**Regulatory Capitalism or Regulatory Capture? Analyzing the Relationship between the Public and Private Sectors in the Case of Cyber Defense in Israel**

**Abstract**

The study deals with the relationship between the private and public sectors through a case study of cyber defense in Israel. The unique characteristics of cyberspace and the increase in cyber events in recent years make cyber defense a high priority at the national level, promoting the use of regulatory mechanisms. The study looks at the creation of cyber defense regulation in Israel, using a theoretical framework that examines the relationship between the public and private sectors, drawing on regulatory capture theory, regulatory capitalism, and Kingdon’s multiple streams. Thirty-one interviews were conducted with politicians, regulators, bureaucrats, and representatives of defensive organizations, cyber security companies, and consulting companies. The analysis reveals a complex picture in which although policy processes are “captured” by interest groups, the involvement of the private sector also reflects a sense of public responsibility. These two processes, described as regulatory capture and regulatory capitalism, co-exist in cyber defense regulation in Israel. The study contributes to the regulatory capture literature by examining in depth the processes of creating regulation and treating the private sector as composed of various different actors.

**Key words:** Regulation, Regulatory Capture, Regulatory Capitalism, Multiple-streams, Cyber Defense, Cyberspace

# Introduction

Cyberspace is a unique space in many respects, given its lack of physical boundaries and its embedded technology. In recent years, the prevalence and severity of cyber events and attacks have increased, and cyber protection has become more significant both for states and for the private sector. State regulation has therefore been developed to regulate the security protocols required by organizations (Wiggins et al. 2015).

Given the unique characteristics of cyberspace and the technological nature of cyber defense, in the field of cyber defense regulation the relationship between the public and private sectors is of major importance. In this context, a common concern is the regulatory capture theory, according to which a policy process can might be “captured” by industry )Boehm 2007; Carrigan 2013; Dal Bó 2006; Laffont and Tirole 1991; Stigler 1971; Mitchell and Munger 1991; Grossman and Helpman 1996; Peltzman 1976; Carpenter and Moss 2014). At the same time, another approach based on neoliberal economics has developed, with the concept of regulatory capitalism at its center. According to this approach, the increasing involvement of the private sector in regulation creation processes does not necessarily reflect capture but arises from a developing perception of the role and public responsibility of the private sector (Levi-Faur 2010; Carrapico and Farrand 2017; Cahill 2015; Vogel 1996; Braithwaite 2008; Levi-Faur and Jordana 2005).

The aim of this study is to explore the relationship between the public and private sectors in the regulation creation process, using a case study of cyber defense regulation in Israel. An integrated framework is used, which includes regulatory capture theory, regulatory capitalism, and the multiple streams framework (Kingdon 2011) to conduct a qualitative content analysis of interviews with various actors.

# Literature Review

## 2.1 Regulation and Cyber Defense

In recent years, there has been a significant increase in the prevalence of cyber events and their severity around the world (Levi 2017). This trend is largely attributed to the unique characteristics of cyberspace that facilitate hostile activity, such as the rapid changes it goes through, the irrelevance of physical distance, and its relative anonymity. This deteriorating trend affects personal and state security and economic activity, and demands consideration at the national level (Peterson 2013).

Cyber defense is defined as “control, development, management and use of information security, Operational Technology (OT) and Information Technology (IT), in order to achieve regulatory compliance, protection of assets, and damaging enemy assets” (Galinec et al. 2017, 273). Cyber defense policy is focused on prevention, identification, and timed responses to attacks on or threats to information infrastructures (Galinec et al. 2017). In recent years, cyber policies have included innovative defense methods in response to new challenges (Miao et al. 2018).

Given the unique characteristics of cyberspace and existing threats, regulation has emerged for the security protocols that organizations are required to apply (Wiggins et al. 2015). The concept of regulation was first introduced during the 1970s with the “economic theory of regulation” (Stigler 1971) and developed during the 1980s and 1990s. Definitions of regulation vary according to different disciplines and terminologies; here, we define it as “all the efforts of the state agencies to steer the economy” (Koop and Lodge 2015, 3). The use of regulatory mechanisms is one of the actions taken by states to promote processes such as identification, protection, detection, and response to cyber threats (Mee and Morgan 2017).

## 2.2 Public and Private Sectors in the Creation of Regulation

Several studies dealing with cyber defense regulation have focused on the relationship and cooperation between the private and public sectors (Lafen 2018; Clinton 2011, 2015; Tropina 2015), on the grounds that the unique characteristics of cyberspace make this cooperation necessary (Clinton 2011, 2015; Neutze and Nicholas 2011; Tropina 2015). This argument is based on specific characteristics of cyberspace, such as the fact that computer networks are operated mainly by the private sector and the state does not have the technical ability to implement full cyber defense (Clinton 2015), alongside the supranational nature of cyber defense, which requires interstate coordination (Tropina 2015). The basic assumption is that since this cooperation occurs for the public good, the two sectors work in harmony to achieve a common goal. At the same time, the dialogue between the sectors raises many issues, such as mistrust, mismatch of expectations, conflict of interest, and governmental laws that may act against the interests of private business organizations (Shore 2011).

Studies examining the effectiveness of cyber defense regulation have concluded that regulation does not enable the benefits of public-private sector partnership to be maximized (Clinton 2011, 2015; Tropina 2015), because it does not allow an equal relationship between the sectors or contribute to the building of trust between them (Clinton 2011, 2015; Tropina 2015). In addition, most business organizations do not want their cyber departments to be under government regulation (Lafen 2018). Nevertheless, in recent years, there have been attempts to address the knowledge and skills that exist in the private sector as inherent components in these processes (Slayton and Clark-Ginsberg 2018; Cavelty 2008).

Several recent studies (e.g. Carrapico and Farrand 2017; Slayton and Clark-Ginsberg 2018) have suggested that, in the field of cyber defense, the private sector has a unique role in developing public policy, different from its role in other industries. Slayton and Clark-Ginsberg (2018) argued that it is difficult to distinguish between legitimate cooperation between the public and private sectors, on the one hand, and regulatory capture, on the other, in which interest groups influence regulatory creation (Posner 1974; Stigler 1971; Carpenter and Moss 2014). Through the lens of a regulatory capitalism theoretical framework, Carrapico and Farrand (2017) claimed that these relations have evolved dramatically in recent years.

In order to analyze the relationship between the public sector (with an emphasis on politicians) and the private sector (defense business organizations, security companies, and consulting companies), this study’s theoretical framework will now be discussed. It is based on three existing theories: regulatory capture theory (Posner 1974; Stigler 1971), regulatory capitalism (Braithwaite 2008), and the multiple streams framework (Kingdon 2011).

## Regulatory Capture Theory

According to regulatory capture theory, regulation is not created to serve the public interest but to serve the interests of interest groups. Interest groups use different methods to influence politicians, such as voters, campaign finance, and bribery (Boehm 2007; Carrigan 2013; Dal Bó 2006; Laffont and Tirole 1991). In return, politicians provide interest groups with their desired regulation in the form of subsidies, entry barriers, or price control (Mitchell and Munger 1991; Stigler 1971), forcing consumers to purchase certain products or services (Grossman and Helpman 1996; Peltzman 1976).

Regulatory formation can be described as an economic process of supply and demand, where interest groups have a demand for regulation and are willing to pay for it, and politicians are able to create regulation, which they sell at the maximum price (Posner 1974; Stigler 1971). According to the definition provided by Carpenter and Moss (2014), in order to “diagnose” capture in an industry, one must (1) identify a change in policy from an action in favor of the public interest to one in line with a special interest of the industry, and (2) show intention and action on the part of the industry or interest groups in pursuit of this change in policy. The current study adopts this definition, but the analysis of the interviews also makes it possible to detect a casual connection between the change in policy and the activities of the actors.

## Regulatory Capitalism

Although, according to some perceptions, we live in an “age of deregulation” (Levi-Faur 2010, 3), contrary to expectations and to the rhetoric used in various social contexts, regulation is increasingly common. The economic crisis of 2008 started a trend for regulation as a tool for monitoring the economic market (Levi-Faur 2010).

The term regulatory capitalism is derived from the neoliberal economic approach (Carrapico and Farrand 2017). Theoretical neoliberal ideas differ significantly from their application, which has been described as “actually existing neoliberalism” (Cahill 2015; Vogel 1996). In practice, instead of the expected deregulation, one can notice a process of re-regulation, in which regulatory bodies and agencies proliferate, both quantitatively and in terms of the responsibilities given to them (Braithwaite 2008; Levi-Faur and Jordana 2005). Therefore, due to the significant increase in the existence of non-state regulation, many authors have proposed that this process be referred to as regulatory capitalism (Carrapico and Farrand 2017; Braithwaite 2008; Levi-Faur and Jordana 2005; Cahill 2015).

Regulatory capitalism provides a general framework for understanding the growing role of the private sector in the division of labor between the public and private sectors (Carrapico and Farrand 2017). Against a backdrop of privatization processes, the formation of independent regulatory bodies is perceived as necessary (Braithwaite 2008). Although the private sector has traditionally not been included in the list of regulatory bodies, it plays an increasing role in the re-regulation process by encouraging regulation by state and regulatory agencies, especially in the technology and information-based industries (Carrapico and Farrand 2017).

Another theory used in the current study to analyze the relationship between the private and public sectors is the multiple streams framework (Kingdon 1995), which is briefly presented in Section 2.5.

## 2.5 Kingdon’s Multiple Streams Framework

Some recent studies have used Kingdon’s multiple streams framework (2011, originally 1995) to analyze public policy in various fields (e.g., Giese 2020; De Bruijn and Janssen 2017; Stanifer and Hahn 2020). The framework identifies three streams in the system: the problem stream, the policy stream, and the political stream. The problem stream includes the relevant problems and the way certain conditions are framed as problems by the media or policymakers (Kingdon 2011; Travis and Zahariadis 2002; De Bruijn and Janssen 2017; Giese 2020). The policy stream is the policy alternatives, which include a wide range of policy ideas created by experts, academics, group and community leaders, bureaucrats, and politicians (Kingdon 2011; Travis and Zahariadis 2002), which may be formed into concrete policy proposals or may simply disappear (Travis and Zahariadis 2002). The political stream includes changes of bureaucrats and politicians and consequent changes in political attitude (Travis and Zahariadis 2002). Kingdon’s model suggests that at some point in time, the combination of streams creates a window of opportunity in which policy can be accepted (Kingdon 2011; Travis and Zahariadis 2002; Giese 2020). Policy entrepreneurs who identify the window of opportunity can present a “package” of problem and solution to a policymaker (Kingdon 2011; Travis and Zahariadis 2002). In the context of cyber defense, such a solution could be a regulation that the policymaker is interested in promoting (Gorwa and Peez 2018; Lawson 2013).

The last part of this review (Section 2.6) presents the Israeli case and its significance for analysis of the relationships between the public and private sectors in the field of cyber defense.

## The Israeli Case

Despite having been recognized as a significant force in cyberspace for over a decade, Israel has received little research attention in the context of cyber defense. The few studies dealing with cyberspace and Israel have focused on other security aspects (Adamsky 2017; Baram 2013, 2017; Tabansky and Ben Israel 2015; Siboni and Assaf 2016). In 2011 in Israel, the National Cyber Bureau (INCB) was established as a consulting agency to the government, with a committee in relation to the formation of cyber policy (Adamsky 2017; Sabillon et al. 2016). In 2015, the government established a new agency, the National Cyber Security Authority (NCSA) and constituted a single national cyber directorate (Tabansky 2017). Today, the National Cyber Directorate (INCD) is the highest authority in the cyber field in Israel. It reports directly to the prime minister’s office and has two branches: the National Cyber Bureau (INCB), which is responsible for strategy planning, and the NCSA, which is responsible for implementation and regulation at the national level (Adamsky 2017).

The characteristics of the Israeli case, where there is technological pioneering in the field of cyber defense (Adamsky 2017; Tabansky 2017) but also a lag in certain aspects of regulation and policy (Adamsky 2017; Sabillon et al. 2016), make it uniquely interesting for the purpose of analyzing public-private sector relationships (MacKinnon et al. 2013).

## 2.7 Rationale of the Current Study

Most recent studies of the relationship between the public and private sectors in the context of cyber defense regulation have focused on quantitative variables, such as regulatory outcomes, and have treated the private sector as a single coherent actor. The current study contributes to the literature in the following two respects. First, instead of focusing on the results of regulation, it offers a perspective on the processes of regulatory formation as reflected in the words of different actors. Second, it does not treat the private sector as a single coherent actor but recognizes that it contains at least three different actors: defense organizations, security companies, and consulting companies. The implementation of a qualitative approach thus sheds new light on the dynamics and the relationships between the various actors in the context of the evolving technological field of cyber defense regulation.

# Methodology

## 3.1 Study Design

This study is based on the qualitative paradigm that seeks to describe the attitudes and perceptions of various actors. As such, it does not measure any quantitative variables or correlations but explores the processes of regulatory creation and design as perceived by the actors (Ben-Joshua 2016; McNabb 2015).

## Research Questions and Hypotheses

Research question 1: Is there an influence of the private sector on politicians in the processes of creating regulation in cyber defense in Israel?

Hypothesis 1a: The private sector (defense organizations, consulting companies, and information security companies) is trying to influence politicians by creating a demand for regulation.

Hypothesis 1b: The private sector plays an active role in the processes of creating regulation and influences the content of regulation.

Research question 2: What are the motives for the involvement of the private sector in the processes of creating regulation?

Hypothesis 2a: In accordance with regulatory capture theory, interest groups from the private sector are involved in the process of creating regulation for rent-seeking purposes.

Hypothesis 2b: In accordance with the theory of regulatory capitalism, the involvement of the private sector in the processes of regulatory creation reflects a development in the perception of the role and public responsibility of the private sector.

## 3.3 Participants

A total of 31 interviews were conducted with representatives of the regulatory process: regulators and bureaucrats, politicians, high-ranking officers in the INCD, and various representatives of the private sector. The politicians represent a number of different authorities: the NCSA, the INCB, the Israel Director of Security of Defense Establishment (Malmab), the legislature (the Knesset), and the INCD. The respondents from the private sector are representatives of manufacturers and communications systems, defense organizations, and consulting companies. Some of the interviewees can be regarded as representing more than one group, as they previously worked for a different actor. In these cases, the interviewees were asked about the perspectives of both actors. Thus, in total, 18 interviewees represented the public sector (nine regulators or bureaucrats, three politicians, and six members of the INCD), and 14 interviewees represented the private sector (11 from defensive organizations and three from other interest groups). Three of the respondents were professionals in other aspects of cyber defense (such as academia or media).

## 3.4 Tools

The study is based on open interviews, in which there was an open conversation between the interviewer and the interviewee about the research topics. The interview included questions such as the following: Who are the actors that influence regulation? What are the roles of each actor? What are the power relations between those actors? How do these relationships change over time? What drives the regulatory/decision-making process?

## 3.5 Data Analysis

The analysis of the interviews was carried out via content analysis. In the first stage, the author read the transcripts of the interviews in their entirety and identified the main themes. In the second stage, the statements of the interviewees were categorized systematically according to the themes found. In the third stage, the recurring topics in each theme were identified. In the fourth stage, the statements in each theme were arranged according to the different attitudes of the interviewees. In the fifth stage, the findings that express the different positions were presented, focusing on the research questions and hypotheses.

# Results

Most of the interviewees, who had different roles in different organizations, explicitly stated that actors from the private sector, such as defense organizations, security companies, and consulting companies, influence regulation. Interviewees who mentioned this described two complementary, non-exclusive modes of influence: creating a demand for regulation (that is, influencing regulators to create regulation), and influencing the content of the regulation. In these ways, actors from the private sector intervene in the content of regulation, with various motives. The results reported here are organized into four parts in line with the research hypotheses.

## 4.1 Creating a Demand for Regulation

A large proportion of the respondents stated, implicitly or explicitly, that various actors from the private sector, for example, information security companies, are actively creating a demand for regulation:

The manufacturing companies, let’s call them the manufacturers, the security products, they also have an interest. (Interviewee 10, defense organization)

As one of the interviewees explained:

There are all kinds of stakeholders who influence the regulators, try to influence the regulators, call them lobbyists. Not exactly lobbyists, but there are those who actually activate lobbyists and I would say that first and foremost the bodies that deal with the commercial side of information security, they have a very big interest in regulation. And first and foremost it’s the manufacturers. (Interviewee 18)

This interviewee represents the private sector, being a manager at a cyber security company. The description given by the interviewee states explicitly that information security companies actively influence regulators in order to create regulation.

An almost identical claim indicating the existence of demand for regulation by actors from the private sector was made by an interviewee who represents a consulting company:

Consulting companies may have some influence, but […] their vision is not really a broad forward vision. They think about how they will make the money now, consulting in places that they feel convenient in. (Interviewee 19)

That is, according to this interviewee, consulting companies generate a demand for regulation that increases their sales.

The citations presented in this section are just a few examples of issues raised by the interviewees from which it is clear that various actors from the private sector are actively creating a demand for regulation. This supports Hypothesis 1a.

## 4.2 Influence on the Content of Regulation

The second way in which different actors from the private sector influence regulation is by influencing its content. For example:

Most of them are trying to sell today, to increase their sales based on regulations […] the biggest use case is GDPR, suddenly everyone provided dashboards for GDPR and checklists and compliances and all kinds of controls […] they have built functionally regulation support products [they…] are involved in the drafting stages. (Interviewee 15)

This interviewee claims that actors from the private sector, in this case information security companies, influence not only the process of creating regulation but also the content of regulation. In this case, he does not claim that information security companies initiated a demand for the GDPR privacy security standards; however, he states that they were involved in the drafting stages.

In the responses of interviewees who referred to other actors from the private sector, such as consulting companies, there is evidence that, like information security companies, consulting companies influence regulation by designing its content:

The consultants too, which is a very significant category in the industry, have such an interest […] I think consultants are very influential, because they often write the regulation for these bodies. (Interviewee 18)

Yes, you also sometimes see tenders that are translations from English to Hebrew. In 2008 for that matter, when a tender was issued for [name of governmental project] it was [names of international consulting companies] translated to Hebrew, by the way. (Interviewee 7)

These interviewees, who represent a defense organization (18) and an information security company (7) in the private sector, emphasize that the impact of consulting companies on the content of regulation is widespread because they write the regulations for the regulators. The response of another interviewee, who represents a defense organization, elaborates on the nature of that influence:

Once you are involved in determining X, you have an interest, you push your services, your desires, your agenda, which is fine too. In the end of the day, they are not doing it because they are paid. They do it because they have clear interest, if suddenly there is a demand for, I don’t know … supplier checks. (Interviewee 10)

This interviewee describes how consulting companies not only influence the content of regulation, but do so in a way that is in line with their interests. She emphasizes that consulting companies do not get paid by the regulators for their services but are rewarded by having their interests advanced.

Support was thus found for Hypothesis 1b, according to which the private sector plays an active role in creating regulation and influences its content. This aspect is further clarified in Section 4.3, on the existence of regulatory capture.

## 4.3 Regulatory Capture and Rent-Seeking

In the words of the respondents, there is a great deal of evidence for the existence of regulatory capture as defined in the current study. For example:

So he will go to the regulator and say: “It’s time …,” as is now happening in the banks. Someone there told them, “Now it’s time to move to the cloud.” But did someone there tell them, “Now it’s time to define what you really do for cyber defense”? […] there is a lobby of the manufacturers here. It is some of the consulting companies that go hand in hand with them. There’s a lot of them. Most of the consulting companies have products they market […] Regulation is actually a server tool of consultants and manufacturers. It does not really stand alone, it does not really take everything into account. It is influenced. (Interviewee 19)

This interviewee expresses in her own words, but precisely, the idea of regulatory capture. She describes how the initiative for regulation comes from stakeholders in the private sector, and how regulation is designed to serve their interests. It is a “server tool” of consultants and manufacturers; that is, interest groups have both intention and action in the creation of regulation.

Another respondent, who represents both the private sector for his past work and the Cyber Directorate in the present, refers to the consulting companies, claiming that they also have an influence:

surely the big consulting companies, KPMG, TWC, TY, and so on, they have influence […] they wrote the methodology. No doubt it has an influence. (Interviewee 16)

This respondent also addresses the factor that allows consulting companies to exert influence: the writing of various procedures and documents for regulators, which are thus captured by the interests of interest groups in the private sector.

Another interviewee, who also represents an information security company from the private sector, explains that the representatives of the information security companies with whom the regulator consults are biased in favor of their own products:

Listen, I know so many people in this field, and they are painted in the colors of the products they come from. They don’t mind, a day after they move to another vendor, to trash on the vendor they worked for […] That’s why I say that when your first interest is your bonuses and achieving your goals […] I don’t think it’s a matter of evil. You know, when you know something and you know it works for you properly … so it’s the most correct one. (Interviewee 7)

This interviewee explains that, whether intentionally or innocently, the representatives of the security companies are biased in favor of the products they represent. Another example of regulatory capture is seen in this quote:

In addition, there are all those companies with an interest, the various consulting companies, who we also saw them in previous regulation involved and directed […] Take the supervisor over insurance, which is a regulation of 2006, number 257. We see there … it almost reaches the level of which model of [one of the information security companies] to choose. […] So there are interests there. It’s also, also in the new regulation. When they ask to make a risk management every 18 months … it’s clear that someone has defined it, because there is no point in doing it every X time. There is a point in making it after any significant change. If there was no change in 18 months, it’s not sure that there is a point in checking. It depends on what. This push for this test […] it is shown that there are interests there. (Interviewee 10)

Interviewee 10 emphasizes that the involvement is very specific. The information security companies draft regulations for the regulators, such that the regulations dictate the use of their specific products (“it almost reaches the level of which model of [one of the information security companies] to choose”).

Thus, in accordance with Hypothesis 2a, the interviewees illustrate the existence of regulatory capture in the processes of creating and designing regulation in the field of cyber defense in Israel. In other words, various actors from the private sector are involved in creating regulations out of a desire to advance their own interests.

Nevertheless, a question remains as to whether rent-seeking is the main motive for the involvement of the private sector. In this connection, Section 4.4 deals with the evolving responsibilities of the private sector in the field of cyber defense.

## 4.4 Regulatory Capitalism and Public Responsibility

As the interviewees report, the involvement of the private sector stems from a number of motives that do not necessarily reflect the narrow interests of the various actors. There is considerable evidence that the involvement of the private sector in regulation processes is related to a growing public responsibility. For example:

If it’s a government, so [one the security companies] are there a lot and [another security company], because they won the tender a few years ago, a public tender. They are there and [a representative of the regulator] knows them and it’s like that […] but to tell you that I think they influence the regulation somehow? No. I know the people and what they do. No, or not enough. In the past they used to do a lot more work. I don’t want to say, “When I worked there,” but we did much more work with bodies that are regulation. […] Between 2005 and 2010 I worked at [one of the information security companies]. One of the products we had was [the name of the product] […] and I said, “Let’s try and sit down with the Banks’ Supervisor and start to create regulations that are Israeli.” (Interviewee 7)

This interviewee, who represents the private sector through the security companies, claims initially that information security companies do not influence the regulators. However, in the same breath he adds that he himself was involved in influencing such a process in the past. Moreover, he states that managers “do not do enough”; that is, as he perceives it, influencing regulation is part of the role of managers in information security companies, and if they do not influence the regulation they are not doing their job well. Similar claims were made not only among interviewees representing the private sector but also among interviewees representing the Cyber Directorate. For example:

No doubt they are actors in the lobby. With difference, but as weapon manufacturers in the United States have their own lobby in order not to cancel the law that everyone could hold 17 weapons. I am convinced that large companies gain well from sorts of such processes, but these are moves that are part of democracy. (Interviewee 16)

This interviewee points out that he does not see this process as normatively problematic, because it is a “part of democracy.” Another interviewee, who represents an information security company, confirms that she is involved in the process of drafting regulation:

If someone comes to me and asks me, then I will make an appointment with him, have a cup of coffee with him, and answer any questions he has. And if he invites me to come to a committee, then I’ve been to all kinds of committees in my life and … I’ll say what I have to say and that’s it […] I do not work with regulators on a regular basis. There are a lot of people in [one of the security companies], and when they ask me to come to a meeting I come to a meeting […], and if people ask me then I answer them. I don’t need … I do not dig into what purpose they ask, so like … I guess some of the people who asked me in my life did it for purpose of regulation. (Interviewee 9)

The responses illustrate the complexity that exists in the involvement of the private sector in the creation of regulation. On the one hand, there is widespread agreement that this involvement exists, and is even legitimate in terms of the “rules of the democratic game.” On the other hand, it is presented as the responsibility of the private sector to contribute from its professional knowledge while remaining “neutral” and acting without specific interests.

Hypothesis 2b suggests that the involvement of the private sector in creating regulation reflects a development in the perception of its public responsibility. The analysis of the interviewees’ statements does not allow an unambiguous determination of whether there has been such a development, but there is evidence that the private sector plays an important role in these processes.

# Discussion, Summary, and Conclusion

The current study analyzes the relationship between the public and private sectors in creating regulation in cyber defense in Israel. The content analysis of the interviews reveals a complicated picture that reflects the complexity of this advanced technological field.

From the interviewees’ responses it is clear that actors from the private sector create a demand for regulation. This idea is found, in some form, in the words of most of the respondents. This finding is consistent with previous studies showing that, although the private sector has not traditionally been included in the list of regulatory bodies, it plays a developing role in regulation processes by encouraging the state and regulatory agencies to create regulations (Carrapico and Farrand 2017). In addition, the interviewees say that the private sector is trying to influence regulation not only through a demand for regulation but also through involvement in its content. This involvement is in line with the literature that describes the relationship between the public and private sectors in this field as demanding cooperation between states and the private sector, given the unique character of cyberspace (Clinton 2011, 2015; Neutze and Nicholas 2011; Tropina 2015). According to the interviewees, the involvement of the private sector is manifested in professional counseling to politicians, and also in writing and drafting the regulations themselves; that is, they create a demand for regulation and influence its content. This provides support for Hypotheses 1a and 1b.

The words of the interviewees also provide evidence that the involvement of the private sector in the regulatory process emerges from rent-seeking interests, in a way that is compatible with the regulatory capture theory (Stigler 1971; Posner 1974). For example, some interviewees noted the existence of special interests in the involvement of the private sector, and the prominent interest found was promotion of the use of specific manufacturers or products. This finding is consistent with the regulatory capture literature (Carpenter and Moss 2014; Mitchell and Munger 1991; Stigler 1971), which describes the way regulations are created in order to serve the interests of various interest groups, including the desire to promote the purchase of specific services or products (Grossman and Helpman 1996; Peltzman 1976). Thus, regulatory capture in cyber defense regulation processes is diagnosed, manifested in both the intent and the actions of actors from the private sector, alongside a causal link between the actors’ actions and the regulations that were created. This provides support for Hypothesis 2a.

The interviewees’ responses also provided some support for Hypothesis 2b, in terms of evidence of additional motives for the involvement of the private sector that can be described within the framework of regulatory capitalism (Carrapico and Farrand 2017). For example, there is evidence that the involvement of the private sector is “part of the rules of democracy,” that the role of the private sector is to be involved in these processes, and that the professional knowledge that exists in the private sector is (or should be) an inherent part of regulatory creation processes. These findings are consistent with the literature dealing with the unique characteristics of cyberspace that are regarded as requiring cooperation between states and the private sector (Clinton, 2011, 2015; Neutze and Nicholas 2011; Tropina 2015). More specifically, the explanations emphasize the increasing role of the private sector, as described within the theoretical framework of regulatory capitalism, according to which there is a division of labor between the private and public sector, especially in technological fields such as information security (Carrapico and Farrand 2017). Notably, the words of the interviewees indicate that regulatory capture and the public responsibility of the private sector, far from being mutually exclusive, co-exist in cyber defense regulation processes.

Finally, Kingdon’s multiple streams framework (Kingdon 2011) allows an additional point of view. According to this framework, actors from the private sector are policy entrepreneurs seeking to connect the streams of problems, policy alternatives, and politics (Kingdon 2011; Travis and Zahariadis 2002). Actors from the private sector have broad access to the alternative policies stream via a wide range of policy ideas created by professional experts (Kingdon 2011; Travis and Zahariadis 2002). According to the multiple streams framework, it is only when the three streams intersect that a window of opportunity is created for the adoption of a policy (Kingdon 2011; Travis and Zahariadis 2002). In this terminology, policy entrepreneurs from the private sector identify the window of opportunity by connecting a policy alternative to a problem from the problems stream and locating support from the political stream. In this way, policy entrepreneurs present policymakers with a package that includes both a problem and its solution, where this solution might be a regulation that encourages the use of the company’s products (Gorwa and Peez 2018). However, this interpretation leaves open the question of whether the formation of the package reflects capture or public responsibility (or both).

The current study offers an in-depth examination of the processes of creating regulation in cyber defense in Israel, presenting the viewpoints of various actors, including different actors from the private sector, and not focusing solely on the results of regulation. However, the study has a number of limitations. First, since it deals with the processes and not the results of regulation, it does not determine which of these processes actually influence the regulations that are created. Second, the study deals exclusively with regulatory creation in Israel; although Israel is an interesting case study, it is not possible to generalize the results to other states. Future studies can address these limitations by combining qualitative methodologies that focus on relationships between actors with quantitative methods that focus on the results of regulation. In addition, international comparisons are required.

In summary, the current study deals with the relationship between the public and private sectors in the field of cyber defense regulation. The analysis of interviews with various actors shows that the private sector in Israel, which includes defense organizations, security companies, and consulting companies, is deeply involved in the creation of regulation, both by creating a demand for regulation and by being involved in its content. The motives for this involvement are partly related to rent-seeking by interest groups, but there is also a desire on the part of actors from the private sector to contribute their professional knowledge in a way that reflects public responsibility. These findings offer a new perspective for analyzing the relationship between the public and private sectors, particularly in advanced technological fields where most of the field-specific professional knowledge is concentrated within the private sector, making those fields vulnerable to capture.

**References**

Adamsky, D. 2017. “The Israeli Odyssey toward Its National Cyber Security Strategy.” *The Washington Quarterly* 40(2):113–127.‏

Baram, G. 2017. “Israel Defense in the Age of Cyber War.” *Middle East Quarterly* 24(1):6399.

Baram, G. 2013. “The Effect of Cyberwar Technologies on Force Building: The Israeli Case.” *Military and Strategic Affairs* 5(1):23–43.

Boehm, F. 2007.“Regulatory Capture Revisited – Lessons from Economics of Corruption.” Internet Centre for Corruption Research (ICGG) Working Paper 22.

Braithwaite, J. 2008. *Regulatory Capitalism: How It Works, Ideas for Making It Work Better.* Cheltenham: Edward Elgar.

Cahill, D. 2015. *The End of Laissez-Faire? On the Durability of Embedded Neoliberalism*. Cheltenham: Edward Elgar.

Cavelty, M. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Cavelty, M., and A. Wenger. 2020. “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science.” *Contemporary Security Policy* 41(1):5–32.

Carpenter, D., and D. Moss. 2014. *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*. Cambridge: Cambridge University Press.

Carrapico, H., and B. Farrand, B. 2017. “Dialogue, Partnership and Empowerment for Network and Information Security: The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers*.*” *Crime, Law and Social Change* 67:245–263.

Carrigan, C. 2013. “Captured by Disaster? Reinterpreting Regulatory Behavior in the Shadow of the Gulf Oil Spill.” In *Preventing Regulatory Capture: Special Interest Influence and How to Limit It*, edited by D. Carpenter and D. A. Moss, 239–291. Cambridge: Cambridge University Press.‏

Chen, C. J., and S.W. Hung. 2010. "To Give or To Receive? Factors Influencing Members’ Knowledge Sharing and Community Promotion in Professional Virtual Communities.” *Information & Management* 47(4):226–236.

Clinton, L. 2011. “A Relationship on the Rocks: Industry–Government Partnership for Cyber Defense.” *Journal of Strategic Security* 4(2):97–111.‏

Clinton, L. 2015. “Best Practices for Operating Government–Industry Partnerships in Cyber Security.” *Journal of Strategic Security* 8(4):53–68.‏

Cornish, P. 2015. “Governing Cyberspace through Constructive Ambiguity.” *Survival* 57(3):153–176.

Dal Bó, E. 2006. “Regulatory Capture: A Review.” *Oxford Review of Economic Policy* 22(2):203–225.‏

De Bruijn, H., and M. Janssen. 2017. “Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies.” *Government Information Quarterly 34*:1–7.

Galinec, D., D. Moznik, and B. Guberina. 2017. “Cybersecurity and Cyber Defence: National Level Strategic Approach.” *Automatika* 58(3):273–286.

Giese, K. 2020. “Coronavirus Disease 2019’s Shake-up of Telehealth Policy: Application of Kingdon’s Multiple-Streams Framework.” *Journal of Nurse Practitioners* 16:768–770.

Gorwa, R., and A. Peez. 2018.“Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft’s Cybersecurity Tech Accord.‏” Peace Research Institute Frankfurt Working Paper 11.12.2018.

Grossman, G. M., and E. Helpman. 1996. “Electoral Competition and Special Interest Politics.” *Review of Economic Studies* 63(2):265–286.‏

Kingdon, J. W. 2011. *Agendas, Alternatives and Public Policies, 2nd Ed.* New York: Longman.

Koop, C., and M. Lodge. 2015. “What Is Regulation? An Interdisciplinary Concept Analysis.” *Regulation & Governance* 11(1):1–22.

Lafen, S. 2018. “U.N. Regulation: The Best Approach to Effective Cyber Defense?” *Syracuse Journal of International Law and Commerce* 45(2):249–274.

Laffont, J. J., and J. Tirole. 1991. “The Politics of Government Decision-Making: A Theory of Regulatory Capture.” *The Quarterly Journal of Economics* 106(4):1089–1127.‏

Lawson, S. 2013. “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats.” *Journal of Information Technology & Politics* 10(1):86–103.‏

Levi, M. 2017. “Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues.” *Crime, Law and Social Change* 67(1):3–20.

Levi-Faur, D., and J. Jordana. 2005. “Globalizing Regulatory Capitalism.” *Annals of the American Academy of Political and Social Science* 598: 6–9.

Levi-Faur, D. 2011. “Regulation and Regulatory Governance.” In *Handbook on the Politics of Regulation*, edited by D. Levi-Faur, 3–24. Northampton, MA: Edward Elgar.

MacKinnon, L., L. Bacon, D. Gan, G. Loukas, D. Chadwick, and D. Frangiskatos. 2013. “Cyber Security Countermeasures to Combat Cyber Terrorism.” In *Strategic Intelligence Management*, edited by B. Akhgar and S. Yates, 234–257. London: Butterworth-Heinemann.

Mee, P., and J. Morgan. 2017. *Developing a Cyber Risk Strategy: Five Key Moves beyond Regulatory Compliance*. New York: Oliver Wyman.

Miao, L., L. Wang, S. Li, H. Xu, and X. Zhou. 2018. “Optimal Defense Strategy Based on the Mean Field Game Model for Cyber Security.” *International Journal of Distributed Sensor Networks* 15(2):1–10.

Mitchell, W. C., and M. C. Munger. 1991. “Economic Models of Interest Groups: An Introductory Survey.” *American Journal of Political Science* 35: 512–546.

Neutze, J., and J. P. Nicholas. 2011. “Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms.” *Georgetown Journal of International Affairs* 2013(14):3–15.‏

Peltzman, S. 1976. “Toward a More General Theory of Regulation.” *Journal of Law and Economics* 19(2):211–240.

Peterson, D. 2013. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36(1):120–124.

Posner, R. A. 1974. “Theories of Economic Regulation.” *Bell Journal of Economics and Management Science* 5(2): 335–358.

Stanifer, S., and E. Hahn. 2020. “Analysis of Radon Awareness and Disclosure Policy in Kentucky: Applying Kingdon’s Multiple Streams Framework.” *Policy, Politics & Nursing Practice* 21(3):132–139.

Stigler, G. J. 1971. “The Theory of Economic Regulation.” *Bell Journal of Economics and Management Science* 2(1):3–21.

Vogel, S.K. 1996. *Freer Markets, More Rules: Regulatory Reform in Advanced Industrial Countries.* Ithaca: Cornell University Press.

White, J. 2016.*The Cost of Carelessness*.‏ Medford: Tufts University.

Wiggins, J., C. Erlanger, & T. Harris. 2015. *Regulatory Efforts to Improve Cyber Security*. Washington, DC: Office of Nuclear Security and Incident Response