2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy

Lior Tabansky
Blavatnik Interdisciplinary
Cyber Research Center (ICRC)
Tel Aviv University (TAU)
Tel Aviv, Israel
cyberacil@gmail.com

Abstract: Cyber power has become a topical issue for many democracies, but policy and scholarly debates often default to the cyber means alone. However, throughout history, superior means were never enough to secure strategic advantage. Strategy – seeking various ways and diverse means to serve clear ends – is the missing ingredient.

I outline indicators of cyber power and develop an interdisciplinary framework for strategic analysis. Cyber power manifests itself when one leverages means to operate in cyberspace towards achieving a political end. I apply this strategic ends-ways-means framework to an Israeli case study to determine its scholarly value. The analysis suggests that Israel demonstrated cyber power when applying various means towards achieving ends beyond enhanced cyber security. In soft power efforts, Israel harnessed cyber technology for economic growth and increased cooperation with like-minded nations. Israel purportedly developed and applied cyber warfare to attain its top strategic priority through hard power – preventing Iran from acquiring nuclear weapons. Another finding challenges conventional wisdom on the value of formal policies for national cyber power.

Security studies scholarship on strategy and economics scholarship on National Innovation Systems facilitate improved understanding of soft and hard cyber power. Strategic studies offer valuable insights into adaptation process, which can help policy makers avoid predictable pitfalls. Fostering society-wide innovation capacity crucially helps to better adapt to the volatile future. The National Innovation System scholarship helps to comprehend and obtain better means. Scholars of cyber power should venture further beyond the core technical disciplines.

Keywords: *strategy, Israel, Stuxnet, National Innovation System, R&D*

1. STRATEGY: THE MISSING INGREDIENT OF CYBER POWER

Cyber technology provides new and affordable tools for actors to pursue their interests.[1] Unsurprisingly, cyber debates often default to a focus on the more easily quantifiable technology: networking and system architecture, cryptography, malware samples, military commands, and cyber defender headcounts. Despite years of effort and many billions of dollars invested in vastly improved technology, cyber power remains elusive.

Western cyber insecurity is a familiar situation for a strategist: throughout history, superior *means* were never enough to secure strategic advantage. Cyber power manifests when one leverages *means* to operate in, or to mould, the man-made cyber substrate[2] towards achieving a political *end*. But in the recent words of a leading strategist,

> 'Senior people in the ranks of strategic studies have by and large ignored the growing cyber challenge, while those who are technically highly cyber knowledgeable typically have scant background in strategy'.[3]

Strategy – seeking various ways and diverse *means* to serve clear *ends* – is the missing ingredient in cyber power scholarship and policy. In this essay I develop an interdisciplinary analytical framework of cyber power, to bridge the gap between cyber technology and strategy. It stems from an ongoing interdisciplinary analytical effort to advance a more comprehensive understanding of cyber power in strategic studies and international relations, and builds on the author's first case study of Israeli cyber security policy.[4]

2. OUTLINE

This study uses strategic studies scholarship on strategy together with economics studies of National Innovation Systems to lay out the new interdisciplinary analytical framework for cyber power. Case studies in social science can be a source of new theoretical development and a powerful tool for testing theories. Theory-building from case studies is an increasingly popular and relevant research strategy that forms the basis of influential studies.[5] Qualitative research enables the researcher to capture the complexity of the object of study.[6] Thus, the Israeli empirical case study is analysed to demonstrate the way in which an interdisciplinary

1 Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,' *International Security* 38, no. 2 (2013).
2 Chris C. Demchak, *Wars of Disruption and Resilience Cybered Conflict, Power, and National Security* (Athens, Ga.; London: The University of Georgia Press, 2011).
3 Colin S. Gray, *Making Strategic Sense of Cyber Power : Why the Sky Is Not Falling*, ed. Strategic Studies Institute Army War College (2013).
4 Lior Tabansky and Isaac Ben-Israel, *Cybersecurity in Israel*, ed. Sandro Gaycken, Springerbriefs in Cybersecurity (Springer, 2015).
5 Kathleen M. Eisenhardt, 'Building Theories from Case Study Research,' *The Academy of Management Review* 14, no. 4 (1989).
6 John W. Creswell, *Qualitative Inquiry and Research Design: Choosing among Five Approaches* (Sage publications, 2012).

strategic analysis of cyber power seeks the *ends-ways-means* nexus. The case selection is driven by the high regard for Israeli cyber security globally.[7]

The article demonstrates the framework's realistic analytical value: applied to the Israeli case study it reveals national cyber power and helps assessing it. The article presents the thesis in section 2, followed by a brief introduction to key themes in strategic studies in section 3. The Israeli case study is then presented in section 4: the country's main economic and social indicators of innovation; policy efforts; and its cyber warfare experience. Bridging the interdisciplinary gap, I harness strategic and economic scholarship to analyse selected Israeli academic, business and defence sector contributions to cyber power. Section 5 examines how cyber *means* support grand strategy *ends*, through various instrument of hard and soft power. The study's findings challenge the common wisdom on formal policy's role in national cyber power. The article's principal academic value lies in applying grand strategy and economics study of national innovation systems to analyse national cyber power. Future research directions are offered in section 6.

3. ON STRATEGIC THOUGHT

Strategic studies became an interdisciplinary academic field studying international conflict and peace strategies after WWII. However, strategic thought has been crucial since the time of the ancient civilisations.[8] Despite, or perhaps because of, technological and social change, power and strategy have remained essential.

A. Power

Power, like many basic ideas, is a contested concept. It depends on context, perception, and anticipation, not just on the application of force. Power is both a tool and a goal in itself, in peace no less than in war.

Joseph Samuel Nye, Jr., one of the most influential international relations scholars and a former chairman of the US National Intelligence Council, distinguished hard and soft power along a spectrum from command to co-option in a seminal 1990 article.[9] Hard power behaviour relies on coercion and payment, while soft power uses the framing of agendas, attraction, or persuasion. Nye also discussed cyber power, masterfully including both physical and informational instruments, soft and hard power aspects, and ramifications within and beyond cyberspace.[10] Cyber power is not limited to information, but cuts across the other facets, elements and instruments of power, often referred to as Diplomatic, Informational, Military, and Economic (DIME). Cyber connects these elements in new ways to produce preferred outcomes within and outside cyber space. Kuehl's definition set out the central concepts for cyber power:

7 B. Grauman, 'Cyber-Security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness around the World,' ed. Security & Defence Agenda (SDA) and McAfee Inc. (Brussels: Security & Defence Agenda (SDA), 2012). 'Cyber-Boom or Cyber-Bubble? Internet Security Has Become a Bigger Export Earner Than Arms,' *The Economist*, Aug 1 2015.

8 Sun Tzu, *The Art of War* (Shambhala Publications, 2011). Thucydides, *History of the Peloponnesian War*, The Penguin Classics (Harmondsworth, Eng.: Penguin Books, 1972).

9 Joseph S. Nye, 'Soft Power,' *Foreign policy* (1990).

10 Joseph S. Nye, '*Cyber Power*.' Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

> '…the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power'[11]

The very inclusion of the desired outcomes in the definition entails that such ends should be defined, and should guide the development and application of power.

B. Strategy

The term 'strategy' originated in the context of conflicts between city-states in ancient Greece, and in addition to its continued military uses, has been adopted by business, governments, political campaigns, and more, becoming ubiquitous.[12] In analysing cyber power, I adopt Sir Lawrence Freedman's recent definition: 'Strategy is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power'.[13]

By definition, getting more out of a situation presents obvious difficulties. In his seminal article, *Why Strategy is Difficult*, Colin S. Gray discussed three major reasons why it is difficult to do strategy well:

- Its very nature, which endures through time and in all contexts;
- The multiplicity and sheer variety of sources of friction; and
- It is planned for contexts that have not occurred and might not occur; the future has not happened.[14]

Cyber technology can offer many benefits; it cannot cure the Thucydidean 'honour, fear and profit' trinity, the human causes of policy already clear 2,400 years ago.[15] Strategic history suggests that developed states, tasked with securing their respective societies, are in for extraordinary shocks and surprises.[16] Recent strategic developments such as the Arab uprisings, the rise of Daesh, and Russia's moves in Ukraine and Syria, prove that Clauzewitz's fog and friction concepts remain valid.[17]

C. Grand strategy

The essence of strategy remains designing an effective relationship between *ends*, *ways* and *means* in potentially competitive or adversarial dynamic relations. In international power, an *'end'* is a *political* objective defined by the state's leadership. *'Way'* is the selected form of

11 Daniel T. Kuehl, 'Cyberspace and Cyberpower,' in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (National Defense University Press: Potomac Books, 2009).

12 Key strategic studies scholarship issues are covered in the edited collection of most of the influential essays: Thomas G. Mahnken and Joseph A. Maiolo, *Strategic Studies: A Reader* (Milton Park, Abingdon, Oxon; New York: Routledge, 2008).

13 Lawrence Freedman, *Strategy: A History* (Oxford: Oxford University Press, 2013).

14 Colin S. Gray, *Strategy and History: Essays on Theory and Practice* (London: Routledge, 2006).

15 Robert G. Gilpin, 'The Richness of the Tradition of Political Realism,' *International Organisation* 38, no. 02 (1984); Steven Forde, 'International Realism and the Science of Politics: Thucydides, Machiavelli, and Neorealism,' *International Studies Quarterly* 39, no. 2 (1995).

16 Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2006); Ian Arthur Bremmer, *The J Curve a New Way to Understand Why Nations Rise and Fall* (New York: Simon & Schuster, 2006); Paul M. Kennedy, *The Rise and Fall of the Great Powers Economic Change and Military Conflict from 1500 to 2000* (New York: Random House, 1987); Edward N. Luttwak, *Strategy the Logic of War and Peace* (Cambridge, Mass: Belknap Press of Harvard University Press, 2003).

17 Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976).

action, boiling down to a mix of soft and hard power. *'Means'* refers to the resources available: people, money, land, trade influence, weapons etc. Strategy has several levels.

The focus of this article is the highest level, known as grand strategy:

> 'Grand strategy is a coherent statement of the state's highest political ends to be pursued globally over the long term. Its proper function is to prioritise among different domestic and foreign policy choices and to coordinate, balance, and integrate all types of national means – including diplomatic, economic, technological, and military power – to achieve the articulated ends'.[18]

Ideally, the political echelon defines the national strategy from which the security strategy is derived.[19] Alas, in practice rarely is it clearly and formally articulated. However, Edward Luttwak, the leading scholar on the hierarchical approach to defining grand strategy, writes: 'All states have a grand strategy, whether they know it or not.'[20]

TABLE 1: THE LEVELS OF STRATEGY[21]

Level	Geographic Scale	Temporal Scope	Types of Ends	Types of Power (Means)
Grand Strategy	Global	Long term (decades)	Highest political ends	All (diplomatic, informational, military, economic)
Strategy	All theaters of war (and conflict)	Mid term (years)	Overall military victory	Military, informational, economic
Operations	One particular theater of war	Short term (weeks to months)	Campaign victory	Military, informational
Tactics	Battlefield	Very short term (minutes to days)	Achievement of tactical objectives	Military
Technology	Home front/ academia Industry	Variable time horizon	Competitive advantage over enemies	Technical expertise

D. Israel's enduring grand strategy

Zionist political ideology emerged with modern nationalism in 19th century Europe, seeking self-determination through the establishment of a Jewish democratic state in the Land of Israel and the ingathering of the remaining Jewish diaspora to it.[22] But the volatile geo-political

18 Ibid.

19 Thomas G. Mahnken, 'U. S. Strategic and Organisational Subcultures,' in *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights into Comparative National Security Policymaking*, ed. Jeannie L. Johnson, Kerry M. Kartchner, and Jeffrey A. Larsen (New York: Palgrave Macmillan US, 2009).

20 Edward N. Luttwak, *The Grand Strategy of the Byzantine Empire* (Cambridge, Mass.: Belknap Press of Harvard University Press, 2009).

21 William C. Martel, *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy* (2015), p.30.

22 Anita Shapira, *Israel: A History*, http://site.ebrary.com/id/10628397.

environment has made the task daunting.[23] The founding fathers of Israel designed a national security strategy with the following elements continually present:[24]

- Seek qualitative superiority (including investment in education, science and technology);
- Seek an alliance with a global superpower, and normal diplomatic and economic relations with all countries;
- Emphasise early warning intelligence to balance the total lack of strategic depth (including heavy investment in signal intelligence); and
- Seek an ultimate deterrent (including heavy early investment in nuclear research).[25]

The overarching strategy, applied with varying degrees of prudence and effectiveness, has served the nation well. The Israeli population has grown ten-fold since 1948, and the GDP per capita has increased three-fold since 1990.[26] Israel was accepted into the OECD in 2010, and now ranks 18th among 188 nations on the UN's Human Development Index.[27] Recent political science scholarship shows the real-world effects for international governance and soft power that such ranking systems have.[28]

The geopolitical predicament persists. The implosion of the 1916 colonial Sykes-Picot political order in the Middle East along sectarian lines and the rise of global Jihadist organisations present volatile security challenges for Israel.[29] While Israeli national leadership avoids publishing formal national strategy documents,[30] Israel has viewed the nuclear ambitions of the Islamic Republic of Iran as the top strategic threat for over two decades.[31]

4. MEANS AND WAYS OF ISRAELI CYBER POWER

Having outlined the strategic ends, I now turn to survey the means and ways, towards a strategic analysis of cyber power. Technical innovation is central for cyber security. Israel is perceived

23 Avi Shlaim, *The Iron Wall: Israel and the Arab World* (2014).

24 Yisrael Tal, 'National Security the Israeli Experience,' Praeger, http://ebooks.abc-clio.com/?isbn=9780313001635; Yehezkel Dror, *Israeli Statecraft: National Security Challenges and Responses*, vol. 15, Besa Studies in International Security (Milton Park, Abingdon, Oxon; New York: Routledge, 2011); Efraim Inbar, *Israel's National Security: Issues and Challenges since the Yom Kippur War*, vol. 49, Cass Series-Israeli History, Politics, and Society (London; New York: Routledge, 2008).

25 Uzi Eilam, *Eilam's Arc: How Israel Became a Military Technology Powerhouse* (Brighton; Portland, Or.: Sussex Academic Press, 2011).

26 World Development Indicators 2015, (2015), http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=948695.

27 United Nations Development Programme, *Human Development Report 2015* (United Nations, 2016).

28 Judith G. Kelley, and Beth A. Simmons. "Politics by Number: Indicators as Social Pressure in International Relations." *American Journal of Political Science 59, no. 1* (2015).

29 Eran Zohar, 'Israeli Military Intelligence's Understanding of the Security Environment in Light of the Arab Awakening,' *Defence Studies* 15, no. 3 (2015).

30 Such as the French *Le Livre Blanc sur la Défense et la Sécurité Nationale* or the American *Quadrennial Defense Review*.

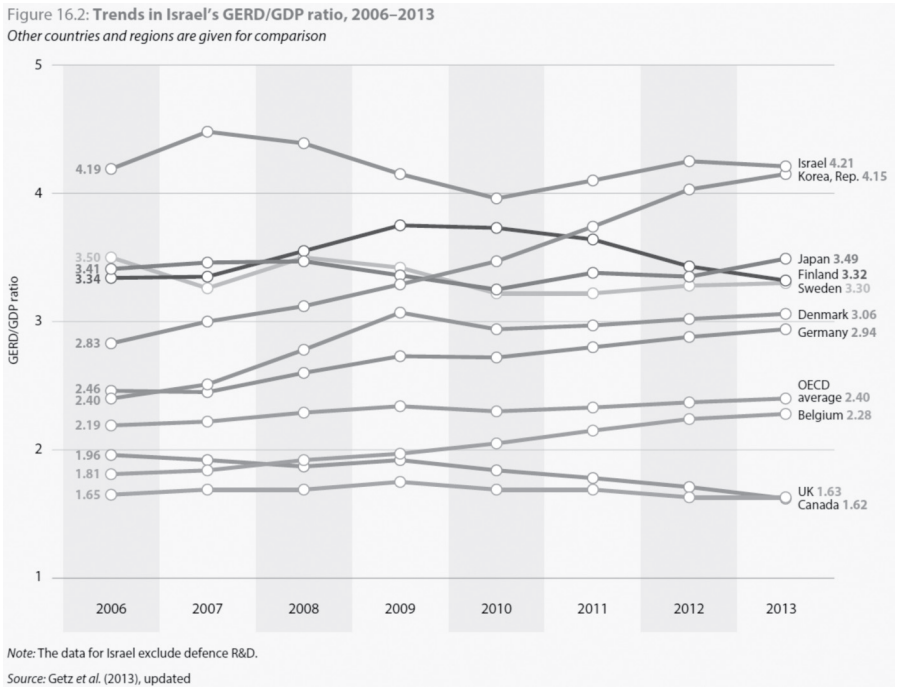
31 Ronen Bergman, *The Secret War with Iran: The 30-Year Clandestine Struggle against the World's Most Dangerous Terrorist Power* (Simon and Schuster, 2008); Wyn Q. Bowen and Jonathan Brewer, 'Iran's Nuclear Challenge: Nine Years and Counting,' *International Affairs* 87, no. 4 (2011); Yaakov Katz and Yoaz Hendel, *Israel Vs. Iran: The Shadow War* (Washington, D.C: Potomac, 2012). The Iranian nuclear program was first presented as an existential threat by Prime Minister Yitzhak Rabin in the early 1990s. In 2002, evidence of Iran's 'secret' nuclear program began to emerge. Israel's fear of an Iranian regime armed with a nuclear weapon takes at least three cumulative distinct forms: fear of annihilation, fear of a more difficult security environment, and fear of a challenge to Israel's founding Zionist ideological principles.

as a global leader in information technology.[32] Innovation capacity plays another, less tangible but important role; it indicates the likelihood of successful adaptation to change. The National Innovation System (NIS) concept refers to all the interacting social and political factors inside a country that affect the creation and diffusion of innovation. However, cyber capacity building debates have rarely used innovation studies, which have thrived in recent decades in economics, business management, political economy, technology, and engineering policy.[33]

A. The Israeli National Innovation System

Israel's gross domestic R&D expenditure is the highest in the world, and almost double the OECD average.

FIGURE 1: TRENDS IN ISRAEL'S GERD/GDP RATIO, 2006-2013[34]



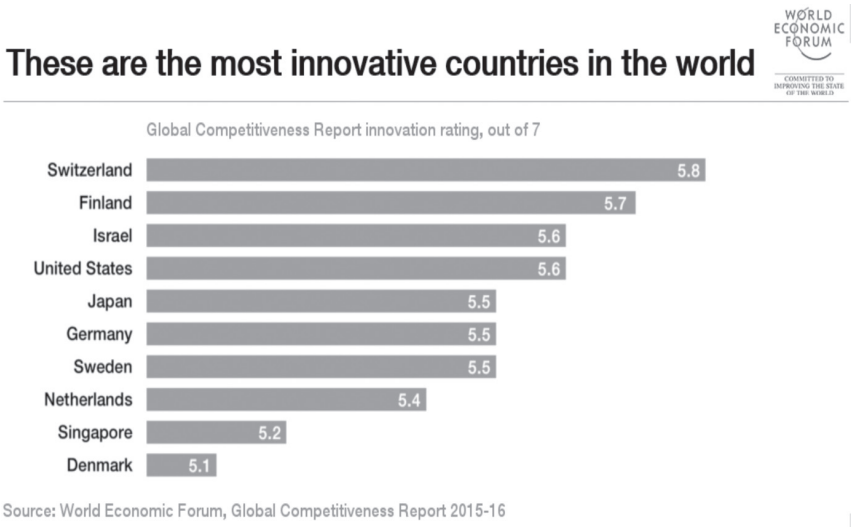
Importantly, the OECD figures exclude defence R&D expenditure. Israel ranks among the most innovative countries.

32 Grauman, 'Cyber-Security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness around the World; Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracl*e (New York: Twelve, 2009).

33 Mark Z. Taylor, 'Toward an International Relations Theory of National Innovation Rates,' *Security Studies* 21, no. 1 (2012).

34 OECD. 'R&D in OECD and Key Partner Countries, 2013.' Paris: OECD Publishing, 2015.

FIGURE 2: THE MOST INNOVATIVE COUNTRIES IN THE WORLD[35]



B. Universities

In the Israeli NIS, public research universities conduct basic research and participate in most applied research. Israeli universities compete globally, and have had remarkable success in the EU's Seventh Framework Programme (FP7).[36] Each university owns a technology transfer company (TTC) to protect and proactively commercialise scientific innovations made by researchers.

Regarding cyber security, Israeli universities host four of the top 50 Computer Science departments.[37] Tel Aviv University (TAU) hosts the Blavatnik Interdisciplinary Cyber Research Centre, the first institutionalised Israeli government-academia cooperative venture into cyber-related research. It was inaugurated in September 2014 by Prime Minister Netanyahu during TAU's 4th Annual Cyber security Conference.

C. Business R&D

Since the domestic market is small, Israel's industry can only prosper through exports. To succeed in global competition, the industry has to seek rich diversity and cutting-edge competitiveness. Even the Israeli defence industries export some 70% to 76% of the output.[38,39] This global orientation is one of the reasons that Business Expenditure on R&D (BERD) in Israel, as a share of GDP, is around 80%, the second highest in the OECD.[40] Half of Israel's

35 Klaus Schwab, 'Global Competitiveness Report, 2015-2016,' in *World Economic Forum* (2015).
36 Commission European, Research Directorate-General for, and Innovation, *Research and Innovation Performance in the EU: Innovation Union Progress at Country Level, 2014* (Luxembourg: EUR-OP, 2014).
37 Fabio Kon et al., 'A Panorama of the Israeli Software Startup Ecosystem,' *Orit and Yuklea, Harry, A Panorama of the Israeli Software Startup Ecosystem (March 1, 2014)* (2014).
38 Inbal Orpaz, 'Preserving the Madness' in Idf Intelligence,' *Haaretz*, September 26 2013.
39 John Stone, 'Politics, Technology and the Revolution in Military Affairs,' *Journal of Strategic Studies* 27, no. 3 (2004).
40 OECD Science, Technology and Industry Scoreboard 2015: , (Paris: OECD Publishing, 2015), http://dx.doi.org/10.1787/sti_scoreboard-2015-en.

total R&D expenditure as a share of GDP is foreign, and increased from 28% in 2007 to 47% in 2011.[41] It mostly consists of direct BERD investment and competitive funding awarded by European Research Programmes. The ratio of foreign investment indicates the degree of internationalisation of business R&D and the country's attractiveness to foreign investors.[42]

Conflict-laden Israel hosts R&D centres from most major IT multi-national corporations (MNCs).[43] In the 21st century, the latest R&D centres came about as a result of an MNC acquiring an Israeli company start-up in the software and IT security niches.

D. Cyber security industry exports

In 2014, Israeli companies held almost 10% of the global cyber security market, valued at $60 billion in 2013 by Gartner. Israeli companies exported IT security solutions (mostly software) worth $6 billion, double the $3 billion of exports in 2013.[44] According to the Israel National Cyber Bureau (INCB) estimates, Israeli cyber security exports reached $3.5 billion in 2015, about 5% of the global cyber security market valued now at $75 billion.[45] The dynamic innovation continues; Israeli society produced some 300 cyber security start-ups in 2015, up from 150 in 2012.

E. Formal national cyber policies

Government Resolution 3611 issued on August 7, 2011 – *Advancing the national capacity in cyberspace* – is the first Israeli national cyber strategy. It was the result of an external expert review, the 2010 *National Cyber Initiative*.[46] In order to promote the strategy which sought to 'make Israel a top-five global cyber power by 2015', an advisory body *Mat'e ha-Cyber ha-Leumi* (the Israel National Cyber Bureau INCB) was established in the Prime Minister's Office.[47]

A national contact point for cyber security incidents, the Israel National Cyber Event Readiness Team (CERT-IL), has operated since 2015.[48] In 2016, cyber protection of the civilian sector beyond critical infrastructure has yet to be developed in Israel. Accepting the recommendation of Isaac Ben-Israel's 2014 task force, the government resolved on February 15, 2015 to establish a new *Rashut Le'umit le-Haganat ha-Cyber* (National Cyber Security Authority, NCSA) to enhance cyber security in the civilian sector.[49] Before 2014, academic cyber research was

41 In the EU, *foreign* R&D expenditure as a share of GDP averages 10%. 'Gross Domestic Expenditure on R&D, by Type, 2013,' (OECD Publishing, 2015).

42 Richard R. Nelson, *National Innovation Systems a Comparative Analysis* (New York: Oxford University Press, 1993).

43 Uzi de Haan, 'The Israel Case of Science and Technology Based Entrepreneurship: An Exploration Cluster,' in *Science and Technology Based Regional Entrepreneurship* Global Experience in Policy and Program Development, ed. Sarfraz A. Mian (Cheltenham, UK: Edward Elgar Publishing, Inc., 2011).

44 'Cyber-Boom or Cyber-Bubble? Internet Security Has Become a Bigger Export Earner Than Arms.'

45 Author's interview with government officials, 02/2016. The nominal decrease is explained by foreign (mostly American) firms acquiring Israeli exporters, for a total of $1.3 billion in 2015, almost double $700 in 2014.

46 Lior Tabansky and Isaac Ben Israel, 'The National Cyber-Strategy of Israel and the Incb,' in *Cybersecurity in Israel, Springerbriefs in Cybersecurity* (Springer International Publishing, 2015).

47 Government of Israel, 'Government Decision 3611: Promoting National Capacity in Cyber Space,' (Jerusalem, Israel: PMO Secretariat, 2011).

48 https://cert.gov.il/

49 Israel Prime Minister's Office, 'Cabinet Approves Establishment of National Cyber Authority ' http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokeCyber150215.aspx.

dispersed and uncoordinated in Israel. The story of cybersecurity policy in Israel shows Israel gained cyber power without many formal elements.

The various IDF branches and units have been operating relevant technology and capabilities towards highly ambitious goals without a joint cyber command. The decision to establish one was announced in June 2015.[50]

F. Defence experience

Qualitative superiority is imperative in Israel's strategy.[51] Israel's extensive defence R&D stems from the strategy. Defence R&D probably contributes an additional 1.5% of the GDP.[52] The Israeli Air Force (IAF), C4I Corps, and Intelligence Corps have long embraced cyber technology to perform their missions. Brigadier General (Ret.) Pinchas Buchris, the then Director General of the Israeli Ministry of Defence, said in a 2007 interview:

> 'I can only say we're following the network attack technology with great care. I doubted this technology five years ago. But we did it. Now everything has changed. Any such capabilities are top secret'.[53]

5. STRATEGIC CYBER POWER: THE ENDS-WAYS-MEANS NEXUS REVEALED

The brief discussion on strategic thought, the Israeli grand strategy, the Israeli national innovation system performance, and defence experience laid out the foundation for the strategic analysis. But technological prowess alone does not create power, nor can it compensate for strategic mistakes. Cyber power can only be meaningful in context; when one applies the means towards one's goals and tests both in action.

A. Soft power: R&D, innovation, business and diplomacy

Education, science, and research are the enduring cornerstones of the Israeli strategy to gain a qualitative edge. The National Innovation System drives scientific and economic development as well as cyber defence capability. The government explicitly leverages the academic, business and defence sectors for soft power.[54] The research universities serve (albeit not on purpose) the strategic goal of achieving and maintaining a qualitative edge by consistently developing human capital and advancing fundamental scientific research and applied technology. The business sector serves (again, not on purpose) strategic goals beyond the evident economic sphere. Israel has been consistently using its technological advances for diplomatic purposes, its assistance to Africa and Asia since the 1950s being the prominent example.[55] Nowadays, PM Netanyahu offers Israel's technological and operational expertise to other countries to

50 Gabi Siboni and Meir Elran, 'Establishing an IDF Cyber Command,' INSS, http://www.inss.org.il/index.aspx?id=4538&articleid=10007.

51 Jacob Amidror, 'Israel's Strategy for Combating Palestinian Terror,' *JFQ: Joint Force Quarterly*, no. 32 (2002); Eilam, *Eilam's Arc: How Israel Became a Military Technology Powerhouse*; Shlaim, *The Iron Wall: Israel and the Arab World*; Tal, 'National Security the Israeli Experience'.

52 Tabansky and Ben-Israel, *Cybersecurity in Israel*.

53 David A. Fulghum, Robert Wall, and Amy Butler, 'Israel Shows Electronic Prowess,' *Aviation Week & Space Technology* 168(2007).

54 Author's interview with senior Ministry of Foreign Affairs and the Prime Minister's Office officials.

55 Michael Curtis and Susan Aurelia Gitelson, *Israel in the Third World* (New Brunswick, N.J.: Transaction Books, 1976).

counter the forces that exploit cyberspace to wage war against Western values. Academic and business performance also attracts foreign direct investment (FDI) in Israeli science and high technology.

Strategic analysis shows how universities and business develop soft power, applied for the strategic goals:

- Reduce the cyber threat;
- Develop a prosperous economy;
- Increase cooperation with like-minded nations;
- Gain diplomatic benefit.

B. Hard power: Stuxnet

Operation Olympic Games, which has been attributed to the USA and Israel, demonstrated the real-world feasibility of striking high value, heavily defended targets with bits alone.[56] Probably implanted in late 2007, *Stuxnet* malware was specifically written to infiltrate air-gapped[57] networks and silently disrupt industrial control systems (ICS).[58] *Stuxnet* slowly and stealthily damaged the nuclear enrichment process at the Natanz facility in Iran by reprogramming the Siemens-made programmable logic controller (PLC) to spin the motor out of the safe range.[59] Stuxnet was a precision-guided weapon; the payload was only executed when the target met all predetermined conditions.[60]

Stuxnet targeted the Iranian *means*, towards the top Israeli strategic goals:

- Reduce and postpone the nuclear threat by rendering useless at least 1,000 of the 9,000 IR-1 centrifuges deployed at Natanz in late 2009 and early 2010, and having the unexpected failure rate introduce profound insecurity throughout the Iranian nuclear project;[61] and
- Reduce cyber risks, as developing cutting-edge capabilities in the ICS realm can improve critical infrastructure protection.

The effectiveness of Stuxnet remains a source of heated scholarly and policy debates. Critics argue that Operation Olympic Games failed to stop Iran's nuclear weapons programme; others argue it increased Iran's determination to pursue it.[62] There is, however, substantial strategic logic in this use of cyber capability as an instrument of power. The 'end' was to harm capacity,

56 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012).

57 In IT-security, air-gapped refers to a network secured to the maximum by keeping it (often physically) disconnected from other local networks and the Internet.

58 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

59 Ralph Langner, 'Stuxnet: Dissecting a Cyberwarfare Weapon,' *Security & Privacy, IEEE* 9, no. 3 (2011); Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.

60 Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

61 David Albright, Paul Brannan, and Christina Walrond, 'Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant?,' (Washington, DC: Institute for Science and International Security, 2010).

62 Ivanka Barzashka, 'Are Cyber-Weapons Effective?,' *The RUSI Journal* 158, no. 2 (2013); Randall R. Dipert, 'Other-Than-Internet (Oti) Cyberwarfare: Challenges for Ethics, Law, and Policy,' *Journal of Military Ethics* 12, no. 1 (2013); James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War,' *Survival* 53, no. 1 (2011); Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare,' *Security Studies* 22, no. 3 (2013).

not intent. Expecting to alter the strategic course of a 78-million-strong nation is surely beyond realism. The 'way', a novel clandestine sabotage operation, was aligned with the 'ends' and echoes Israel's strategic culture.[63] The 'means', a first-of-its-kind, destructive, stealthy, precision-guided cyber weapon, expressed Israel's longstanding focus on its qualitative edge. The attempted physically destructive, precision-guided, prolonged, stealthy cyber attack to delay the main strategic threat to Israeli national security fits the definition of cyber power.

C. On formal policies

Strategy requires that decision-makers formulate and clearly communicate long-term ends in a reiterative fashion. Mundane democratic politics – structural checks and balances; coalition politics; electoral cycles; public opinion campaigns and more – make it difficult, yet some national leaderships have recently performed this task. However, the findings of the Israeli case study suggest cautious optimism; the formal process is not *sine qua non*.

6. SUMMARY, THEORETICAL IMPLICATIONS AND FUTURE RESEARCH

This essay outlined a new interdisciplinary analytical framework that integrates strategic studies and innovation system studies for strategic analysis of cyber power, and applied it to the Israeli case study. Western cyber insecurity stems largely from the skewed focus on means. Strategy – seeking how *means* and *ways* serve the exercise of soft and hard power for the national *ends* – is the missing ingredient in cyber power. A democracy seeking cyber power should optimally engage in an iterative strategic process loop:

- Reassess its particular strategy to clarify desired *ends*;
- Design cyber *means* by which *ways* can feasibly serve the defined strategic *ends*, focusing on non-military aspects, innovation and soft power;
- Experiment with and implement cyber means; and
- Reassess and continue to seek improvement.

A. Summary of the findings

Israel effectively develops cyber technology in the National Innovation System. But mere possession of technology does not neatly translate into power. The true manifestation of cyber power is in the application of means to achieve political ends. Crucially, the new analytical framework allows an improved understanding of cyber power. Israel exercises cyber technology for soft and hard power to meet national ends:

- Reduce the cyber threats and risks through security efforts;
- Develop a prosperous national economy;
- Increase cooperation with like-minded nations;
- Gain diplomatic benefit; and
- Reduce the Iranian nuclear threat.

63 Strategic culture refers to a set of national beliefs, attitudes and norms towards the use of force. See Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel* (Stanford, Calif.: Stanford University Press, 2010) for a discussion of Israel's strategic culture.

Although strategy is best organised formally, the Israeli case shows a serendipitous process prior to 2011. Israel gained cyber power without many formal elements: an official national cyber strategy, a committed government agency to coordinate cyber activity, a unified military command, a national CERT, or a dedicated academic thrust. The enduring strategic necessity to maintain a qualitative edge in order to develop a safe and prosperous State of Israel is what drives innovation throughout academia, industry, and defence operations. Much of the innovation is now expressed throughout cyber technology, and used in soft power efforts seeking strategic goals. Opting for cyber hard power to delay the main strategic threat to Israeli national security is a definite manifestation of cyber power.

B. Theoretical implications

This analysis aims to advance scholarly efforts, rather than grade policy. It may be tempting to present some of the findings on Israeli technological prowess as lessons[64] and offer sensible recommendations; to promote innovation, to invest more in R&D, or attract foreign business investment, all while cutting corners to escape the bureaucratic quagmire. Such 'lessons' would repeat the major flaw in countless cyber power debates; the focus on *means* and *ways*.

Western cyber insecurity stems largely from a common pitfall: the skewed focus on means. A society's capacity for innovation is one of the central enablers of successful adaptation to change; it drives ways and means. The economics scholarship on NIS can also contribute to scholarly and policy cyber power efforts alike. Even when properly integrated into systems and implemented by trained personnel, cyber technology cannot erase the difficulties that impede strategic excellence.[65] Only when applied towards clear ends, can ways and means be assessed. Strategic thought shows that the focus on means will take a heavy toll on cyber power scholarship and policy alike. Developing and adhering to strategic ends-ways-means logic will facilitate a transition from cyber technology to cyber power.

C. Future research directions: venture beyond technology

Advancing cyber power requires venturing beyond means, beyond the core technical disciplines and defence circles. Fields as disparate as international relations, change management in organisations, public policy, psychology, and many others can contribute potentially crucial knowledge. I partially illustrated the value of two disciplines: strategic studies and the economics of innovation. Cyber presents special obstacles. Distinct separate professional and scholarly communities, which interact only intermittently, is the academic reality. Secrecy concerns also further inhibit cyber research. In this era of change, leaders and strategists cannot afford the scientists' luxury of seeing experiments through; they must act under uncertainty. An improved understanding of cyber power demands further cross-disciplinary research and policy efforts to integrate more elements into the analytical framework.

ACKNOWLEDGEMENTS

This research was supported by a grant from the Blavatnik Interdisciplinary Cyber Research Centre (ICRC) at Tel Aviv University (TAU).

64 William C. Fuller Jr., 'What Is a Military Lesson?,' *Strategic Studies: A Reader* (2008).
65 Colin S. Gray, *Strategy and History* (2006).