ROUTLEDGE
COMPANIONS

Routledge Companion to Global Cyber-Security Strategy

Edited by Scott N. Romaniuk and Mary Manjikian

Israel

Cyber defense and security as national trademarks of international legitimacy

Fabio Cristiano

in Romaniuk S. N. and Manjikian M. (2020, eds.) *Routledge Companion to Global Cyber-Security Strategy*, New York: Routledge.

In the last two decades, Israel established itself as a leading actor in the global arena of cyber security governance, strategy, and industry. Transferring knowledge from the military to the civilian sphere, the country can today be considered as a normative power for its cyber security policies, research, and innovative market ventures. Thanks to their notorious – yet contentious – operations, the Israel Defense Forces (IDF) are internationally recognized as pioneers in the field of offensive cyber defense. Different elements contribute to Israel's national success in cyber security, and this chapter maps them through a critical perspective on the country's conflation of military strategies with cyber security governance and market initiatives. This problematic merging of different domains creates in fact the conditions for a distinctive – and growlingly exported abroad – profitable approach to the securitization and militarization of cyberspace.

Between defense and security: a governance model in the making

In a cyber context characterized by rapid changes and continuously renewed security needs, Israeli authorities have – through the years – adopted diverse institutional arrangements to govern national cyber security (Tabansky and Ben Israel, 2015; Housen-Couriel, 2017). The governance of national cyber security commonly separates the military domain, and the protection of critical infrastructures, from civilian cyber security and crime.

Whereas the governance of cyber defense involves the cooperation between the army and national security agencies, national cyber security traditionally rests in the hands of law enforcement and local system administrators (Galinec et al., 2017; Carr, 2016; Mueller, 2017). This common setup reflects an understanding of cyberspace as a network constituted of nodes that can be governed and protected independently (on this debate, see Broeders and van der Berg, 2020).

Different levels of fragmentation in fact attribute calibrated protection and assign the responsibility to respond to each nodal unit, this way oscillating between different degrees of trust and control (van den Berg & Keymolen, 2017). The breakup of national cyber security governance into smaller units tends to be praised for enhancing organizational networking and effectiveness (see, Shackelford, 2013 on "polycentric" cyber security governance). Governance fragmentation, however, poses the risk of prioritizing particular cyber security concerns, and areas, over others while delegating national security to private 'trustees'.

Applying a centralized – but incomplete in its scope – governance approach, the Israeli government initially assigned responsibility for cyber security to the Shabak/Shin Bet (the Israel Internal Security Service), through a specific sub-unit: the National Information Security Authority (NISA). Besides administering national internet infrastructures as an element of information security, one of NISA's tasks included the safeguarding of cyber security for those public organizations that, by their very nature, were considered to be mostly at risk: the Israel Electric Corporation and the national water supplier Mekorot. Similarly, on the trail of a traditional defense-based approach, major national service providers were included in the compass of critical infrastructures to be protected (Tabansky, 2013). At this stage, in 2002, the majority of Israeli networks had to henceforth arrange their cyber security independently, making the entire national network more vulnerable, as the country lacked a central unit of control for cyber security, and part of a unified national strategy (Cohen et al, 2016).

Once authorities recognized the limitations and potential risks connected to such an approach, in 2011 an ad-hoc team of experts was given a prime minister's mandate to assess existing national cyber security shortcomings and to produce relevant recommendations. The so-called "National Cyber Initiative" (NCI) concluded that the country needed a substantial restructuring of its cyber security governance (Adamsky, 2017).

Besides insisting on the crucial need of investments to bridge automated activities with manned ones, the team emphasized the necessity to strengthen cyber security for those nodes of the national network that were, at that point, not part of a nationally-integrated system of protection and control. In other words, the NCI argued in line with a national strategy that would regard cyberspace as "one and unified" national milieu, with no substantial distinction between its critical/military infrastructures and civilian nodes. Acting on these suggestions, the Israeli government established the Israeli National Cyber Bureau (NCB) that, reporting directly to the prime minister, produced a new and comprehensive national strategy for cyber security (Benoliel, 2014). In particular, the NCB highlighted the country's need to institute an operational body to oversee, expressly, at affairs related to civilian cyber security (Tabansky & Ben-Israel, 2015).

In 2017, the government aligned to this mission goal by giving the newly founded National Cyber Security Authority (NCSA) the specific mandate of governing security for Israeli civilian cyberspace (NCB, 2017). At the operational level, the NCSA relied on the CERT (Computer Emergency Response Team) that, together with its subordinated units, monitored and protected civilian organizations from minor and major cyberattacks (such as the infamous Wannacry, NotPetya, and more), regardless of their political or criminal nature. For its globally acclaimed expertise and renowned preventive abilities, NCSA also partnered with analogous international units to cooperate on matters related to the prevention of cyber threats.

Later in 2017, the NCSA received the additional task of putting in place cyber security measures to protect the Israel Electric Company and Israel Railway, as well as to develop pedagogical activities to engage the Israeli society at large (such as specific trainings targeting the ultra-orthodox communities).[1] During the same year, the NCSA published the "Cyber Defense Methodology for an Organization," a thorough guide that outlines foundational elements of organizational cyber security as well as practical measures to be taken for securing networks and infrastructures (NCSA, 2017). Introducing local network administrators to practical security solutions, as well as to a broader systemic perspective, the methodology guide aimed at fostering cohesiveness and ownership towards the establishment of a unified national vision for cyber security. At the same time, this methodology extended the military language of 'cyber defense' to national cyber security.

As soon as the mission of the NCSA – i.e., progressing civilian cyber security at the same level of excellence of military cyber defense – appeared to be accomplished, the government decided to merge, in December 2017, both cyber security tracks (military and civilian) into the National Cyber Directorate (NCD). Part of the prime minister's office, the NCD aims at erecting a unified "cyber-shield" to protect the entire national internet network and its ramifications. With the NCD guiding national cyber security as an *unicum,* military and national security personnel ultimately took on a directing role within the directorate, thus supervising both military/public and civilian cyber security.

Encouraging the continuous exchange of military/civilian and public/private know-how, the NCD unceasingly consolidates the Israeli cyber security ecosystem as a focused and unified national enterprise. Going back to its origins – i.e., assigning major responsibilities to a single unit – Israeli authorities organized national cyber security in light of the understanding of cyberspace as an integrated national space. If on one hand this governance model benefits the country by assisting authorities to control network nodes in unison, on the other it raises a set of ethical and political questions regarding the risks associated to the merging of military/public governance and technologies with civilian ones, as well as to the militarization of cyberspace.

The role of the military

Long-since targeted by cyberattacks,[2] the Israeli military developed unique expertise and responsiveness in the context of cyber-defense, at a time when many major global powers had not yet taken significant steps in securing their national networks (Tabansky 2013; Grauman, 2012). IDF's cyber-operations – both defensive and offensive – are in fact internationally recognized for their sophistication and innovativeness (Baram, 2017). On one hand, this level of military expertise can be explained as a natural consequence of the contested political role played by the country, and its defining security concerns and defensive needs. On the other, looking at its development over time, this expertise rather emerges as the result of a long-term governance strategy that, fruitfully combining military and civilian approaches, created strategic advantages for the country in the field of cyber security as a whole.

At the center of a highly cooperative organizational structure, the Computer and IT Directorate – which comprises four subunits – monitors the security of information, networks, and communication within the army. Existing military intelligence capabilities, and infrastructures, also contributed to shape Israel's preparedness once, particularly in the last decade, cyber-warfare emerged as a significant strategic domain. Founded in 1952, four years after the creation of the state of Israel, IDF's Unit 8200 holds major responsibility for gathering signal intelligence and writing code decryption (Cordey, 2019). Upholding a primary role in defining security priorities and strategies, in fact the unit constitutes the largest division within the army. In particular, one of its operational sub-units – the Urim SIGINT Base (unknown to the public until 2010,[3] and located in the Negev desert) – intercepts communication of interest and reports to the main unit, or pertinent agencies, for analysis and investigation.

IDF units also hold major responsibilities for information security, a domain traditionally overseen by other national security agencies. Through predictive policing techniques – such as algorithmic scanning and data analytics – these technologies are used to identify presumed early warnings of violence midst Palestinians' online contents. Primarily targeting social media, these controversial practices have led to the arrest of hundreds of Palestinians, both in Israel and in the

West Bank (Cristiano, 2019a; 7amleh, 2019). The army has been criticized for its aggressive methods and for conducting intrusive operations to control and blackmail Palestinians, both in Israel and in the occupied territory (Cristiano, 2019b; Zureik, 2020).

While the history of espionage and monitoring of Palestinians dates back, and even precedes, the foundation of the Jewish state (see, Friedman, 2019), digital communications and the internet constitute a new source of private data for the Israeli army and security agenciesIn 2014, forty-three agents of Unit 8200 undisclosed a report describing that private data and communication of Palestinian users are constantly subjected to the Unit's hacking and data manipulation (Derfner, 2014; Levy 2014). These violations of privacy and digital rights intentionally target vulnerable subjects – such as women and homosexuals[4] – forcing them into sharing security-relevant information with Israeli security agencies .

IDF's strategy to foster national cyber-defense also contemplates the recurrence to offensive methods, often justified through logics of prevention, deterrence, and pre-emptive self-defense (Tabansky, 2020; Garwood-Gowers, 2011). In September 2007, the Israeli air forces conducted a nighttime strike on Deir-al-Zor (also referred to as Al Kibar) in Syria on a nuclear facility under construction. Prior to the airstrike, an Israeli cyberattack decisively compromised the Syrian government's monitoring systems, to the point they altogether failed to detect Israeli airplanes. Thank to this expedient, the airstrike efficaciously destroyed the facility, killing seven North Korean technicians who were working on its development (IAEA, 2008). Exemplifying a perfect mixture of cyber-espionage techniques with conventional cyber-attacks, the so-called "Operation Orchard" succeeded thanks to the cooperation between the IDF and the Mossad (see, Harel & Benn, 2018).

Moreover, the operational mechanics suggest two relevant considerations. First, its backstory would strikingly point at the importance of imagining, and protecting, national cyberspace as "one." Installing a trojan malware on a Syrian officer's laptop, during a 2006 short visit to London for a conference, Mossad agents accessed confidential data and kept track of the Syrian officer's communication. At a first glance, none of the intercepted information appeared to be of security relevance. However, once they came across the picture of an Eastern Asian-looking man posing in the desert with a local, they commenced an investigation on the issue. Additional evidence ultimately pointed at a Syrian-North Korean partnership for the construction of a nuclear facility in Eastern Syria.[5] As a result, an individual's negligence – in securing a single computer – lead to the disclosure of a secret nuclear plan, and eventually to the bombardment of its facilities.

The Unit 8200 also holds allegedly responsibility for developing and deploying the multi-model computer worm Stuxnet through a partnership with the United States (Zetter, 2014; Langer, 2013). In 2010, this worm seriously compromised the programmable logic controllers of vital Iranian nuclear machines. As these are responsible for the automatic activation and control of mechanic operations as well as crucial industrial processes, for the first time, cyber-attacks appeared to raise to the level of cyberwar. A typical distinctive trait of these circumstances, neither country claimed responsibility for the attack, but strong evidence points at an Israeli-American partnership in designing and launching the offensive, with analysts attributing Stuxnet to Israeli Unit 8200 (Sanger, 2012; Cordey, 2019).

Whereas Stuxnet appeared as an unprecedented – and still today unmatched – moment of cyber-warfare for its destructive outcome, Israeli cyberattacks have also manifested in more hybrid forms, in fact uniquely questioning the distinction between information and cyber warfare. Defined by Symantec (2011) to be "nearly identical to Stuxnet," 2011's malware Duqu is also believed to be a Unit 8200's creation. Gathering information, rather than compromising mechanic operations, its activities consisted in data theft and espionage. With an identical genesis and goal, 2014's Duqu 2.0 damaged Kaspersky Lab's systems, and was detected on the computers of the hotel hosting the negotiations for the Iranian Nuclear Deal (Bencsáth, Pék, Buttyán & Félegyházi, 2012; Kaspersky Lab, 2015).

Beside enforcing defensive and offensive cyber-strategies, the Unit 8200 also contributes to the mainstreaming of cyber security in Israeli society at large, establishing this field as a recognizable national trait, which unfolds through the conflation of military and civilian activities. Most of Unit 8200's officers are teenage-conscripted soldiers, who are selected for their tech abilities and innovative thinking. In line with the substantial efforts made by the national education system to include cyber security as an independent topic of school programs[6], the military functions as the primary *locus* where cyber security thinking and entrepreneurial spirit are matched and activated.

<HEAD1><TITLE>**Conclusion: from the cyber-battlefield to the market, and back**</TITLE></HEAD1>

Benefiting from a highly interconnected military-industrial complex, Israel has been often considered an exception when analyzing the negative impact that military expenditures can have on national economic growth (see, Swed & Butler, 2013). The overall consensus in macroeconomic studies asserts, in fact, that high military spending has a negative impact on a country's aggregated economic performance (Lifshitz, 2003). Disproving this assumption, Israel successfully combines growing investments for the military with national economic growth (Broude, Deger & Sen, 2013). The cross-fertilization of military expertise with a favorable environment for hi-tech entrepreneurship constitutes one of the driving forces behind this positive, yet exceptional, correlation. Acquiring know-how and extensive training in various IDF units, veterans often develop their hi-tech careers outside the military (Senor & Singer, 2009) – with cyber security becoming a privileged market sector.

Assisting these entrepreneurial ventures to disclose their full potential – i.e., creating innovative cyber security solutions and marketable products – the Israeli government also directs extensive financial support[7] to dozens of promising enterprises. To guide the transition from the army to the market, the Israel Innovation authority (IIA) – previously known as the Office of the Chief Scientist – manages public and private financial support, thus arising as an additional piece of the complex governance puzzle that governs Israeli cyber security. Established in 1974 to support innovative economic initiatives, the IIA functions today as an important node of a network connecting military, businesses, investors, governmental units, research institutes, and the global market. Besides encouraging large and comprehensive partnerships with other countries, the IIA targets international investors in order to boost cooperation across the international public/private divide. The authority also supports R&D activities and – thank to its renowned incubators[8] – provides crucial support for newly formed cyber security startups. Moreover, the IIA regularly produces research reports focusing on market trends, intelligence analysis, and commercial opportunities. These reports are meant to advise governmental and security entities, thus making the multi-stakeholder Israeli governance model of cyber security to come full circle.

Operationalizing considerable public/private financial investments, Israeli integrated governance model has escorted Israeli companies to the acquisition of a stable leadership in the global market of cyber security products. With extensive resources available for R&D, Israeli companies are encouraged to envision future security scenarios and to produce timely solutions. Besides a consolidated dominant position in the market of traditional cyber security products – such as email security, firewalls, antiviruses, and more – Israeli companies are placing themselves at the forefront of emerging market areas (such as IoT and cognitive cyber security). Similarly, Israeli enterprises also specialize in developing security solutions for cryptocurrencies, blockchain, SDP technologies, and cloudnative security. In this scenario, a recent INCB's report (2018) estimates that Israeli cyber security exports – presently constituting ten per cent of the entire global market – are expected to rise substantially in the upcoming years.

Israeli headship in the market of cyber security contributes to foster transnational collaborations with international allies and their markets (such as the United States and its market). Profiting on a long-sighted governance strategy, the country has made its cyber security technologies (and knowledge) attractive, and at times indispensable, to other countries. For this reason, a growing number of countries (such as India, Singapore, and Romania) relies on partnerships with the Israeli government, army, and private companies to secure their national networks. Widening the spectrum of military and security related exports, cyber security products bring much more to the country than ever-growing market revenues: other countries' reliance on Israeli tech exports ensures renewed legitimacy and political support for the country.

From this perspective, it can be argued the extensive governmental support for cyber security pays back in multiple ways: economic development, up-to-date knowledges available for national cyber-defense, and strengthening the political/diplomatic role of the country in the international arena. The growing involvement of Israeli prime minister's office[9] in the coordination of multiple actors – such as authorities, military, businesses, and universities/research centers – indicates the strategic relevance that cyber security holds for the country. At the same time, as elucidated by the recent restructuring of cyber security governance through the NCD, integrating military and civilian cyber security appears, once again, to have consigned an important sector of Israeli society to its security and defense elites.

References

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

Argaman, S., & Siboni, G. (2014). Commercial and industrial cyber espionage in Israel. *Military and Strategic Affairs*, *6*(1).

Benoliel, D. (2014). Towards a cybersecurity policy model: Israel national cyber bureau case study. *NCJL & Tech.*, *16*, 435.
Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M. (2012). "The Cousins of Stuxnet: Duqu, Flame, and Gauss," *Future Internet*, *4*(1): 971–1003.

Broeders, D., & van den Berg, B. (2020). Governing Cyberspace. *Governing Cyberspace: Behavior, Power and Diplomacy*, Lanham: Rowman & Littlefield.

Broude, M., Deger, S. & Sen, S. (2013). "Defence, Innovation and Development: The Case of Israel". *Journal of Innovation Economics & Management*, *12*(2): 37–57. doi:10.3917/jie.012.0037.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Cohen, M. S., Freilich, C. D., & Siboni, G. (2016). Israel and cyberspace: Unique threat and response. *International Studies Perspectives*, *17*(3), 307-321.

Cordey, S. (2019). The Israeli Unit 8200–An OSINT-based study: Trend Analysis. ETH Zurich.

Cristiano, F. (2019a). "Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory," in G. Blouin-Genest, M. C. Doran & S. Paquerot (eds.), *Human Rights as Battlefields* (pp. 178–201). Basingstoke: Palgrave Macmillan.

Cristiano, F. (2019b). Deterritorializing cyber security and warfare in Palestine: Hackers, sovereignty, and the National Cyberspace as normative. CyberOrient, 13(1), 28-42.

Derfner, L. (2014, September 16). "Against Spy Revelations, Israel Doth Protest Too Much," *+972mag.*

Friedman, M. (2019). *Spies of No Country*. Chapel Hill: Algonquin Books.

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

Garwood-Gowers, A. (2011). "Israel's Airstrike on Syria's Al-Kibar Facility: A Test Case for the Doctrine of Pre-emptive Self-Defence? *Journal of Conflict and Security Law*, *16*(2): 263–291.

Grauman, B. (2012). *Cyber-Security: The Vexed Question of Global Rules. An Independent Report on Cyber-Preparedness around the World.* Brussels, Belgium: Security & Defence Agenda (SDA) and McAfee Inc. (Security & Defence Agenda).

Harel, A. & Benn, A. (2018, March 23). "No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor," *Haaretz*.

Housen-Couriel, D. (2017). *National Cyber Security Organisation, Israel.* NATO Cooperative Cyber Defence Centre of Excellence.

IAEA. (2008). "Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic," Report by the Director General.

Kuntsman, A., & Stein, R. L. (2015). *Digital militarism: Israel's occupation in the social media age*. Stanford University Press.

Langner, R. (2013). *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Hamburgh/Munich: The Langner Group.

Levi, E. (2014, December 9). "IDF Intelligence Soldiers Refuse to Serve: We Won't Work against Innocent Palestinians," *Ynet.*

Lifshitz, Y. (2003). *The Economics of Producing Defense; Illustrated by the Israeli Case*. Amsterdam: Kluwer Academic Publishers.

Lindsay, J. (2012). "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, *22*(3): 365–404.

Mueller, M. (2017). "Is cybersecurity eating internet governance? Causes and consequences of alternative framings", *Digital Policy, Regulation and Governance*.

NCB. (2017). *Israel National Cyber Security Strategy*. Tel Aviv: Israel Prime Minister's Office – National Cyber Bureau.

NCSA. (2017). *Cyber Defense Methodology for Organizations*. Tel Aviv: Israel Prime Minister's Office – National Cyber Security Authority.

Rid, T. & Buchanan, B. (2015). "Attributing Cyber Attacks," *Journal of Strategic Studies*, *38*(1): 4–37.

Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power*. Crown.

Senor, D. & Singer, S. (2009). *Start-Up Nation: The Story of Israel's Economic Miracle*. New York: Hachette Book Group.

Shackelford, S. J. (2013). "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance," *American University Law Review*, *62*(5): 1273–1364.

Siboni, G. & Assaf, O. (2016). *Guidelines for a National Cyber Strategy*. Tel Aviv: Institute for National Security Studies.

Swed, O. & Butler, J. S. (2013). "Military Capital in the Israeli Hi-tech Industry," *Armed Forces & Society*, *41*(1): 123–141.

Symantec. (2011). "W32.Duqu: The Precursor to the Next Stuxnet."

Tabansky, L. (2013). Cyberdefense Policy of Israel: Evolving Threats and Responses. *Chair de Cyberdefense et Cybersecurite.*

Tabansky, L. & Ben-Israel, I. (2015). *Cyber Security in Israel.* New York: Springer.

Tabansky, L. (2020). Israel Defense Forces and National Cyber Defense. Connections: *The Quarterly Journal*, 19(1), 45-62.
Tan, T. C. C., Ruighaver, A. B. & Ahmad, A. (2010) "Information Security Governance: When Compliance Becomes More Important than Security," in K. Rannenberg, V. Varadharajan & C. Weber, (eds.), *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). Berlin: Springer.

van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: control versus trust. *International Review of Law, Computers & Technology*, 31(2), 188-205.

Whitaker, B. (2006). *Unspeakable Love – Gay and Lesbian Life in the Middle East.* Berkeley: University of California Press

Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books.

Zureik, E. (2020). Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel. *Middle East Critique*, 1-17.

[1] Through the years, religious authorities have attempted to discourage internet diffusion amongst the ultra-orthodox community. Targeting in particular the young generations, these internet-ban campaigns seem to have failed in isolating the community from the online world. In 2016, the Israel Democracy Institute published the "Statistical Report on Ultra-Orthodox Society in Israel" that outlines major social changes occurring within the ultra-orthodox society in Israel. Amongst these, the report indicates a substantial increase in internet use among ultra-orthodox Israelis, from 28 per cent in 2009 to 43 per cent in 2016. In particular, women access the internet more than men – 47 per cent versus 39 per cent. The full report is available at: https://en.idi.org.il/articles/20439

[2] Already in 2000, Hizbollah's hackers attacked Israeli government, IDF and major e-commerce websites (Kuntsman & Stein, 2015).

[3] In September 2010, for the first time, an article authored by Nicky Hager on Le Monde Diplomatique provided detailed evidence regarding the existence of Urim SIGINT Base and its location. The article can be accessed here: https://mondediplo.com/2010/09/04israelbase

[4] With homophobia increasing in Palestinian society (Whitaker, 2006), Israeli security agencies have recurred to the blackmailing of Palestinian homosexuals into sharing information of interest in exchange for secrecy regarding their sexual orientation.

[5] Israeli authorities officially admitted responsibility about the attack only in March 2018. The IDF also undisclosed classified footage, photographs, and intelligence documents about the airstrike.

[6] In Israel, cyber security is part of school programs already in middle school. Through high school, the topic can be chosen as an undergraduate specialization. As the country was the first to host a

specific PhD program in Cybersecurity, there are today six different university research centers dedicated to the topic.

[7] In 2018, the IIA, the Ministry of Economy and Industry, and the NCD announced a three-year plan to further boost the cyber security industry. The plan, particularly encouraging Israeli ventures abroad, included a public investment of ca USD$24 million.

[8] Offering long-term technological, business, and administrative supports, IIA's incubators program supports Israeli startups in turning innovative ideas into commercial ventures through generous funding for R&D. A 2018 report published by data firm CB Insights indicates that Israel accounted for the second-highest number of global deals in cyber security – with the country's share of 7 per cent only surpassed by the United States' share of 69 per cent.

[9] A recently proposed bill, advanced by the prime minister to the Knesset, aims at expanding NCD powers in such a way that would further make its decisional process independent from the Parliament. As the NCD falls under prime minister's supervision, critics have argued this might lead to an imbalance amongst institutional and decisional powers.