**Regulatory capitalism or regulatory capture? Analyzing the relationship between the public and the 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 high-priority at the national level, and promote the use of regulatory mechanism. The study looks at the processes of creating cyber defense regulation in Israel, through theoretical framework that examines the relationship between the public and private sectors, based on the regulatory capture theory, regulatory capitalism, and Kindgon's multiple-streams. 31 interviews were conducted, with representatives of various actors involved in these processes: politicians, regulators, bureaucrats, and representatives of defensive organizations, cyber security companies, and consulting companies. The analysis reveals a complex picture in which on one hand, policy processes are "captured" by interest groups, but on the other hand, the involvement of the private sector occurs out 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 offering an in-depth look over the processes of creating regulation, in addition to treating the private sector as composes out of various and different actors.

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

**Introduction**

Cyberspace is a unique space in many aspects, such as the lack of physical boundaries within it, and its embedded technology. In recent years, the prevalence and the severity of cyber events and attacks have been increasing, and in light of this, cyber protection is becoming more significant both for the private sector and for states. Based on this, state regulation has been developed, which regulates 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 theory is the regulatory capture theory, according to which, a policy process such as regulation might be "captured" by the 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, in recent years, another approach based on neo-liberal economic has developed, and in the center of it the concept of "regulatory capitalism". According to this approach, the increasing involvement of the private sector in the regulation creation processes does not necessarily reflects 'capture', but is occurring out of a developing perception of the role and public responsibility of the private sector (Lev-Faur 2010; Carrapico and Farrand 2017; Cahill 2015; Vogel 1996; Braithwaite 2008; Levy-Faur and Jordana 2005).

The aim of the current study is to explore the relationship between the private and public sectors in the regulation creation processes, using a case study of cyber defense regulation in Israel. For this, an integrated framework is used, which include regulatory capture theory, regulatory capitalism, and in addition, the Multiple Streams Framework (Kingdon 2011), in order to conduct a qualitative content analysis of interviews with various actors involved in the relevant processes.

**Literature review**

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 within it, such as the rapid changes it goes through, the irrelevance of the physical distance, its relative anonymity, and so on. The risk of this deteriorating trend is affecting personal and state security and economic activity, and demands consideration at the national level, that is developing national cyber defense (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, Moznik and Guberina 2017, 273). Cyber defense policy is focused on prevention, identification and timed responses to attacks or threats on information infrastructures (Galinec, Moznik and Guberina 2017). In recent years, developing cyber policy include innovative defense methods for the new posed challenges (Miao *et al*. 2018).

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

1. **The relationship between the private and public sectors in the creation of regulation**

Several studies dealing with cyber defense regulation have focused on the aspects of the relationship and cooperation between the private and public sectors (Lafen 2018; Clinton 2011; Clinton 2015; Tropina 2015), and based on the assumption that due to the unique characteristics of cyberspace, protection requires this cooperation (Clinton 2011; Clinton 2015; Neutze and Nicholas 2011; Tropina 2015). This argument is based on cyberspace characteristics such as the fact that computer networks are operated mainly by the private sector, and the state does not have the technical ability to fully implement cyber defense (Clinton 2015), alongside the supranational nature of cyber defense that 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 two sectors raises many problematic 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 the regulation does not enable to maximize the benefits of the public-private sector partnership (Clinton 2011; Clinton 2015; Tropina 2015), because it does not allow an equal relationship between the sectors, and thus, not contribute to the building trust between them (Clinton 2011; Clinton 2015; Tropina 2015). In addition, most business organization do not want their cyber departments to be under government regulation (Lafen 2018). Nevertheless, in recent years, there have been attempts to address knowledge and skills that exist in the private sector, as inherent component in these processes (Slayton and Clark-Ginsberg 2018; Cavelty 2008).

Several studies in recent years (e.g. Carrapico and Farrand 2017; Slayton and Clark-Ginsberg 2018) suggest that in the field of cyber defense, the private sector has a unique role in developing public policy, that differ from its role in other industries. Slayton and Clark-Ginsberg (2018) argue that there is a difficulty to distinguish between legitimate cooperation between the public and private sector, and the existence of regulatory capture, in which interest groups influence regulatory creation (Posner 1974; Stigler 1971; Carpenter and Moss, 2014). Carrapico and Farrand (2017) claim through the lens of a Regulatory Capitalism theoretical framework 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 (in the current study, divided into three main actors: the defensive business organizations, the security companies, and consulting companies), the theoretical framework will now be discussed. This framework is based on three existing theories: the regulatory capture theory (Posner 1974; Stigler 1971), regulatory capitalism (Braithwaite 2008), and the Multiple Streams Framework (Kindgon 2011).

* 1. **Regulatory capture theory**

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

Regulatory formation can be described as an economic process of supply and demand, where interest groups have a demand for the regulation and they are willing to pay for it, and politicians have a regulation to offer by virtue of their ability to create one, which they are willing to sell at the maximum price (Posner 1974; Stigler 1971). According to a definition provided by Carpenter and Moss (2014), in their book "Preventing Regulatory Capture", in order to "diagnose" capture in an industry, one must identify a change in the policy from an action in favor of the public interest to another special interest of the industry, and in addition, to show both intention and action on part of the industry or interest groups, in chase of this change in policy. The current study adopts this definition, but in addition, the analysis of the interviews makes it possible to detect a casual correlation between the change of policy and the activities of the actors.

* 1. **Regulatory capitalism**

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

The term "Regulatory Capitalism" is based on the neo-liberal economic approach (Carrapico and Ferrand 2017). At the same time, theoretical neo-liberal ideas significantly differ from their actual application, which is describe as "actually existing neoliberalism" (Cahill 2015; Vogel 1996). In practice, instead of the expected deregulation process, one can notice a process of re-regulation, in which regulatory bodies and agencies are proliferating, both quantitatively and in terms of responsibilities given to them (Braithwaite 2008; Levy-Faur and Jordana 2005). Therefore, due to the significant increase in the existence of non-state regulation, a large number of authors propose to refer to this process as "regulatory capitalism" (Carrapico and Farrand 2017; Braithwaite 2008; Levy-Faur and Jordana 2005; Cahill 2015).

Regulatory Capitalism provides a general framework for understanding processes such as the growing role of the private sector in the division of labor between the private and public sectors (Carrapico and Farrand 2017). In the background of occurring privatization processes, the formation of independent regulatory bodies is perceived as necessary (Braithwaite 2008). Although the private sector, traditionally, is not included in the list of regulatory bodies, it is taking an increasing role in this re-regulation process, by encouraging state and regulatory agencies regulation, especially in 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). Therefore, the following section briefly presents this theory.

* 1. **Kingdon's Multiple Streams Framework**

Some recent studies have used the Kingdon's (2011, originally in 1995) Multiple Streams Framework 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, politicians, and so on (Kingdon 2011; Travis and Zahariadis 2002), that might form into concrete policy proposals, or simply disappear (Travis and Zahariadis 2002). The political stream includes mainly the change of bureaucrats and politicians, and the consequent change in the political attitude (Travis and Zahariadis 2002). Kingdon's model suggests that the combination of streams, in some point in time, create 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 as a "package" of both "problem and solution" to a policymaker who is interested in such a package (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 the review presents the Israeli case, and its significance to analyzing the relationships between the private and public sectors in the field of cyber defense.

1. **The Israeli case**

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

The characteristics of the Israeli case, where on the one hand there is technological pioneering in the field of cyber defense (Adamsky 2017; Tabansky 2017), but on the other hand, a lag behind in aspects of regulation and policy (Adamsky 2017; Sabillon *et al.* 2016), make the Israeli case unique and interesting for analyzing private-public sectors relationships (MacKinnon *et al*. 2013).

**Rationale of the current study**

Most of the recent studies that have dealt with the relationship between the private and public sectors in the context of cyber defense regulation focused on quantitative variables, such as regulatory outcomes, and have tended to treat the private sector as a single and coherent actor. The current study contributes to the existing literature in these two aspects. First, the study does not deal with the results of the regulation but offers a perspective on the processes of regulatory formation, as they are reflected in the words of the different actors. Second, the private sector is not treated as a single, coherent actor, but as containing at least three different actors: the defensive organizations, security companies, and consulting companies. The implementation of the qualitative approach shed new light on the dynamics and the relationships between the various actors, in the context of an evolving technological field such as cyber defense regulation.

**Methodology**

**Study design**

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

**Research model and questions**

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

**Research hypothesis:**

1. The private sector (defensive organizations, consulting companies and information security companies) is trying to influence politicians by creating a demand for regulation.
2. The private sector takes an active role in the processes of creating regulation and influences its content.
3. What are the motives for the involvement of the private sector in the processes of creating regulation?

**Research hypothesis:**

1. In accordance with regulatory capture theory, interest groups from the private sector are involved in the process of creating regulation out of rent-seeking.
2. 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.

**Participants**

In total, 31 interviews were conducted with representatives of the regulatory process: regulators and bureaucrats, politicians, high-ranking officers in the National Cyber Directorate (INCD), and various representatives of the private sector. The politicians were of different authorities: The Israel National Cyber Authority (NCSA), the Israel National Cyber Bureau (INCB), the Israel Director of Security of Defense Establishment (Malmab), representatives of the Israel legislature (the Knesset), and representatives of the INCD. The respondents from the private sector were representatives of manufacturers and communications systems, of various defensive organizations, and consulting companies. Some of the interviewees can be regarded as representing more than one group in cases where an interviewee previously represented another actor. In these cases, the interviewees were asked about the perspectives of two different actors. so, in total, 18 interviewees represented the public sector (9 regulators or bureaucrats, 3 politicians, 6 from the INCD), and 14 interviewees represented the private sector (11 from defensive organizations, 3 from other interest groups). 3 of the respondents were professionals in another aspect of cyber defense (such as academia or media).

**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 question like: Who are the actors that influence regulation? What are the roles of each actor? What are the power relations between those actors and how do these relationships change over time? What drives the regulatory/decision-making process? And so on.

**Data analysis**

The analysis of the interviews was done via content analysis. In the first stage, the author read the transcripts of the interviews entirely and identified the main themes. In the second stage, the statements of the interviewees were systematically divided 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 hypothesis.

**Results**

Most of the interviewees, from different roles and different organizations, explicitly stated that actors from the private sector, such as defensive organizations, security companies and consulting companies, influence regulation. Interviewees who mentioned this, described two different, complementary, non-exclusive ways of influence: the first is creating a demand for regulation, that is, influencing regulators to create regulation. The second is influencing the content of the regulation. In this way, actors from the private sector intervene in the content of regulation, out of various motives. Based on this, the results chapter is organized and divided into four parts, according to the described above research hypotheses.

**Creating a demand for regulation**

A large part of the respondents stated, explicitly or implicitly, that various actors from the private sector are actively creating a demand for regulation. 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, defensive organization). For example, one of the interviewees explain that:

There are all kinds of stakeholders who influence the regulators, try to influence the regulators, call them 'lobbists'. Not exactly lobbists, but there are those who actually activate lobbists 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 one of the cyber security companies. By this description, information security companies activate influence on regulators in order to create regulation. This interviewee says this explicitly.

An almost identical argument, from which the existence of a demand for regulation by actors from the private sector emerges, was raised also by interviewee 19 which represents the consulting companies: "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, by this interviewee, consulting companies will generate a demand for regulation that will increase their sales.

The citations presented in this section are just a few examples of issues raised by many interviewees, from which it is clear, and in support of the first research hypothesis, that various actors from the private sector are actively creating a demand of regulation.

**Influence on the content of regulation**

The second way in which different actors from the private sector influence regulation is through 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).

Out of this quote it can be seen that the interviewee claims that actors from the private sector, in this case information security companies, not only influence the process of creating regulation, but also on the content of regulation. In this case, interviewee 15 does not claim that information security companies initiated a demand for the privacy security standards GDPR, however, he states that they were involved in the drafting stages.

In the answers of interviewees who referred to other actors from the private sector, such as consulting companies, evidence can be found also that, in similar to 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 the defensive organizations (18) and information security companies (7), which belong to the private sector, emphasize that the impact of consulting companies on the content of regulation is widespread because they write the regulation for the regulators. The answer of another interviewee, who represent one of the defensive organizations, expands more on 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 do not only influence the content of regulation, they also do it in a way that is in line with their interest. She emphasizes that consulting companies do not get paid from the regulators for their services but are rewarded by advancing their interests.

Support was thus found for the second research hypothesis, which argued that the private sector takes an active role in processes of creating the regulation and influence its content. This aspect is also related to the next section, which is the existence of regulatory capture.

**The existence of regulatory capture – involvement out of rent-seeking**

In the words of the respondents, there can be found a large number of evidences for the existence of regulatory capture, by its definition that is adopted 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 told 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 in account. It is influenced. (Interviewee 19)

This interviewee expresses in her own words, but precisely, the idea of regulatory capture. She describes how the regulation's initiative 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 an intention and action in creating regulation.

Another respondent, represents both the private sector for his past work and the Cyber Directorate in the present, also refers to the consulting companies, and claims 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 influence: the writing of various procedures and documents for regulators, which are in fact "captured" by the interests of interest group from 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 of innocently, usually the representatives of the security companies will be biased in favor of the products in which they work for. 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 month, 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 regulation for the regulators, such that the regulation will 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 the third research hypothesis, the interviewees illustrate the existence of regulatory capture in the processes of creating and designing regulation in the field of cyber defense in Israel. That is, various actors from the private sector are involved in the processes of creating the regulation out of a desire to advance their own interest.

But is rent-seeking really the main motive for the involvement of the private sector? In this aspect, the next section deals with the evolving responsibilities of the private sector in the field of cyber defense.

**Regulatory Capitalism – public responsibility of the private sector**

As the interviewees say, the involvement of the private sector also stems from other motives, which do not necessarily reflect narrow interests of the various actors. There can be found also a lot of evidence for the involvement of the private sector in regulation processes out of a growing public responsibility. For example, this interviewee claims that:

If it's a government so [one the security companies] are there a lot and [another security company] because they won the tender 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 create regulations that are Israeli. (Interviewee 7)

This interviewee, which represents the private sector through the security companies, claims in the beginning of the quote that information security companies do not influence the regulators. But in the same breath he adds that he himself was involved in such an influence process in the past. Moreover, the interviewee states that managers "do not do enough", that is, by his perception, influencing regulation is part of the role of managers in information security companies, and if they do not influence the regulation, they do not perform 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 of sorts of such processes, but these are moves that are part of democracy. (Interviewee 16)

The Interviewee adds that he does not see this process as normatively problematic, because it is a 'part of democracy'. One of the interviewees, who represents the information security companies, 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)

In these things it is shown the complexity that exists in the involvement of the private sector in the processes of creating regulation. On one hand, there is a widespread agreement that this involvement is positively exists, and even legitimately in few aspects such as being part of the 'rules of the democratic game'. At the same time, it is shown that it is the responsibility of the private sector to contribute from its professional knowledge, but still to remain "neutral", and act without specific interests.

The fourth research hypothesis in the current study was 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 to determine unambiguously whether there has been such a development, but there is evidence that the private sector has an important role in these processes.

**Discussion, summary, and conclusion**

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

From the words of the interviewees emerges saliently that actors from the private sector create a demand for regulation. This idea is found, this way or another, in the words of most of the respondents. These findings are consistent with the literature describing that although the private sector is traditionally not included in the list of regulatory bodies, it takes a developing role in the regulation processes, through encouraging the state and regulatory agencies to create regulation (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 compatible with the literature which describes the relationship between the private and public sectors in this field as demanding cooperation between states and the private sector, due to the unique character of cyberspace (Clinton 2011; Clinton 2015; Neutze and Nicholas 2011; Tropina 2015). In support of the two first hypothesis in this study, according to the interviewees, the involvement of the private sector is manifested in professional counselling to politicians, and also in writing and drafting the regulation itself, that is, both in creating a demand for regulation and influencing its content.

The words of the interviewees also show evidence that the involvement of the private sector in the regulatory process emerges out of rent seeking interest, 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, while the prominent interest found was the will to promote 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 regulation is created in order to serve the interest of various interest groups, with one of the described topics that is the desire to promote the purchase of specific services or products (Grossman and Helpman 1996; Peltzman 1976). That is, in support of the third research hypothesis, a regulatory capture was 'diagnosed' in the cyber defense regulation processes, manifested in both intent and action of actors from the private sector, alongside a casual link between the actors' action and the actually created regulation.

Nevertheless, in the words of the interviewees there was also found some support for the fourth research hypothesis, through evidence to additional motives for the involvement of the private sector, which can be described under the framework of "Regulatory Capitalism" (Carrapic and Farrand 2017). For example, there was evidence that the involvement of the private sector is 'a 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 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 characteristic of cyberspace which requires cooperation between states and the private sector (Clinton, 2011; Clinton, 2015; Neutze and Nicholas, 2011; Tropina, 2015), and in particular, the explanations described under the theoretical framework of Regulatory Capitalism, according to which, the division of labor between the private and public sector, and especially in technological sectors such as information security, emphasize the increasing role of the private sector (Carrapico and Farrand 2017). Importantly, the words of the interviewees show that public responsibility of the private sector, and regulatory capture, co-exist, and do not exclude each other, 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', looking to connect between the streams of 'problems', 'policy alternatives', and 'politics' (Kingdon 2011; Travis and Zahariadis 2002). Actors from the private sector have broad access to 'alternative policies stream', using 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 in some point in time, a window of opportunity is created in which policy can be adopted (Kingdon 2011; Travis and Zahariadis, 2002). In this terminology, policy entrepreneurs from the private sector identify this window of opportunity by connecting policy alternative to a problem from the problems stream, and by locating support from the political stream. In this way, policy entrepreneurs present in front of the policymakers a 'package', that include both the problem and the solution, where this solution might be a regulation that will encourage the use of the company's products (Gorwa and Peez 2018). Yet, this interpretation still leaves open the question whether this 'package' formation reflects 'capture' or public responsibility (or both).

The current study offers an in-depth look over the processes of creating regulation in Israeli cyber defense, since it presents viewpoints of the various actors, includes different actors from the private sector, and does not focus only on the results of regulation. However, the current study has number of limitations. First, since this study deals with processes and not the results of regulation, it is hard to tell which of these processes actually influence the created regulation. Second, the study deals with regulatory creation only in Israel, and 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 the relationship between actors, and quantitative methods that focus on the results of regulation. In addition, an international comparison is required.

In summary, the current study deals with the relationship between the private and public sectors in the field of cyber defense regulation. The analysis of interviews with the various actors shows that the private sector in Israel, which include various actors such as defensive organization, security companies and consulting companies, is deeply involved in the creation of regulation, both in creating a demand for regulation, and in involvement in its content. The motives for this involvement are partly related to rent seeking interests of interest groups, but alongside them there is also a desire of actors from the private sector to contribute from their professional knowledge, in a way that reflects public responsibility. These findings offer a new perspective for analyzing the relationship between the private and public sectors, and particularly in advanced technological fields, which are vulnerable to be 'captured' by the industry, since most of the field-specific professional knowledge is concentrated within the private sector.

**Bibliography**

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* Winter 2017.

Baram, G. 2013. "The effect of cyberwar technologies on force building: The Israeli case." *Military and Strategic Affairs* 5(1).

Boehm, F. 2007."Regulatory Capture Revisited–Lessons from Economics of Corruption." Working Paper.

Braithwaite, J. 2008. *Regulatory capitalism: how it works, ideas for making it work better.* Edward Elgar, Cheltenham

Cahill, D. 2015. *The end of laissez-faire?: on the durability of embedded neoliberalism*. Edward Elgar, Cheltenham, UK.

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.

Cavelty, M. 2008. *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge

Carpenter, D. and D. Moss. 2014. *Preventing regulatory capture*. Cambridge University Press

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 & 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.

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 Soc Change* 67:245-263.

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." *The 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*.‏ Working Paper.

Grossman, G. M., and E. Helpman. 1996. "Electoral competition and special interest politics." *The Review of Economic Studies* 63(2):265-286.‏

Kingdon, J. W. 2011. *Agendas, Alternatives and Public Policies*. (2nd ed.). 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.

Levy-Faur, D. and J. Jordana. 2005. "Globalizing regulatory capitalism." *The 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*. 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." *The 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*." The 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." *The 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.* Cornell University Press, Ithaca.

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