PAPER
DECEMBER 2020

UNIVERSITÀ DEGLI STUDI FIRENZE

TOWARDS THE CENTRAL ROLE OF CYBER SECURITY: THE CASE OF ISRAEL

CAMILLA LUPERTO

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

TOWARDS THE CENTRAL ROLE OF CYBER SECURITY: THE CASE OF ISRAEL

Camilla Luperto

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

December 2020

ABOUT THE AUTHOR

Camilla Luperto is Master student in Public and Political Communication Strategies at School of Political Science “Cesare Alfieri” (University of Florence). Consistently with her interest in cyberspace and, more specifically, with this new domain’s security issues, she is currently writing her Master thesis on the Israeli approach to cyber security policy. She also collaborates as research assistant at the Centre for Cyber Security and International Relations Studies (CCSIRS) at the University of Florence. In particular, her research interests include diplomatic efforts and initiatives in the cyber domain.

TOWARDS THE CENTRAL ROLE OF CYBER SECURITY: THE CASE OF ISRAEL

Introduction

In the new era of cyberspace, nation-states have to face new threats and new challenges that are increasingly blurring boundaries. Threats can come from both public and private actors, damages can be both virtual and physical, cyber attacks can be both isolated or part of a cyber war. In such a complexity, as we will see, a nation-state in particular seems to know how to manage it: Israel. Indeed, we will take it as a case-study to better understand why cyber security has become so important and how Israel has developed such a superiority in this sector. To do so, we will consider the country's peculiarity under the light of the new challenges that cyber space arises, and we will provide an example of cyber attack that Israel had to face.

To approach the issue, we will adopt a qualitative case study approach. Starting from a theoretical overview of cyber space and Israel's concept of defence, we will then move to the empirical level to find the application of the theoretical concepts. We will, therefore, analyse the Israeli national cyber security strategy as framed by both a general cyber defence and country's historical and geopolitical framework. At the end of the excursus we will provide an empirical evidence of Israel's defence capability through an example of cyber attack that the country has faced.

A new domain

Cyberspace needs cyber security

Far from having a unique definition, cyberspace has been described in various ways in the last 30 years. To simplify our subsequent analysis, we will consider just two of them. The first one comes from Kuehl who considers cyberspace as "an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructure" (Kramer et al.

2009, 4). Such a definition does not take into account the impact or value of information, but it emphasizes the physical and informational nature of cyberspace instead (Van Puyvelde and Brantly 2019, 26-7).

The second one is given by the US Department of Defense (DoD) and it identifies the cyberspace as composed by three layers: the physical network, which is the medium where data travel; the logical network, which is made by those elements that are related to one another in a way that is abstracted from the physical network; and the cyber persona which is the digital representation of an individual or entity identity in cyberspace (Van Puyvelde and Brantly 2019, 27).

What we get is therefore the profiling of a new domain which involves both physical and virtual elements and personas and comes in addition to the classical ones: land, sea, air and outer space. Such an innovation deeply affects the concepts of war and conflicts as long as it provides a new battlefield for old and new actors where boundaries appear blurred (Van Puyvelde and Brantly 2019, 28). Cyberspace can indeed host a wide range of activities like bullying, criminal activities, espionage and sabotage that can constitute an effective threat to critical infrastructures, economies, property and the well-being of citizens (Van Puyvelde and Brantly 2019, 91-92). In this sense, the plurality of the actors exceeds the limits of the nation-state's monopoly bringing us, as Joseph Nye underlines, in front of a diffusion of power where non-state actors are increasingly involved in this new domain (Martino 2018, 70).

At this point a clarification is needed: not all the cyber attacks are necessarily identified as act of war. Moreover, while some scholars like Thomas Rid think that "cyber war will not take place" thus delegitimizing the definition itself (Martino 2018, 69-70), the US government is of another opinion.

In their words, cyber war requires "to proximately result in death, injury or significant destruction" (Koh 2002). Such a controversy is emblematic of the contradictions and doubts that cyberspace arises thus being an open question itself which, nevertheless, gained a high degree of relevance in the political, social and economic discourse.

As a proof of it, we can see how cyber security has become a fundamental concept at the global level for a variety of actors who therefore attempt to guarantee both physical safety and national values protection (Van Puyvelde and Brantly 2019, 77).

In this sense, the continuous operation of a country's essential computer system is a core need. For a long time, it was common practice to refer to the protection of computer systems as "information security," reflecting the idea that the most important thing to be protected was sensitive information. More recently, this approach has been abandoned to include new threats like disruption of services and paralysis of essential computer-based processes which can be perpetrated by different actors (Baram 2013, 26).

The term "cyber warfare" is nowadays very common as it indicates "the actions by a nation-state or international organization to attack and attempts to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks" (Baram 2017, 1). This implies a deep connection between military communication infrastructures and their civilian counterparts which demands for computer's protection for both civilian and national security purposes (Baram 2017, 2). Indeed, hacktivists, cyber criminals, nation-state actors and cyber espionage, represent a real threat to both of these sectors (Fernandes et al. 2014, 426).

We are in front of a growing potential of cyber conflict which relies on our even more growing dependence on vulnerable technologies that can lead to both virtual and physical damages. In this sense, the Stuxnet episode constitutes a prime example in terms of cyber weapon with huge impact (Mc Graw 2013, 109-110) and may be one of the reasons for the centrality of cyber security in the policy agendas all around the world (Tabansky 2020, 48). It is therefore clear that security must be built in our systems to address the security problem and slow down the accelerating slide into cyber war (McGraw 2013, 109-10).

Israel: a case study

Two significant reasons make Israel a great example of cyber security's implementation. First of all, the nation sees around 1000 cyber attacks within a hierarchy of threats every minute (Benoliet 2015, 442-43) and yet it seems to handle them admirably, gaining a global recognition in terms of cyber defence apparatus. Second, Israel's exports more cyber related products and services than all other nations combined, excluding the US (Benoliet 2015, 442-43).

The centrality of cyber security in Israel is therefore undoubtable, but the deeper reason for that must be sought in a more specific environment, even if framed by the broader context of cyberspace.

Israeli peculiarities: the view of defence

The increasingly cybernetic nature of threats has made Israel adopt a security system which combines home-grown capabilities, relying on "Jewish" developments and inventiveness, with global technologies (Baram 2013, 27).

Moreover, the Israeli defence sector has been the first one to adopt the cyber technologies acknowledging their impact on trans-social issues (Tabansky 2013, 78). Evolving together with cyber technologies it is gaining relevant results and placing itself as a leader to be emulated in the international arena (Adamsky 2017, 113).

Though, the use of technology in the Israeli defence is not new. It has indeed been crucial since the early days of statehood aiming to establish a qualitative edge over its vastly more populated and better endowed Arab adversaries (Baram 2017, 1). Despite its small size, Israel gave proof of its unexpected strength and modernization in contrast with the general backwardness of the Middle East (Sabbatucci and Vidotto 2008, 243-44) in a conflict that dates back to the first decades of the XX century. The English authorization for the Zionist movement to create an official national headquarters for Jews in Palestine in those years, found indeed the Arabs' resistance who were creating a national movement (Sabbatucci and Vidotto 2008, 167). With the second world war and the creation of the state of Israel by the United Nations in 1948 the conflict was sanctioned (Sabbatucci and Vidotto 2008, 243-44).

In this sense, a superiority in cyberspace has been considered as an integral part of the country's deterrent attack capability, in the Middle East theatre and beyond, in order to maintain its security and its geopolitical location. This capability, as the country's history shows, has been gained turning the quantitative asymmetry into an advantage through the deviation of warfare to the technological plane. "It is easier for Israel to contend with the Arab world in sophisticated air battles and cyber operations (according to foreign sources) than in throwing stones or hand to hand fighting" (Baram 2013, 26-27).

But as long as threats come from multiple side, the ability to protect the essential computer networks is increasingly needed. Israel is indeed subject to about one thousand cyber attacks at any given moment that are likely to disrupt its way of life by damaging its economy, industry, security, or education (Baram 2013, 24). In this sense, "the use of cyber tools, which requires the training of expert manpower rather than the

exertion of great physical force, facilitates operations that help bolster Israel's deterrent capability, and garners it great prestige in the international arena" (Baram 2013, 27-28). Also, "all that is necessary is a high level of trained manpower for developing systems that make it possible to carry out operations against remote targets without risking human life and without requiring many resources" (Baram 2013, 27-28).

Such an acknowledgement both arises and justifies the more punctual Israeli concept of defense which dates back to the pre-state era and which, conscious of the elusiveness of the peace, continued to evolve. In this sense, in order to face the many threats that it had to address after the war of independence (Benoliet 2015, 3-4), two main principles have been adopted.

Firstly, the idea of "an army of the people" that could rapidly mobilize and comprise mainly of draftees on mandatory military service and reserves.

Secondly, the "security triangle" constituted by the three main concepts: deterrence, early warning and a decisive operational victory (Baram 2017, 3-4). While the first one refers to develop defensive and offensive capabilities in order to discourage the country's enemies from attacking it; the second one denotes receiving advance warning about developments in neighbouring countries that could represent a threat to Israel's security; and the last one is predicated on building sufficient military power to win a conflict if the previous one fails (Baram 2017, 3-4).

Israel's cyber security

Once we clarified what have may made cyber security so vital for Israel, we can turn theory into practice that is analysing how this system effectively works. Approaching to the country's cyber odyssey and its crucial point we try to address the question about the reason of the Israeli leadership in the international cyber defense scenario, to conclude with an example of cyber attack.

Towards a model of cyber strategy

Israel's cyber national strategy had to pass through a cyber odyssey before it could see the light, but with the result of being the Israeli first successful effort to produce a coherent national security strategy that drives long-term policy formulation and regulates it operational execution (Adamsky 2017, 122-23).

Even if cyber security's activities have already started in the country in the mid 1990s, an information technology (IT) security efficiency across the government didn't show up until 2002. The government's realization that cyber security was not just a technical matter but a huge policy issue that demanded cultural-organizational transformation, has indeed been part of a gradual process of acknowledgement (Adamsky 2017, 114).

That year, the 'Special Resolution B/84' opened the era of a national civilian cyber security policy (Tabansky 2013, 79) with the establishment of the critical infrastructure protection (CIP) and the definition of the goals and means of the country cyber security (Adamsky 2017, 115).

Since then, updates and revisions have been an ongoing process as cyber risks rapidly intensified together with the growth of cyberspace. The Prime Minister itself, Benjamin Netanyahu, launched in 2010 an initiative aimed to review on cyber security and Israel's policy thus forming the basis for a substantial change under the vision "to preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities in cyberspace, to ensure financial and national resilience as a democratic, information-based, and open society" (Tabansky 2013, 81).

Adopting the recommendations of the National Cyber Initiative, the Government Resolution 3611, "Advancing the national capacity in cyberspace", was passed in August 2011 establishing the Israel National Cyber Bureau (INBC) in the Prime Minister's office (Tabansky 2013, 82-84).

Three years of internal staff work by the INCB resulted in two legislative initiatives: the establishment of the National Cyber Security Authority in 2015 and the publication of the comprehensive National Cyber Security Strategy as the culmination of an almost decade-long odyssey thus providing a comprehensive policy framework (Adamsky 2017, 116-17).

Key points in the cyber strategy

The comprehensive policy framework given by the national strategy provides some clue in order to understand how the Israeli cyber security really works and why it has become such a power.

In this sense we should point out the three interrelated vector that shape this framework: (a) concept of operations, which outlines the actual set of activities aimed at cyber defense; (b) capacity building which outlines the set of R&D, industrial, and educational undertakings aimed at producing capabilities enabling the concept of operations; (c) and structure that outlines the mandate and configuration of the Israeli National Cyber Directorate (INCD) responsible for overseeing the first two endeavours (Adamsky 2017, 116-17).

Between them, concepts like robustness and resilience characterized by a defensive nature, and defence by both a defensive and offensive one, seem to gain particular relevance.

But let's see them closely. Robustness refers to "the capacity of the organization to perform without failure, by repelling and containing threats in the national cyber domain" (Adamsky 2017, 117) under a wide range of conditions.

Resilience highlights instead the "capacity to handle attacks in order to regain overall normal functioning" of the organization. In other words, it is the ability to recover from threats and the state's capability to prevent the potential cumulative national effect of these strikes.

Finally, the defence concept stands for the national efforts of both offensive and defensive nature. Going back to their defensive or offensive nature, it will appear crucial as it highlights a dualism which is reflected in, respectively, the deterrence by denial or by punishment (Adamsky 2017, 117-18). In the cyber domain, deterrence has gained both a central and an ambiguous role as long as cyberspace is facing the problem of the identity of the perpetrator, that is the problem of the attribution. This latter is indeed a substantial challenge to effective cyber defence which as Jon Lindsay pointed out "requires great technical expertise, analytical skill, and organizational coordination" (Van Puyvelde and Brantly 2019, 132-33).

To solve this, Israel has developed a unique technique which might be one of the reasons of its success: the perpetrator-indifferent approach that encompasses the entire range of cyber challenges and creates a national-level holistic remedy. The core idea is the fact that protection of the specific asset is more important than dealing with the perpetrator. This leads to focus on critical national targets that should be protected against threats (Adamsky 2017, 121-22) which indicates that Israel has correctly identified the looming threat to its national

infrastructures, thus acting to set up a defense apparatus at the national level (Baram 2013, 31).

An example of cyber attack: Op-Israel

"The most influential action for shaping threat perception education is the discovery by a government that their networks have been penetrated" (James 2014, 571). Taking this for grant, even if Israeli officials says that the campaign Op-Israel "was a minor irritation compared to cyber attacks that originated in Iran and Gaza" (James 2014, 571), this attack is useful for our purpose in a broader analysis of cyber threats.

Op-Israel indicates a campaign of cyber attacks carried out by the hacker group Anonymous together with pro-Palestinian hacker groups, against Israeli Internet sites to disconnect the country from the cyber world.

The first cyber attack has been perpetrated on the eve of Holocaust Remembrance Day on April 7, 2013 and becoming since then an annual tradition which includes a variety of attacks: from crashing websites to preventing them from providing services, from hacking databases and leaking information to taking control of websites interfaces and defacing pages (ICT 2017).

The peculiarity of Op-Israel lies on the psychological damage which, outweighing the economic one which is still not clear, aims to influence public awareness (ICT 2017).

It is indeed an act of activism which finds its reason why in the Israeli-Palestinian cyber warfare began in October 2000, shortly after the Lebanese Shi'ite Hezbollah movement abducted three Israeli soldiers (Denning 2001, 1). Still growing since then, the Israeli-Palestinian cyberwar illustrates a growing trend in which cyberspace is increasingly used as a digital battleground for rebels, freedom fighters, terrorists and others who employ hacking tools to protest and participate in broader conflicts. In this scenario, hacktivists like Anonymous believe that nation-states are not the only actors allowed to engage in war and aggression (Denning 2001, 1).

Thinking of this, it will then appear clear that, even if the of Op-Israel campaign is not considered a big threat to the Israeli nation, it is still interesting in a broader sense as long as it is emblematic of the

multiplicity of threats. Actors involved are no longer just political or military thus aiming for a more inclusive view on the security sector.

More relevant to our analysis, this episode constitutes an empirical evidence of the effective Israel's capability in cyber security. Jerusalem was in fact well-prepared for these attacks as the national Computer Emergency Response Team (CERT) reported that most of the websites attacked were operating normally (Baram 2017, 8).

Conclusions

The optimal preparation of Israel to cyber attacks constitutes an empirical evidence that the country can really be considered a reference case in the implementation of cyber security. What we have tried through our analysis to identify the reasons for this success and for the centrality itself of cyber security for Israel. Starting from a broader contextualization of the cyber domain, we have attributed those reasons to the rise of new challenges and to the country's geopolitical and historical peculiarity. In this sense, we have seen how the Israeli concept of defence has shaped the national cyber security strategy which has been explored to understand if this could be the reason for its leadership in the sector. It seems that the need of keeping this little nation safe from the thousands of daily attacks has been translated into a national-level holistic remedy which mostly relies on the concept of deterrence. A concept that, in its high ambiguity, has been nevertheless faced by Israel with its perpetrator-indifferent general approach.

Still, challenges in cyberspace are always increasing and the question if such an approach can be the right one remains open; especially if we consider the declination of the deterrence by punishment which is not excluded, even if not preferred, by Israel.

References

Adamsky, Dmitry. 2017. "The Israeli Odyssey toward its National Cyber Security Strategy." *The Washington Quarterly* 4, no. 2: 113-127. https://doi.org/10.1080/0163660X.2017.1328928.

Baram, Gil. 2013. "The Effect of Cyberwar Technologies on Force Buildup: the Israeli Case." *Military and Strategic Affairs* 5, no. 1: 23-43.

Baram, Gil. 2017. "Israeli Defense in the Age of Cyber War." *Middle East Quarterly* 24, no. 1 (Winter) 1-10.

Benoliel, Daniel. 2015. "Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study." *North Carolina Journal of Law & Technology* 16, no. 3: 435-486.

Denning, Dorothy. 2001. "Cyber Warriors: Activist and Terrorist Turn to Cyberspace." *Harvard International Review* 23, no. 2: 70-75.

Fernandes, Diogo A.B., Liliana F.B. Soares, João V. Gomes, Mário M. Freire, and Pedro R.M. Inácio, 2014. "A Quick Perspective on the Current State in Cyber security." In *Emerging Trends in ICT Security*, edited by Babak Akhgar and Hamid R. Arabnia, 423-442. Waltham: Elsevier.

International Institute for Counter Terrorism (ICT). "ICT Cyber-Desk Report: Op-Israel 2017." Cyber Desk Report, March 28, 2017. Accessed September 8, 2020. https://www.ict.org.il/Article/1975/Op-Israel#gsc.tab=0.

Koh, Harold Hongju, "International Law in Cyberspace." Keynote address at the US Cyber Command Inter-Agency Legal Conference. September 18, 2002.

Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz. 2009. *Cyberpower and National Security*. Washington DC: National Defense University Press.

Lewis, James A. 2014. "National Perception of Cyber Threats." *Strategic Analysis* 38, no. 4: 566-576. https://doi.org/10.1080/09700161.2014.918445

Martino, Luigi. 2018. "La quinta dimensione della conflittualità, l'ascesa del cyberspazio e i suoi effetti sulla politica internazionale." *Politica&Società*, no. 1 (January-April): 61-76.

McGraw, Gary. 2013. “Cyber War is Inevitable (Unless We Build Security In).” *Journal of Strategic Studies* 36, no. 1: 109-119. https://doi.org/10.1080/01402390.2012.742013.

Tabansky, Lior. 2013. “Critical Infrastructure Protection Policy: The Israeli Experience.” *Journal of Information Warfare* 12, no. 3: 78-86.

Tabansky, Lior. 2020. “Israel Defense Forces and National Cyber Defense.” *Connection QJ* 19, no. 1: 45-62.

Van Puyvelde, Damien, and Aaron F. Brantly. 2019. *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Cambridge: Polity Press.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies