodies. In 2002, the state determined that the professional supervisor for these institutions would be the National Information Security Authority, which is subordinate to the Israel Security Agency (Shin Bet).[46] Furthermore, the

state determined that the institutions receiving directives from the National Information Security Authority would be carefully selected by a special steering committee; in practice, the list of bodies swelled with the passage of time. In other words, bodies defined as critical to the state, based on the impact of the potential damage (for the GDP, for example), received a state-mandated directive, whereas many other bodies, which were not defined as having the potential for great damage, were left without guidelines, thus leading to a situation in which the economic considerations of the market forces became the major factor in their defense. It should be noted that the institutions receiving directives include both private and public ones (oil refineries, El Al, the Israeli Electric Corporation, Israel Railways, and so forth).

In 2011, Israel entered the second stage of its development of cyberspace regulation when the government changed its approach and started to address the work required with the private sector. The National Cyber Bureau (NCB) was established under the Prime Minister's Office, a move designed to create better integration with market actors. Later, in 2015, the National Cyber Authority was founded with the objective to work directly with the civic sector and serve as the executive body for the state's cyber defense efforts. The Israeli regulatory state in cyberspace can be described schematically as follows:

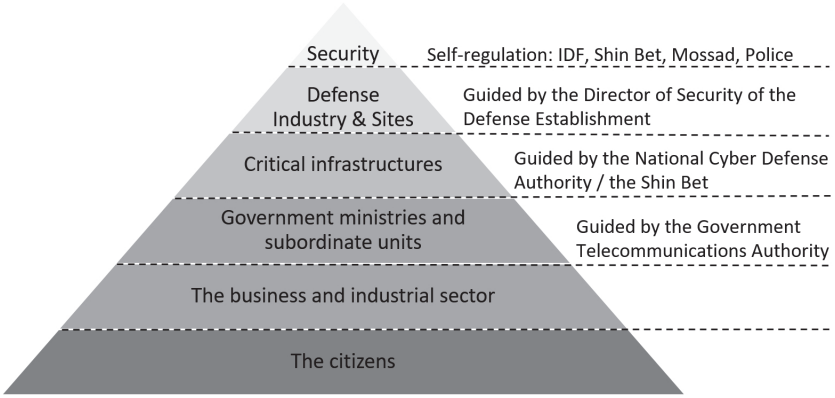

Figure 2: State regulation of cyberspace in Israel

The chart above particularly highlights two aspects. As previously noted, the civic sector is mostly left unsupervised. Although there are little islands

of supervision—the financial, energy, and healthcare sectors—guided by directives from government units, themselves subject to the guidelines of the Government Information and Communication Technology (ICT) Authority. But by and large, the civic sector engages in self-regulation, lacks information sharing, and mitigates data breaches to its customers as it sees fit.

Other than its selective supervision of different sectors, Israel recently issued two significant policy guidelines. The first, designed to enhance supervision already carried out by the Defense Exports Supervision Division at the Defense Ministry, expanded the list of products requiring state supervision, reflecting the state's desire to supervise the cyberspace arms race and maintain Israel's relative advantage.[47] The state has decided to halt this process and continue consulting with the cyber industry about the issue and, for now, adhere only to international supervisory arrangements, given the opposition from the local industry that was concerned it would not be able to compete with industries in unsupervised states.[48] The desire to maintain Israel's standing in the world as a leading cyberspace exporter relative to its population[49] resulted in the preservation of the status quo in the issue of supervision. This is instructive regarding the depth of the mutual understanding and extensive cooperation between the various industries and the Defense Ministry.[50] The ministry listened to the concerns of the industry, managed to get a toehold, and is now part of the decision-making process for every cyberspace product designed for attack.

The objective of the second guideline is to nurture human capital and create standards for those defending cyberspace. This is an entry regulation, based on official recommendation, in which the state delineates the professional level required of personnel in all forms of cyber defense.[51] This is a significant guideline, which has not been tried extensively elsewhere in the world. It may, on the one hand, raise the professional level on the short term through various training programs that could be developed especially for regularization; yet, on the other hand, this guideline could obviate the self-taught model by which most experts in this dynamic field currently attain their knowledge.[52]

Cyberspace Regulation in the Civic Sector: Importance and Difficulties

Despite the wide range of efforts described herein, the civic sector in Israel is not subjected to cyberspace regulation and its security lacks state

supervision.[53] This challenge traverses national borders, as manifested both in the United States and the European Union (until the two most recent European Union directives, which for the first time also cover industries in the civic sector). When it comes to the resilience of the shared cyberspace, it is difficult to overstate the importance of the civic sector. First, the civic sector represents the lion's share of the sphere. It is exposed to most of the threats and is traditionally the weakest link through which attacks begin and spread to other sectors. Second, private companies regularly provide services to government ministries and sensitive state institutions, making their resilience in cyberspace a primary concern. Third, damage to the private sector is damage to the stability of the entire economy. Under certain conditions, this could significantly harm the nation's resilience. The policy of expanded privatization has only exacerbated the problem, making the private sector the key player in the state's regulatory efforts. Fourth, the civic sector is responsible for technological developments upon which more sensitive sectors rely; thus, damage to it could serve as a backdoor to attacks on sensitive information.[54] This is especially true for startups poor in defensive resources, but that sometimes end up developing defense products for general use.[55]

The private sector's basic opposition to regulation is not surprising and is a familiar phenomenon in other contexts as well. State regulation and supervision are seen as hamstringing commercial companies and costing them a great deal in return for little value.[56] Moreover, the private sector considers the state to be slow to react to technological change and incapable of meeting the inherent challenges in supervising a dynamic, constantly changing technological sphere.[57] Instead of increasing the resilience of commercial companies, state regulation might force them to adopt standards that do not match current threats and take away the flexibility they enjoy today. Finally, the idea of state intervention is inconsistent with the neo-liberal approach that has spread like wildfire in twentieth century's capitalist societies,[58] where the regnant paradigm is one of privatization and deregulation, whereby the state intervenes only minimally, if at all, in the market to maximize the benefits accrued by commercial entities.[59]

Concluding Insights

Although Israel is developing its National Cyber Authority, many economic sectors still lack guidelines and supervision that would ensure appropriate protection. There is no road map to ensure the resilience of the civic sector and to serve as a model to be adopted by the different players in the economy. Such a model would have to address several key issues:

First, the model would have to generate a structured process that would provide civilian bodies with the incentive to adopt cybersecurity. Entry regulation, such as a local government business licensing law, is one way, but other options also may be considered. The state is currently working on a "cyber law" that aims to create a kind of cybersecurity verification seal that would define a uniform defense standard necessary to market companies.[60] The need for such a security seal might incentivize institutions to protect themselves better.

Second, it is necessary to consider the various layers of the civic sector. There is no one-size-fits-all solution; rather, it is crucial that the regulation be tailored to the type of enterprise, its level of information sensitivity, manufacturing processes, and supply chains of the various companies on the market. Therefore, it is necessary to rank the civic sector by its exposure to risk and the damage that a systems breach is liable to cause; an insurance company, for example, cannot be treated the same as a pharmaceutical manufacturer. The proposed model would have to address these essential differences.

Third, it is necessary to consider expanding the risk strategies the state is using. The lateral look at Israeli regulation in this essay teaches us that the state is primarily involved in preventing cyber risks from being realized. Mechanisms now emerging in the United States[61] to encourage information sharing—with the built-in tension over safeguarding the right to privacy—might make it possible to relieve the bottleneck of information sharing and create a more effective, proactive cybersecurity. In addition, it is necessary to enhance transparency over data breaches by requiring all sectors to notify a national CERT and share information with the public. This will help others understand where caution is needed and the extent to which sensitive information is at risk. These could serve as incentives for better defense and more effective damage mitigation. Commercial companies that worry about

having to pay for damage mitigation by law will defend themselves ahead of time as best they can.

To conclude, the need for regulating cyberspace in the civic sector is obvious, but the difficulties of developing such regulation are numerous; they range from the problems and battles between state institutions, the tensions between competing interests, the costs involved in adhering to regulation, and the attempts to find the right balance between transparency and secrecy as well as between centralization and decentralization. At present, even though cyberspace is essentially a civic sphere—most of it being based on civilian infrastructures, systems, and technologies operated by civilian organizations—this sector has not yet been regulated and incorporated into Israel's regulatory regime. The responsibility for cybersecurity currently rests on the organizations alone, even though the lone organization lacks the expertise and resources to confront cyber threats without creating an infrastructure for cooperation between the various sectors in the economy. Israel is quite active in the state's cyberspace as cyber units were established in the Prime Minister's Office, the decision to establish a cyber force was made, and various R&D settings and national research centers were founded. Nonetheless, it is incumbent upon the state to continue to strive to strengthen the defense of the relevant civic sectors using a range of tools and capabilities, because damage to the civic sector is liable to cause fundamental harm to the entire nation.

Notes

1 The resilience of cyberspace refers to the sphere's ability to withstand possible attacks aimed at software and hardware weaknesses, non-secure protocols, and unauthorized information access.

2 The development of these protocols met the needs at the beginning of the worldwide web in the 1960s. In those days, it was necessary to allow connectivity among just a few dozen computers. At the time, nobody predicted that a web consisting of billions of users would be using the same protocols.

3 Zero-day weaknesses are hardware or software weaknesses, generally unknown to the manufacturer, that have yet to be fixed. Sometimes they are known weaknesses for which patches have not yet been issued to all relevant systems. About this flourishing market, see Andy Greenberg, "New Dark-Web Market is Selling Zero-Day Exploits to Hackers," Wired.com, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

4 Internal documents of an Italian company, Hacking Team, recently were exposed, showing the company trafficked in weaknesses and the development

of attack tools. The documents showed the company's commercial ties with various regimes around the world. For more on the phenomenon, see Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *New York Times*, May 29, 2016, http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?ref=topics&_r=0.

5 Jason and Peter, "Cyber Security: A critical examination of information sharing versus data sensitivity issues for organizations at risk of cyber attack," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2014):10–111.

6 Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*, Memorandum 153 (Tel Aviv: The Institute for National Security Studies, 2016) http://www.inss.org.il/uploadImages/systemFiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf.

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

8 Nate Lord, "The History of Data Breaches," digitialguardian.com, September 28, 2015, https://digitalguardian.com/blog/history-data-breaches.

9 Ulrich Beck, *Risikogesellschaft: auf dem Weg in eine andere Moderne* (Frankfurt am Main: Suhrkamp, 1986). The book appeared in English as *Risk Society: Towards a New Modernity* (London: Sage,1992).

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

11 Ibid.

12 See the full defense circle in Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affair*s, May 7, 2015.

13 Third-party risks in cyberspace are the risks to the privacy of customers of commercial companies damaged by cyberattacks and by the theft of personal information. On the other hand, insurance companies are less than thrilled to ensure first-party risks because there is a lack of actuarial data that would help them price the insurance premiums for cyberspace risks of the companies themselves (i.e., first-party risks).

14 David Levi-Faur, "Regulation: Conceptual and Historical Background," (University of Haifa, no date), (in Hebrew). See also, David Levi-Faur "The Odyssey of the Regulatory State," *Jerusalem Papers in Regulation & Governance*, Working Paper no. 39 (November 2011), http://regulation.huji.ac.il/papers/jp39.pdf.

15 Ibid.

16 Ibid.

17 A state that mainly regulates for efficiency purposes, through laws, rather than investments and subsidies. See Giandomenico Majone, "The Rise of The Regulatory State in Europe," *West European Politic*s 17, no. 3 (1994): 77–101, http://dx.doi.org/10.1080/01402389408425031.

18 In his essay "Regulation and Regulatory Governance," Levi-Faur explains why deregulation obviates the formation of more agencies and the hiring of more bureaucrats to supervise privatization processes and guard the state's interests while it also accelerates the process. See David Levi-Faur, "Regulation and Regulatory Governance," *Jerusalem Papers in Regulation & Governance*, Working Paper no. 1 (February 2010), http://levifaur.wiki.huji.ac.il/images/Reg.pdf.

19 Ibid.

20 Shurik Dryshpitz, "Regulation: What, Where, and When? A Theoretical and Comparative Perspective" in "Who Privatized My State? Privatization, Regulation, and the Third Sector: Theory and Practice," *Parliament* 64 (Jerusalem: The Israel Democracy Institute, 2012), (in Hebrew), http://www.idi.org.il/parliaments/64/11149.

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

22 For an empirical research on the actions of interest groups in the United States, see Frank R. Baumgartner and Beth L. Leech, "Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics," *Journal of Politics* 63 (2001):1191–1213.

23 On the way that policy networks to protect privacy in Europe created stronger institutions, which passed more rigid privacy laws contrary to the spirit of the time, see Abraham L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62, no. 1 (2008): 103–130.

24 On the consistency of the modern welfare state, see Paul Pierson, ed. *The New Politics of the Welfare State* (Oxford: Polity Press, 2001).

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

26 John Kingdon's study coined phrases such as "window of opportunity" and "policy entrepreneur," which explain—with astonishing accuracy—public policy procedures. See John W. Kingdon, *Agendas, Alternatives, and Public Policy*, 2nd edition (Boston, Little Brown, 1995).

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

28 While the European Union differs from the classical state institution, it is still a seminal object for comparative research in the field. Decisions at the EU level led to a rigid information security policy through the European Union (see Newman 2008 and below), and the directives formulated at the EU level led the way for the individual states. This is valid not only for the world of cyberspace, but also can also be observed in contexts of food safety regulation and the introduction of genetically engineered food throughout the continent. For the importance of EU regulation, see David Bach and Abraham L. Newman, "The European Regulatory

State and Global Public Policy," *Journal of European Public Policy* 14 no. 6 (2007): 827–846.

29 Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security," *Georgetown Journal of International Affairs*, International Engagement on Cyber, IV, (2014): 69–78.

30 For the ways in which hackers share information in the darknet, see the interview with Stuart Madnick from MIT in Linda Tucci, "Stuart Madnick: Dark Web hackers trump good guys in sharing information," techtarget.com, April 30, 2016, http://searchcio.techtarget.com/news/450295259/Stuart-Madnick-Dark-Web-hackers-trump-good-guys-in-sharing-information.

31 Increased government intervention and centralization.

32 See the thought-provoking philosophical debate over the terms "zero-sum game" and "necessary balance" between security and individual liberty in Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy* 11, no. 2 (2003): 191–211.

33 These methods to confront the risks come up in the examination of how regulation has been put in place over the years in the United States (at the federal and state levels) and in the European Union (at the EU level and individual state levels).

34 For example, US courts recently gave the Federal Trade Commission the authority to enforce information protection laws in the private sector. For more information, see Brent Kendel, "Appeals Court Affirms FTC Authority Over Corporate Data-Security Practices," *Wall Street Journal*, August 24, 2015, http://www.wsj.com/articles/appeals-court-affirms-ftc-authority-over-corporate-data-security-practices-1440425754.

35 The abbreviation stands for Cyber Emergency Readiness Team, a regulatory agency now in existence in virtually every state. It collects data on all cyberbreaches requiring notification and integrates responses to significant events happening in cyberspace.

36 Gabi Siboni, May 7, 2015.

37 For example, guidelines issued by the Information Security Authority in Israel about the way to secure organizational networks.

38 For an explanation of ISO standards at the official website, see http://www.iso27001security.com/html/27032.html.

39 For an explanation of PCI standards at the official website, see https://www.pcisecuritystandards.org/.

40 See, for example, the standards the organization issued: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

41 For example, the latest FINRA report issued on the topic: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

42 Richard J. Harknett and James A. Stever, "The New Policy World of Cybersecurity," *Public Administration Review* (2011): 455–460.

43 For details, see National Conference of State Legislators (NCSL), Security Breach Notification Laws, April 1, 2016, http://www.ncsl.org/research/

telecommunications-and-information-technology/security-breach-notification-laws.aspx.

44 For details on the effect of European regulation on the security level of commercial companies, see Ashford Warwick, "Breach Notification the Biggest Impact of EU Datalaw Overhaul, Says Law Firm," computerweekly.com, November 27, 2015, http://www.computerweekly.com/news/4500258249/Breach-notification-the-biggest-impact-of-EU-data-law-overhaul-says-law-firm.

45 Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

46 In 2015, the National Cyber Defense Authority was established, assuming responsibility of most of Israel's critical infrastructure.

47 The expansion applies primarily to penetration products, hacking analysis, and knowledge of software and hardware weaknesses.

48 For more information, see article by guest writer, "What Lay Behind the Repeal of the New Cyber Injunction," *Geektime*, April 2016, (in Hebrew), http://www.geektime.co.il/the-decline-of-the-israeli-cyber-law/.

49 For the change in the southern city of Beer Sheba, which the state decided to recreate as the region's cyberspace export capital, see Ashford Warwick, "Israel's cyber security frontier," computerweekly.com, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier.

50 See Wexman and Hindin, "How Does Israel Regulate Encryption?" lawfareblog.com, November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

51 For the official regularization document, see Prime Minister's Office, National Cyber Staff, "Profession Regulation Policy for Cyberdefense in Israel," December 31, 2015, (in Hebrew), http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf.

52 See report on the subject, National Academy of Science, "Professionalizing the Nation's Cybersecurity Workforce," 2013, http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making.

53 This is with the exception of specific entities, such as the banks, and the privacy law, which applies to the entire economy, although it is not sufficiently up-to-date in terms of all aspects of information security. For a survey of the situation, see Raphael Kahan, "Netanyahu markets Israeli cyber but legislation is full of holes," *Calcalist*, June 2015, (in Hebrew), http://www.calcalist.co.il/internet/articles/0,7340,L-3662815,00.html.

54 For a more in-depth survey of some of these reasons, see Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security," *Georgetown Journal of International Affairs,* International Engagement on Cyber, IV, (2014):69–78.

55 Gabi Siboni and David Israel, "Cyberspace Espionage and Its Effect on Commercial Considerations," *Military and Strategic Affairs* 7, no. 3 (December 2015): 39–58, http://www.inss.org.il/uploadImages/systemFiles/INSS.MASA-7.3-Full(ENG).pdf.

56 Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security."

57 Ibid.

58 For a survey of the neo-liberal trend in capitalist societies, see John Dryzek, *Democracy in Capitalist Times: Ideas, Limits, and Struggles* (Oxford University Press, 1996).

59 Does privatization really lead to deregulation? For a challenge to the justifications for privatization, see Yitzhak Gal-Noor, "The Policy of Privatization: Whose Burden of Proof Is It?" (Jerusalem: Hebrew University and the Van Leer Institute, 2014), (in Hebrew). For regulation in the privatization era, see David Levi-Faur, Noam Gidron, and Smadar Moshel, "The Regulatory Deficit of the Privatization Era," (Jerusalem: Van Leer Institute, 2014), (in Hebrew).

60 See Yossi Melman, "Closed code: State promoting cyber defense law in light of increased attacks," *Maariv*, February 2016, (in Hebrew), http://www.maariv.co.il/journalists/Article-524985.

61 See Andy Greenberg, "Congress Slips CISA into a budget bill that's sure to pass," Wired.com, December 16, 2015, http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Tim Greene "CISA Legislation would fit liability for businesses sharing cyber threat information," networkworld.com, October 28, 2015, http://www.networkworld.com/article/2998815/security/cisa-legislation-would-lift-liability-for-businesses-sharing-cyber-threat-information.html.