HÜSEYİN SERHAT SOLMAZ

MASTER'S THESIS

2024

T.C.

ANKARA YILDIRIM BEYAZIT UNIVERSITY

INSTITUTE FOR INTERNATIONAL RELATIONS

AND STRATEGIC RESEARCH

IMPACT OF STATE AND NON-STATE ACTORS ON ISRAEL'S CYBERSECURITY INFRASTRUCTURE AND THE LAW OF INTERNATIONAL RESPONSIBILITY

MASTER'S THESIS

HÜSEYİN SERHAT SOLMAZ

DEPARTMENT OF SECURITY STUDIES

ANKARA, 2024

T.C.
ANKARA YILDIRIM BEYAZIT UNIVERSITY
INSTITUTE FOR INTERNATIONAL RELATIONS AND STRATEGIC RESEARCH

IMPACT OF STATE AND NON-STATE ACTORS ON ISRAEL'S CYBERSECURITY INFRASTRUCTURE AND THE LAW OF INTERNATIONAL RESPONSIBILITY

MASTER'S THESIS

HÜSEYİN SERHAT SOLMAZ

SECURITY STUDIES PROGRAM

Assoc. Prof. Dr. HATİCE KÜBRA ECEMİŞ YILMAZ
Thesis Advisor

ANKARA, 2024

CONFIRMATION PAGE

The thesis study “Impact Of State And Non-State Actors On Israel's Cybersecurıty Infrastructure And The Law Of International Responsibility” prepared by Hüseyin Serhat SOLMAZ is approved anonimously/by majority votes by the jury as Master’s thesis in Ankara Yıldırım Beyazıt University Institute for International Relations and Strategic Studies, Department of Security Studies.

<table>
<tr><th colspan="2">JURY MEMBER</th><th>Institution</th><th>Signature</th></tr>
<tr><td colspan="2">Assoc. Prof. Dr. Hatice Kübra ECEMİŞ YILMAZ</td><td rowspan="2">Ankara Yıldırım Beyazıt University</td><td rowspan="2"></td></tr>
<tr><td>Approved</td><td>Denied</td></tr>
<tr><td colspan="2">Assist. Prof. Dr. İrem ŞENGÜL</td><td rowspan="2">Ankara Yıldırım Beyazıt University</td><td rowspan="2"></td></tr>
<tr><td>Approved</td><td>Denied</td></tr>
<tr><td colspan="2">Assist. Prof. Dr. Yusuf AVCI</td><td rowspan="2">Social Sciences University of Ankara</td><td rowspan="2"></td></tr>
<tr><td>Approved</td><td>Denied</td></tr>
</table>

The Date of Thesis Defense: 28.08.2024

I certify that the conditions for a master’s thesis in Ankara Yıldırım Beyazıt University Department of Security Studies have been met.

The Head of International Relations and Strategic Studies:
Assoc. Prof. İbrahim Demir

DECLARATION

I hereby declare that all information in this thesis has been obtained and presented following academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work, otherwise I accept all legal responsibility. (Date:28.09.2024)

Signature

Hüseyin Serhat SOLMAZ

ACKNOWLEDGEMENT

I would like to extend my thanks to my advisor, Assoc. Prof. Dr. Hatice Kübra Ecemiş Yılmaz, for her support, guidance, and advice on choosing this inspiring topic. I am also grateful to the esteemed jury members, Asst. Prof. Dr. İrem Şengül and Asst. Prof. Dr. Yusuf Avcı, for their valuable insights and evaluations on my thesis. In addition, I want to express my gratitude to my colleague, Research Assistant Abdullah Pekel, for his support and contributions. Finally, I am deeply thankful to the institute's faculty for fostering my research skills and knowledge throughout my program.

ABSTRACT

This thesis explores the impact of state and non-state actors on Israel's cybersecurity realm, their influence on the country's cybersecurity framework, and case analysis within the context of the Law of International Responsibility. The study utilized qualitative document analysis methods to examine the historical evolution of these actors, their adaptation to cybersecurity environments, and their impact on Israel's current cybersecurity landscape. It reveals that the concept of national security, shaped by Zionist thinkers even before the establishment of Israel, and the innovation culture of Israeli citizens significantly influenced the development of the country's cybersecurity infrastructure. The study also highlighted the positive effects of collaboration between Israel's state cybersecurity agencies and private entities and the beneficial relationships established with international allies. The impact of Israel's training programs, which focus on cultivating elite personnel within the military system, strengthens both public and private sector collaborations in cybersecurity. An analysis has been conducted to assess the results of these programs on cybersecurity. The findings are evaluated under international law, and the Pegasus spyware operation associated with Israel is analyzed within the framework of Law of State Responsibility.

Keywords: National security strategy, state and non-state actors, Pegasus Spyware, cybersecurity, state responsibility

ÖZET

Bu tez, İsrail'in siber güvenlik politikaları üzerinde devlet ve devlet dışı aktörlerin etkilerini, bu etkilerin ülkenin siber güvenlik yapılanmasına nasıl yansıdığını incelemektedir ve uluslararası sorumluluk hukuku bağlamında ilgili vaka analizlerini içermektedir. Çalışmada nitel belge analiz yöntemleri kullanılmıştır ve bu aktörlerin tarihsel gelişimlerini, İsrail'in siber güvenlik alanına olan katkılarını ve uyum süreçlerini detaylı olarak ele almaktadır. Ayrıca, Siyonist düşünürler tarafından İsrail'in kuruluşundan önce şekillendirilen milli güvenlik anlayışının ve İsrail vatandaşlarının sahip olduğu inovasyon kültürünün ülkenin siber güvenlik altyapısının gelişimine önemli etkilerde bulunduğunu ortaya koymaktadır. Çalışma, İsrail devletine ait siber güvenlik kurumları ile özel sektör arasındaki işbirliğinin ve uluslararası müttefiklerle kurulan ilişkilerin siber güvenlik ekosistemi üzerindeki olumlu etkilerini tartışmaktadır. İsrail'in askeri sistem içinde elit personel yetiştirme odaklı eğitim programlarının, kamu ve özel sektör işbirliklerini nasıl güçlendirdiği ve bu programların siber güvenlik sonuçları üzerindeki etkilerini analiz etmektedir. Bulgular, uluslararası hukuk bağlamında değerlendirilmiş ve İsrail ile bağlantılı bir siber operasyon olan Pegasus casus yazılımı, devletlerin sorumluluğu hukuku açısından incelenmiştir.

Anahtar Kelimeler: Milli güvenlik stratejisi, devlet ve devlet dışı aktörler, Pegasus casus yazılımı, siber güvenlik, devletlerin sorumluluğu

TABLE OF CONTENTS

INDEX OF ABBREVIATIONS

C4I	:	Command, Control, Communications, Computers and Intelligence
CERT-IL	:	Computer Emergency Response Team- Israel
IDF	:	Israel Defense Forces
INCB	:	Israeli National Cyber Bureau
INCD	:	Israel National Cyber Directorate
ITU	:	International Telecommunication Union
NCSA	:	National Cyber Security Authority
NISA	:	National Information Security Authority
Shin Bet	:	Israel Security Agency
SIGINT	:	Signals Intelligence
UN	:	United Nations
UNDP	:	United Nations Development Program
UNODC	:	United Nations Office on Drugs and Crime

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Cyber security has become one of the main concerns of states and non-state organizations in the 21st century. Due to the development of technology, military and civilian systems integrated with digital platforms, and the increasing use of the Internet, the threats in cyberspace are addressed by all actors, from individuals to states. The number of Internet users in the world is 5.44 billion in 2024. As of the same year, the number of devices interacting with the Internet is 18 billion. Therefore, threats in cyberspace have the potential to affect billions of users. Since the first large-scale cyber-attack in the world, MorrisWorm, which emerged in 1988, there have been many malware, cyber-attacks, and technical problems in cyberspace.

The democratic nature of cyberspace, its openness to malicious users, and low entry thresholds have led to an increasing number of such attacks. Due to the cost of traditional attack methods and the difficulty in accessing the weapons and materials used in these attacks, actors tend to increase their actions in cyberspace. Especially since the 1990s, states have integrated their military and civilian systems, energy, and infrastructure systems with cyberspace, making these “critical infrastructure” systems vulnerable to attack.

With the presence of state actors in cyberspace, cyber security has become an essential issue for states. As a result of the Estonian Cyber Attacks in 2007, infrastructure systems in Estonia were temporarily rendered inoperable. These attacks, which were associated with the Russian Federation, used the DDoS attack method and caused the Estonian state's internet service providers and networks to be disabled by creating intense user demand. Following these attacks, the attacks on Georgia, the Stuxnet attack against Iran, the alleged Russian interference in the US elections, and the Pegasus spyware produced and sold by the Israel-based NSO Group have shown how dangerous cyber-attacks are for states and societies and how much potential they have.

Due to the importance of cyber attacks, operations, and actions, states have created their cybersecurity strategies and included these strategies in their national security documents. Israel is one of the states active in cyberspace. Founded in 1948, the State of Israel is one of the most critical cyber security actors today. According to the CyberPower Index published in 2022, Israel ranks 19th as the most important cyberpower in the world. Israel is an effective element of cyberspace in both military and civilian fields, and analyzing

its successful position in this field is one of the main objectives of the second part of this thesis.

The cybersecurity performance of the State of Israel is a successful outcome of the security policies it has adopted since its establishment. An important issue in this thesis is how the principles and political economy that determine Israel's "grand strategy" have shaped Israel's current cyber power. The fact that Israel has the highest R&D investment relative to its GDP in the world has also been instrumental in making it a competent state in the field of high technology. The "Academic Reserve (Atuda)" programs, which integrate academic education with compulsory military service and enable the country's most elite high school students to gain military experience and elite academic education together, also shed light on the cyber security structure in Israel. For this reason, the first part of this thesis examines Israel's national security understanding, which is thought to be effective in shaping its cyber security, and the policies it has implemented to have high technology.

In the third part of the thesis, the issue of cyber security is examined from a broad perspective. A conceptual analysis of cyberspace, the reference object of cybersecurity, was made. The actions of the actors operating in cyberspace are analyzed separately and the concrete incidents related to these issues are analyzed. A framework of what cyber power, cyber attack, cyber deterrence and cyber diplomacy are and their place in the understanding of cyber security is outlined. This chapter aims to provide a conceptual framework for the topics to be discussed in the following chapters.

State actors play an important role in Israel's cyber security. In 1997, with Tehila, which emerged as Israel's e-government project, Israel officially started to exist in cyberspace. One of Tehila's missions is also to ensure the security of Israel's critical infrastructure systems. Israel first commissioned NISA to ensure information security with "Resolution 84/B" in 2002. In 2011, with "Resolution 3611", it transferred the duties of this authority to INCB and aimed to carry out the necessary policies and studies to make Israel a global power in cyberspace. Resolution 2443, issued in 2015, established a new institution, the NSCA, and tasked it to carry out the country's cyber security together with the INCB. "Resolution 2444 authorized the NSCA not to prepare a cyber doctrine. Finally, "Resolution 3270" issued in 2017 merged the NSCA and INCB under the title of INCD. In addition, Unit 8200 (responsible for cyber operations) and the C4I Directorate (responsible for cyber defense) within the IDF have comprehensively built the country's cyber security.

The fourth and final chapter of this thesis examines the status of cyber operations in international law. In the context of the law on the responsibility of states, the circumstances under which a state is responsible for cyber operations are examined. Whether cyber attacks are a use of force within the framework of the UN Charter is investigated. By comparing cyber attacks with conventional armed attacks, the situation of cyber attacks outside of cyberspace that cause loss of human life or violate the sovereignty of a state is examined, and comments on this situation in the literature are discussed. The issue of attributing the actions and operations carried out by non-state actors in cyberspace to a state and holding that state responsible for this action under international law is discussed in detail. A case analysis was conducted on who is responsible for the damages caused by the Pegasus spyware produced by the NSO Group, an Israel-based cyber warfare company, which the Israeli government allowed to be exported. In this analysis, special technical reports were examined and technical evidence was sought. The case was then analyzed within the scope of the Law of State Responsibility by utilizing the works of authors such as Tallinn Manuel and Ecemiş Yılmaz.

1.1.PURPOSE OF THE STUDY

This thesis seeks to answer the research question: How do state and non-state actors affect Israel's cybersecurity infrastructure and policies, and how can these impacts be assessed within the framework of the Law of International Responsibility? The purpose of this study is to analyze the impact of state and non-state actors in Israel’s cybersecurity field and to assess these impacts and analyze cases within the framework of the Law of International Responsibility. Another aim is to reveal the main factors in the formation of Israel's cybersecurity architecture and their direct or indirect relationship with Israel's cybersecurity policies and practices. To achieve these objectives, the thesis aims to examine in detail the concepts and sub-concepts of cyberspace and cybersecurity, establishing a comprehensive conceptual framework. It also aims to evaluate cyber operations in the context of international law, assessing the validity, shortcomings, and advantages of existing legal practices in cyberspace. Finally, one of the main objectives is to determine in which cases cyber operations may give rise to state responsibility within the context of the International Law on the Responsibility of States.

1.2.**PROBLEM STATEMENT**

This thesis seeks to answer the research question of “How do state and non-state actors impact Israel's cybersecurity structure and strategy, and what are the implications of the Pegasus spyware case within the framework of the Law of International Responsibility?”. The primary objective is to analyze Israel's cybersecurity structure and strategy, focusing on how state and non-state actors influence its development, and to assess these impacts within the context of the Law of International Responsibility. Specifically, the thesis examines the Pegasus spyware case as the central case study to illustrate these dynamics.

To address this overarching question, the thesis will explore the following sub-questions:

- What are the fundamental concepts of cyberspace and cybersecurity, and how can a comprehensive conceptual framework be established?
- What are the main factors contributing to the formation of Israel's cybersecurity architecture and strategy?
- How are cyber operations evaluated within the context of international law, and what are the validity, shortcomings, and advantages of existing legal practices in cyberspace?
- How does the Pegasus spyware case illustrate the impact of state and non-state actors on Israel's cybersecurity, and what are its implications under the Law of International Responsibility?
- Under which circumstances may cyber operations—such as those exemplified by the Pegasus case—give rise to state responsibility according to the Law of International Responsibility?

By exploring these questions, the thesis aims to contribute to a deeper understanding of Israel's cybersecurity policies and practices, the challenges it faces, and the associated international legal responsibilities arising from cyber operations. By addressing these objectives, the thesis aims to contribute to a deeper understanding of Israel's cybersecurity policies and practices, the challenges it faces, and the associated international legal responsibilities arising from cyber operations.

1.3.METHODOLOGY OF RESEARCH

his thesis will adopt a mixed-methods approach, primarily utilizing document analysis of reports, news articles, books, and academic articles, and qualitative data collection through and analyzing a wide range of reports, news articles, books, and academic articles to gather qualitative data. This content analysis will help to identify trends, patterns, and insights related to Israel's cybersecurity infrastructure and international law responsibilities. This thesis provides a detailed examination of official documents, policy reports, relevant cyber incident reports, legal documents, and government publications to extract data that pertains to the research problem

1.4.SCOPE AND LIMITATIONS OF THE RESEARCH

This study covers the period from the establishment of Israel to October 7, 2023. Events after this date are excluded from the scope of the study. This choice was made due to the dynamic process that emerged after the events of October 7 and the state of Israel's unrestricted actions, the war crimes it committed, and the opposition to the situation in the international arena.

1.5.LITERATURE REVIEW

Security

The concept of security has been addressed on a wide scale by different authors in the field of international relations and security studies. A literature review reveals that security definitions are addressed from various focal points. Baldwin argues that the concept of security has a multidimensional structure and should not be limited to military threats. He argues that security should be re-evaluated regarding the reference objects of security, namely individuals, states, international systems, and the threats to these objects.[1] Buzan is among those who argue that the Cold War-era definition of security should be expanded and redefined. He believes that security no longer consists only of military threats but should

[1] David A Baldwin, 'The Concept of Security' (1997) 23 Review of International Studies 5.

also include economic, environmental, and social dimensions.[2] Huysmans, on the other hand, argues that security is expressed in adjectives (environmental, military, or social security), but the focus is not on what security means. He mentions that security has a layered structure and characterizes security as a "thick signifier."[3] Ken Booth goes beyond a traditional understanding of security and considers security in terms of human rights, social justice, and economic welfare.[4] Ole Wæver, one of the Copenhagen School authors, states that threats are "constructed" and discusses this in his article "Securitization and Desecuritization".[5] Michael C. Williams examines the political effects of the concept of "securitization" and its use in international politics. He focuses on the role of "language" and "images" in constructing threats.[6]

National Security

According to Knudsen, national security refers to protecting a country's territorial integrity and political sovereignty, as well as protecting critical public functions and vital infrastructure against various threats. Protecting individuals and groups is essential when human rights and personal security are at risk. There are different studies on the definition of national security.[7] Leffler provided a historical overview of national security and analyzed its use in daily politics.[8] Brown, on the other hand, focused on the redefinition of the concept of national security and explained how the concept has been used since World War II to include different issues. Some of these issues are environmental security and non-military threats.[9] Wolfers, on the other hand, argued that the term national security is ambiguous and has different interpretations in political circles. The reinterpretation of the term is discussed in the study titled "Rethinking National Security," similar to Brown's analysis.[10] While it was a concept that included military threats, it has evolved to include non-military threats as

[2] B Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Harvester Wheatsheaf 1991) <https://books.google.com.tr/books?id=_jETAQAAMAAJ>.

[3] Jef Huysmans, 'Security! What Do You Mean?From Concept to Thick Signifier' (1998) 4 European Journal of International Relations - EUR J INT RELAT 226.

[4] Ken Booth, 'Security and Emancipation' (1991) 17 Review of International Studies 313.

[5] Ole Wæver, *Securitization and Desecuritization*, vol 5 (Centre for Peace and Conflict Research Copenhagen 1993).

[6] Michael C Williams, 'Words, Images, Enemies: Securitization and International Politics' (2003) 47 International Studies Quarterly 511.

[7] Bård B Knudsen, 'Developing a National Security Policy/Strategy: A Roadmap' (2012) 30 Sicherheit und Frieden (S+F) / Security and Peace 135.

[8] Melvyn P Leffler, 'National Security' (1990) 77 The Journal of American History 143.

[9] Lester R Brown 1934-, *Redefining National Security* (Worldwatch Institute 1977).

[10] Theodore C Sorensen, 'Rethinking National Security' (1989) 69 Foreign Aff. 1.

well. Thıs thesıs adopts the theoretıcal framework outlıned by Brown. Sorensen also emphasized that not all external adversities affecting national interests constitute a national security problem. Knudsen, who studies how a national security strategy should be formulated, emphasizes the need to adopt a systematic approach and identify security threats when developing a national security policy. Finally, Doyle takes the national security strategy of the United States as a specific case study and discusses the critical policy issues and challenges of the strategy.[11]

Israel's National Security Strategy

Israel's national security strategy derives from its location in the Middle East and the geostrategic context that this location brings. As a result of thousands of years of Jewish experience, encounters with different threats, and ultimately, their attempt to establish a state amid Arab states, their understanding of national security has evolved. In his study, Horowitz examined Israel's national security philosophy at its founding and argued that "constant readiness for war" was a key element.[12] On the other hand, Gil Merom criticized the perception that Israel's national security challenges are unique and pointed out that they are similar to other states.[13] Rodman's comprehensive analysis examines Israel's geopolitical, military, social, and humanitarian elements and argues that Israel's national security strategy has evolved to sign formal peace treaties with countries deemed threatening.[14] This approach exemplified Israel's efforts to move from territorial defense against Arab states to self-protection through diplomatic engagements.

In Israel's national security strategy, not only military elements but also civilian elements are of great importance. In his study on Founding Prime Minister David Ben Gurion's approach to national defense, Yoram Fried has shown that Ben Gurion was not only a leader who addressed military threats but also saw economic, social, and infrastructural problems as national security issues for Israel.[15] Ben Gurion, who stated that eliminating unemployment was as crucial as a forthcoming war, disagreed with IDF officials. Freilich's

[11] Richard Doyle, 'The U.S. National Security Strategy: Policy, Process, Problems' (2007) 67 Public Administration Review 624.

[12] Dan Horowitz, 'The Israeli Concept of National Security' in Talal Asad and Roger Owen (eds) (Macmillan Education UK 1983) <http://link.springer.com/10.1007/978-1-349-17282-5_4> accessed 20 March 2024.

[13] Gil Merom, 'Israel's National Security and the Myth of Exceptionalism' (1999) 114 Political Science Quarterly 409.

[14] David Rodman, 'Israel's National Security Doctrine: An Introductory Overview' (2001) 5.

[15] Yoram Fried, 'Military, Civilian, or Both: David Ben-Gurion's Perception of National Security After the War of Independence' (2020) 7 Contemporary Review of the Middle East 125.

book “Israeli National Security: A New Strategy for an Era of Change” emphasized the need for a new strategy against changing times.[16] He stressed the need for a strategy that addresses Israel's conventional problems as well as problems such as weapons of mass destruction, terrorism, and cyberattacks.

Cyber Security

The concepts of cyberspace and cybersecurity differ definitively, but they contain some basic expressions. The first work in which the concept of cyberspace appears is William Gibson's 1984 work “Neuromancer.”.[17] Gibson defines cyberspace as “consensual hallucination.” On the other hand, Esther examined the information age and the information economy in a period that can be considered early.[18] In this analysis, she divided the economy into waves and characterized First Wave economies as agriculture-based economies. Second Wave economies are those in which land is valuable, but labor is integrated with machines. The industrial revolution still needs to be completed and is embedded in the Third Wave economy, the knowledge-based economy. She described cyberspace as a product of the information age, “a bioelectronic environment that is literally universal.” She included everything from telephone cables to internet networks and even electromagnetic waves in cyberspace. In addition to academic texts, definitions of cyberspace by relevant organizations and leading non-state actors are also valuable. The National Institute of Standards and Technology defines cyberspace as “The global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[19] Doyle defines cyberspace as a vast, complex, and diverse electronic mass of inter-communication, where all communication networks, databases, and information sources come together to form an extensive, complex, and diverse electronic mass of inter-communication.[20] The nature of cyberspace should be understood not only as a technological construct but also as an area where states can exert

[16] CD Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford University Press 2018) <https://books.google.com.tr/books?id=sPdJDwAAQBAJ>.

[17] W Gibson, *Neuromancer* (Ace Books 1984) <https://books.google.com.tr/books?id=1_9LQuiVDcgC>.

[18] ESTHER DYSON, ‘Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)’ (1996) 12 The Information Society 295.

[19] Richard L Kissel, ‘Glossary of Key Information Security Terms’ [2013] NIST <https://www.nist.gov/publications/glossary-key-information-security-terms-1> accessed 6 June 2024.

[20] Doyle (n 11).

power and influence. In the 1960s, the Advanced Research Projects Agency Network (ARPANET), funded by the US Department of Defense, is considered the Internet's ancestor. ARPANET was developed to enable data sharing and communication between various universities and research centers.

In 1969, the first successful message was sent from the University of California Los Angeles (UCLA) to the Stanford Research Institute (SRI). This event is considered the birth of the Internet. In 1971, Ray Tomlinson sent the first e-mail on the ARPANET, laying the foundation for electronic mail. Work on protocols and standards used in inter-computer communication accelerated during this period. In the late 1970s, the TCP/IP protocol, developed by Vint Cerf and Bob Kahn, became the basic communication protocol of the Internet. TCP/IP laid the foundation for today's Internet by enabling secure and organized transmission of data packets. Warner provides this historical narrative in his article "Cybersecurity: A Pre-history.".[21]

Due to the nature of cyberspace, actors in cyberspace can pose threats and be the target of threats. The elimination of these threats can be called cyber security. What is meant by cyber security is the security of information/data. Merriam-Webster defines cyber security as the protection of computer systems and networks from unauthorized interference.[22] Morten Bay focused on the definition of cybersecurity in the aftermath of the leak of classified information from the NSA by Edward Snowden in 2013.[23] Bay emphasized that cyber security definitions should cover both technical and social issues in the post-Snowden era. In the study titled "Towards a More Representative Definition of Cyber Security," Schatz examined the concept of cyber security with statistical data on the range and frequency of use and similar data. In the light of these data, the meanings and uses represented by cyber security definitions were examined.[24] One of the most comprehensive studies on this subject belongs to Singer and Friedman. Singer and Friedman's "Cybersecurity and Cyberwar: What Everyone Needs to Know", Singer and Friedman

[21] Michael Warner, 'Cybersecurity: A Pre-History' (2012) 27 Intelligence and National Security 781.

[22] 'Cybersecurity Definition & Meaning - Merriam-Webster' <https://www.merriam-webster.com/dictionary/cybersecurity> accessed 4 June 2024.

[23] Morten Bay, 'WHAT IS CYBERSECURITY? In Search of an Encompassing Definition for the Post-Snowden Era' (2016) 6/2016 French Journal for Media Research.

[24] Daniel Schatz, Rabih Bashroush and Julie A Wall, 'Towards a More Representative Definition of Cyber Security' (2017) 12 J. Digit. Forensics Secur. Law 53.

present a comprehensive study of the emergence of the vulnerabilities of information technologies to cyber warfare.[25]

Yang Lu conducts an empirical study on cybersecurity issues in his research. Taking a holistic approach to cybersecurity issues, Lu utilized 50 articles and aimed to obtain a comprehensive result.[26] Myram Dunn Cavelty emphasizes that cyber security is one of today's most important national security issues. Cavelty discusses the technical nature of cybersecurity and cyberspace, cyber threats, military and civilian approaches to cybersecurity, and cyber risks and threats.[27]

One of the biggest threats to cybersecurity is cyber-attacks. In their study, Jibi Biju, Neethu Gopal, and Anju Prakash discuss the different types of cyber-attacks, their methods, and their physical and social consequences.[28] It was stated that due to the easier accessibility of technology in human life, the possibility of being exposed to cyber-attacks has increased. Splunk, a company acquired by Cisco, provides consultancy on cyber threats and published a report, "Top 50 Cybersecurity Threats", explaining the most critical cyber security and how they work.[29] Mahmoud's "Cyber Attacks: The Electronic Battlefield" emphasizes that warfare is now taking place in cyberspace and the role of cyberattacks in cyber-warfare. The report treats cyber-attacks as a form of electronic warfare and examines the security and policy implications.[30] "Impact of Cyber-Attacks on Critical Infrastructure" explores cyber-attacks effects on critical infrastructure, highlighting the vulnerabilities and potential consequences.[31] According to Tabansky, infrastructure systems such as pipelines, communication and healthcare services, roads, and bridges are critical infrastructures that can pose political, strategic, and security challenges in the event of a disruption. Tabansky emphasizes that critical infrastructures now have a cyber dimension, with computerized

[25] PW Singer and A Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*® (Oxford University Press 2013) <https://books.google.com.tr/books?id=p8COAgAAQBAJ>.

[26] Yang Lu, 'Cybersecurity Research: A Review of Current Research Topics' (2018) 03 Journal of Industrial Integration and Management 1850014.

[27] MD Cavelty, *The Politics of Cyber-Security* (Taylor & Francis 2024) <https://books.google.com.tr/books?id=jzAKEQAAQBAJ>.

[28] Jibi Biju, Neethu Gopal and Anju Prakash, 'CYBER ATTACKS AND ITS DIFFERENT TYPES' (2019) 6 International Research Journal of Engineering and Technology <https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf> accessed 7 August 2024.

[29] Splunk, 'Top 50 Cybersecurity Threats' (2024) <https://www.splunk.com/en_us/form/top-50-security-threats.html> accessed 5 June 2024.

[30] Khalid Walid Mahmoud, 'Cyber Attacks: The Electronic Battlefield' (Arab Center for Research & Policy Studies 2013) <https://www.jstor.org/stable/resrep12651> accessed 4 June 2024.

[31] Kutub Thakur and others, 'Impact of Cyber-Attacks on Critical Infrastructure', *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (IEEE 2016) <http://ieeexplore.ieee.org/document/7502286/> accessed 7 June 2024.

components transforming traditional infrastructures into information infrastructures.[32] Daricili, on the other hand, analyzed the cyber-attacks associated with the Russian Federation. Daricili mentioned that the Russian Federation uses its growing power in cyberspace as a sanctioning tool in its international policies. The cyber attacks against Estonia (2007-2008), Georgia (2008), and Ukraine (2014) were associated with the Russian Federation, and the cyber power of the RF was analyzed through these actions.

Cybersecurity in Israel

In his article "Cyber Power in the Changing Middle East" where geopolitical conflicts in the Middle East are discussed in the context of cyber power and cyber security, Tabansky examined the importance of the countries in the region in terms of their cyber power as well as their conventional power.[33] Israel is one of the most capable countries in the cyber security field according to National Cyber Power Index 2022.[34] One of the most comprehensive studies on this subject is the book "Cybersecurity in Israel" by Lior Tabansky and Isaac Ben Israel.[35] The book is the first comprehensive analysis of Israel's cybersecurity. It addresses Israel's cybersecurity on a technological, political, social, and organizational basis, including the factors affecting its development. The relationship between Israel's cybersecurity understanding and its national security understanding and grand strategy is discussed, and it is stated that R&D investments in Israel have led to the development of high technology. State actors in Israel's cybersecurity are discussed comprehensively, and a detailed context of the cybersecurity strategy is presented. Adamsky draws attention to some points regarding Israel becoming one of the leading cyber powers.[36] These are innovative practices, internationally effective solutions, integration across sectors, the ability to adapt to new threats and systems constantly, and the importance given to education. These efforts have made Israel a model in the field of cyber security, enabling it to effectively protect its cyber infrastructure and be effective in this field. Describing Israel as a start-up nation and

[32] Lior Tabansky, 'Israel Defense Forces and National Cyber Defense' (2020) 19 Connections: The Quarterly Journal 45.

[33] Lior Tabansky, 'Cyber Power in the Changing Middle East' <http://turkishpolicy.com/article/804/cyber-power-in-the-changing-middle-east> accessed 25 June 2024.

[34] 'National Cyber Power Index 2022' (Harvard's Belfer Center for Science and International Affairs 2022) <https://www.belfercenter.org/publication/national-cyber-power-index-2022> accessed 7 August 2024.

[35] Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (Springer International Publishing 2015) <https://link.springer.com/10.1007/978-3-319-18986-4> accessed 19 March 2024.

[36] Dmitry (Dima) Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy' (2017) 40 The Washington Quarterly 113.

linking its success in this field to its success in cyber security, Freilich states that Israel is a global leader in this field thanks to the right relationships and innovative approaches of civilian and military organizations in Israel.[37] Another comprehensive study on Israel's cyber security structure is "Israel's National Cybersecurity and Cyberdefense Posture".[38] This study summarizes cybersecurity in Israel with a chronological approach. Then, it discusses Israel's state and non-state actors and compiles the laws and resolutions adopted by the Israeli government in this field. One of the most critical units in the field of cyber security in Israel is Unit 8200. Unit 8200 is the signals intelligence unit of the IDF and is also responsible for activities in cyberspace in the modern era. One of the important studies on this subject is "Trend analysis: The Israeli Unit 8200 - An OSINT-based study".[39] This study discusses the historical background, current position, and activities of Unit 8200. This report also discussed the Israeli cyber security approach. In the report, which discusses Israel's national cyber security understanding, which institutions and organizations are effective, issues such as public-private partnership and academia effect are also mentioned. On the other hand, Raska addressed Israel's cyber security structure with the analogy of the Iron Dome air defense systems in Israel. He stated Israel reinforced its cyber security strategy with multi-layered, automated systems and well-trained personnel.[40]

Cyber Operations and Law of State Responsibility

One of the questions this thesis seeks to answer is the responsibilities of states in terms of cyber operations carried out by non-state organizations. Studies in this field were thoroughly analyzed, focusing on their methodologies and contributions to understanding state responsibilities in cyber operations. In one of the early studies, "State Responsibility for Cyber-Attacks on International Peace and Security," Kulezsa examined the responsibilities of states in cyber operations, the legal interpretation of such operations, and their evaluation in the context of an "attack" in the context of international law.[41] Analyzing the Estonian Cyber Attacks, one of the important events in this field, Andres and Shackleford

[37] CD Freilich, MS Cohen and G Siboni, *Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power* (Oxford University Press 2023) <https://books.google.com.tr/books?id=LnjAEAAAQBAJ>.

[38] Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations' (ETH Zurich 2020) Report <https://www.research-collection.ethz.ch/handle/20.500.11850/440107> accessed 20 June 2024.

[39] Sean Cordey, 'The Israeli Unit 8200: An OSINT-Based Study' (Center for Security Studies 2019).

[40] Michael Raska, 'Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope' (2014) 192 RSIS Commentaries <https://hdl.handle.net/10356/94095> accessed 7 August 2024.

[41] Joanna Kulesza, 'State Responsibility for Cyberattacks on International Peace and Security'.

examined the responsibility of states in the context of cyber operations.[42] They argue that since it is challenging to attribute cyber attacks to a state and to prove the operation in technical terms, the international community should introduce a common control mechanism and standard. Margulies, on the other hand, discusses the inadequacies of international law in terms of the responsibility of states in cyber attacks.[43] Stating that cyber threats bring new burdens to international law, Margulies says that international law is designed for kinetic attacks and the "effective control" test is used. He argues that this approach needs to be revised in the cyber domain and that operations carried out by non-state actors are difficult to monitor and control. Therefore, a 'virtual control' test is proposed for cyber attacks. This test aims to deter states from using these groups by imposing responsibility on the state that assists non-state actors. He argues that this deterrence would provide a more effective route for developing international law in cyberspace.

The 2007 cyber-attacks against Estonia highlighted the potential danger of cyber-attacks for NATO and other countries. Accordingly, NATO established the "Cooperative Cyber Defense Centre of Excellence" in 2008 in Tallinn, where the attacks occurred. This center is NATO's military arm in the cyber domain and provides assistance on issues such as information sharing and cyber defense among member states. At the invitation of this center, a Group of Experts of 20 members was formed. Under the leadership of Michael N. Schmitt, this group conducted a non-binding study on cyber operations as jus ad bellum (right to war) in the context of international law. The "*Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0" is* an academic study that examines cyber operations through different legal approaches, from international humanitarian law to the law of state responsibility. It outlines a theoretical and practical approach to cyber operations and international law.[44] This is one of the most comprehensive studies in the literature. François Delerue has conducted a thorough study on how international law applies to cyber operations. The book provides a systematic assessment of attribution, lawfulness, and legal solutions to cyber challenges, demonstrating the limits of international law and its inadequacies in addressing the problems

[42] Scott J Shackelford and Richard Andres, 'STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM' (2010) 42 Georgetown Journal of International Law 971.

[43] Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melbourne Journal of International Law 496.

[44] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 24 June 2024.

of cyber operations.[45] Waxman analyzes cyber operations within the framework of the UN Charter and examines the use of force in cyberspace.[46] Finlay and Payne focused on the attribution of cyber attacks. They examined how states can attribute cyber-attacks to the actor perpetrating the attack and the limits of how they can react to these attacks.[47] Roscini deals with cyber-attacks in the context of traditional armed attacks and analyzes the applicable law in this context.[48] Tsagourias relates the principles of state responsibility to cyberspace. Focusing on self-defense and the attribution problem, Tsagourias discusses the conditions under which a cyber attack can justify the right of self-defense.[49] Finally, Rid and Buchanan address the attribution problem in cyberattacks and analyze the difficulties in attributing cyberattacks by addressing the technical and political dimensions of attributing a cyberattack to a state.[50]

One of the most recent studies on this topic belongs to Hatice Kübra Ecemiş Yılmaz. The author's book, "Siber Operasyonların Uluslararası Hukukla İlişkilendirilemesi" is a comprehensive work on the legal dimensions of cyber operations.[51] In her study, Ecemiş Y. examines the nature of cyber operations and provides a general assessment. She systematically analyzes cyber operations within the framework of contemporary international law norms, examining how traditional international law rules applicable to conventional attacks, such as the UN Charter and the "Prohibition on the Use of Force," operate in the cyber domain. The book explores the conditions under which a cyber operation can be attributed to a state and what is required for such an operation to create legal responsibility for that state. It discusses under what circumstances cyber operations would be unlawful within the context of "Grounds of Wrongful Act." Finally, it addresses cyber operations in the context of the Law of State Responsibility and examines the application of this law in cyberspace.

---

[45] François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) <https://www.cambridge.org/core/books/cyber-operations-and-international-law/74D210E76E46531542AD27CECF07ABDE> accessed 24 June 2024.

[46] Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) null Information Systems: Behavioral & Social Methods eJournal null.

[47] Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 202.

[48] Marco Roscini, 'Cyber Operations: Identifying the Problem and the Applicable Law (Chapter 1)' (2014) null PSN: Cyber-Conflict (Inter-State) (Topic) null.

[49] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 Journal of Conflict and Security Law 229.

[50] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38 Journal of Strategic Studies 4.

[51] Hatice Kübra Ecemiş Yılmaz, *Siber Operasyonların Uluslararası Hukukla İlişkilendirilmesi* (Yetkin Yayınları 2023) <https://www.seckin.com.tr/kitap/449826444> accessed 24 June 2024.

2. ISRAEL'S NATIONAL SECURITY CONCEPT AND TECHNOLOGY

Israel is a state which has been embroiled in many conflicts and wars since its establishment. It has had a changing and evolving understanding of national security in its conflicts and wars with neighboring states and non-state actors. Today, it is essential to find out the underlying factors behind its cyber security capabilities, its high-tech industry's success compared to its low population, and the fact that it has become a start-up country.[52] Since its official establishment in 1948, Israel has constantly faced security problems and has been striving to strengthen its army and economy with a "Quality versus Quantity" approach.

With this approach, Israel envisioned that it could overcome its weaknesses, such as the economy, the number of troops, and the low population, only by making the best use of the means at its disposal. Israel's first prime minister and minister of defense, David Ben Gurion, laid down this principle. The low population problem led to the establishment of a system where the entire population benefited from educational opportunities. During the compulsory military service, Israel continued this education and discovered the areas of capability of its citizens. Afterward, it provided academic continuity in the army by making offers to the citizens it trained in the army according to their needs.

This structure, which later separated from the army and formed the backbone of high-tech companies, is known as the Academic Reserve. To understand the current state of Israel's cybersecurity, it is necessary to examine the origins of its high-tech industry. At this point, the security policies that Israel has pursued since its establishment are essential because they have shaped (and at some point necessarily directed) the educational system, professionalization, and innovative capabilities of the society, as well as shaping (and at some point necessarily directing) the civilian industries, enabling Israel to gain an essential place in cybersecurity. The national security strategies drafted by Prime Minister Ben Gurion at its founding are fundamental to Israel's grand strategy today. However, Ben Gurion's strategies emphasized that security is not only in the military sense but that actions in the social sphere also ensure the long-term security of a nation. Considering that all these

[52] 'How Israel Turned Itself into a High-Tech Hub - BBC News' <https://www.bbc.com/news/business-15797257> accessed 20 March 2024.

policies are based on a national security strategy, the reasons behind the cyber security, high technology, and start-up country that Israel has achieved today will be understood by examining this strategy.

2.1. Security

Security refers to the absence of threats to individuals, society, or the state, encompassing economic, environmental, social, and traditional military challenges that impact the stability of values and interests. Security can be achieved through different means and methods. The level of security demanded may vary depending on the position, values, and interests of the reference object of security. [53]

Security concerns exist at varying levels for every individual, community, and state. The concept of security can be divided into "Traditional Security" and "Non-Traditional (New) Security". The traditional understanding of security is geopolitical security, including deterrence, power balance, and military strategy.[54] The military security of states until the modern period, as well as their territorial integrity and efforts to protect their borders, can be evaluated in this definition. In the period when the traditional understanding of security was dominant, security was seen as an area that concerned only the armed forces. States pursued policies to increase their military capacities and built their strategies on military superiority to meet their security needs.

The nontraditional or New Security Approach focuses on nonmilitary threats. It does not only take the state as the reference object of security but also the individual and society. Issues such as human security, economic security, or environmental security are evaluated with this approach.[55]

Security is a fundamental issue in international relations, influencing how states shape their domestic and foreign policies. States consider their security needs when determining their domestic and foreign policies. Today, states are exposed to many social and individual threats. These threats create many comprehensive and diversified security problems. Actors, the reference objects of security, have defined security according to their specific situations. Each actor experiences security problems with different intensities at

[53] Baldwin (n 1) 11–12.
[54] Allan Collins, *Çağdaş Güvenlik Çalışmaları* (Nasuh Uslu tr, Uluslararası İlişkiler 2017) 416.
[55] ibid 4-5–416.

different times and places.[56] States with different geopolitical positions in different geographies have different security needs. A country like Turkey, which witnesses the problems created by the straits, different ethnic and religious groups, terrorism, and the struggle of great powers, and the state of Taiwan, which has legitimacy problems in the international arena, cannot be expected to have the same security definitions and tools.

"National Security," the basis of these security concepts, constitutes the primary security ground for nation-states. Many factors influence the formation of definitions of security for countries. The history, geopolitical position, religious and cultural values, and economic and social structure of countries have an impact on the understanding of security. The interests of that state shape the development of national security policies, the threats directed against it, and the point of taking measures.[57] The interests of a nation are the targeted goals and must be protected to increase the country's existence and the nation's welfare.[58] On the other hand, threats are direct dangers to a country's national interests posed by state or non-state actors, either domestically or internationally, in terms of intent and expression, as well as in terms of developing capabilities and engaging in activities. According to Knudsen, a threat is a potential danger or harm that could damage, disrupt, or negatively affect a country's security, interests, or prosperity. Threats can come from various sources, such as other states, non-state actors, natural disasters, technological vulnerabilities, economic instability, and social challenges. In the context of national security, threats are assessed according to their ability and intent to harm or pose risks to a nation's security.[59]

2.2. National Security Strategy

According to Knudsen[60], national security refers to protecting a country's territorial integrity and political sovereignty, as well as protecting critical public functions and vital infrastructure against various threats. Protecting individuals and groups is essential when human rights and personal security are at risk.[61] National security requires a comprehensive

[56] Orhan Karaoğlu and Nail Elhan, *İsrail Bir Ülkenin Akademik Anatomisi* (2023) 136.

[57] Ken Booth, *Theory of World Security* (Cambridge University Press 2007) 186 <https://www.cambridge.org/core/books/theory-of-world-security/CF242B3425F9FFAA026A7789AA7A72CD> accessed 20 March 2024.

[58] Karaoğlu and Elhan (n 56) 137.

[59] Knudsen (n 7) 136.

[60] ibid 2.

[61] ibid 5.

approach that includes social and human security dimensions. This approach ensures that both external and internal security issues are effectively addressed.

A national security strategy (NSS) is a comprehensive plan that outlines a country's approach to using all instruments of state power, both military and non-military, to secure and enhance the country's national interests. It includes setting the nation's objectives, identifying potential threats, and determining the resources and actions needed to achieve those objectives while maintaining security. The strategy also promotes a coordinated approach in several areas, including national defense, foreign policy, and homeland security.[62]

Yarger[63] described strategy as "the art and science of developing and using the political, economic, socio-psychological, and military powers of the state in accordance with policy guidance to create effects and set conditions that protect or advance national interests relative to other states, actors, or circumstances."

According to Sharon[64], a national strategy involves a comprehensive approach to establishing objectives, policies, programs, actions, decisions, or resource allocations to protect or advance a country's national interests about other states, actors, or circumstances.

The National Security Strategy (NSS) document is a key policy document that outlines a nation's approach to national security, including its goals, priorities, and strategies for protecting and advancing its interests. National Security Strategies can be declared an official document, prepared by the state and then kept secret, or an attempt to prepare an official document does not always occur. Some states do not publish them for security reasons, while governments are legally obliged to publish them publicly periodically in other states.

In the U.S., the National Security Strategy is a report provided annually by the President to Congress, as prescribed by the "Goldwater-Nichols Department of Defense

[62] Doyle (n 11) 624.

[63] Harry R Yarger, *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century* (Praeger Security International 2008) 4.

[64] Sharon L Caudle, 'National Security Strategies: Security from What, for Whom, and by What Means' (2009) 6 Journal of Homeland Security and Emergency Management 1 <https://www.degruyter.com/document/doi/10.2202/1547-7355.1526/html> accessed 19 March 2024.

Reorganization Act of 1986".[65] The National Security Strategy (NSS) document in the United States typically includes elements such as the nation's vital interests, threat assessments, strategic objectives, policy approaches, defense and military strategy, diplomatic priorities, economic security considerations, homeland security measures, and resource allocation evaluations. It serves as a guiding framework for policymakers to effectively address security challenges and advance national security objectives.

In short, a national security strategy is a document or plan that a nation creates to protect its interests in a changing global landscape, identify threats to its security, and utilize all available resources to achieve its security objectives.[66]

2.3. Israel's National Security Strategy

In today's world, problems change rapidly and vary in scope and depth daily. In addition to geopolitical problems, security issues concerning humanitarian, economic, and social spheres are the main concerns of countries, necessitating an ongoing comprehensive security strategy. National security policies are more flexible than long-term and short-term strategies.[67]

The State of Israel is a parliamentary democracy structured on the separation of powers. The state does not have a written constitution. Instead of a constitution, Israel is governed by the Fundamental Law passed by the Knesset in 1948.[68] Attempts to create a constitution since 1948 have failed. The system is governed by a quasi-constitutional status based on fundamental laws and rights.[69] The head of state, elected by the Knesset, the parliament, for a 7-year term, has representative powers. The absolute authority is vested mainly in the prime minister and the cabinet. Israel's first president was Chayim Weizmann. The first prime minister was David Ben Gurion.[70] Ben Gurion is considered the father of modern Israel and the intellectual and political leader of its political and social structure.

---

[65] Doyle (n 11) 625.
[66] ibid.
[67] Yehezkel Dror, 'Does Israel Have a National Security Policy?' (Institute for National Security Studies 2011) 38 <https://www.jstor.org/stable/resrep08959.7> accessed 19 March 2024.
[68] KN Sinha, 'Political System of Israel' (1960) 21 The Indian Journal of Political Science 289, 290.
[69] 'Constitution for Israel' <https://knesset.gov.il/constitution/ConstIntro_eng.htm> accessed 20 March 2024.
[70] Sinha (n 68) 292.

The State of Israel has faced many security challenges since its establishment. The intense conflict environment that started with the First Arab-Israeli War in 1948, the year of its establishment, has continued with varying intensity until today.[71] The first war in Israel's official history was the "War of Independence" in 1948. This war has been one of the most critical factors in the formation of Israel's understanding of security. Due to its geographically unprotected borders, much smaller population compared to the enemies they face, and limited access to manpower, military ammunition, and equipment, the state of Israel has defined its security environment as an "existential threat"[72] and based its security policies on the principle of fighting against this threat. This understanding of struggle has evolved over the years, producing the essential elements that shape the Israeli security understanding.[73]

Yaakov Amidror[74] states: "From its very inception, the State of Israel (and before it, the pre-state Jewish Yishuv) had to confront an existential security threat - a narrow territorial entity with its back to the Mediterranean Sea, surrounded by Arab foes sworn to its extinction."

Israel, founded with a strong emphasis on its ethno-religious Jewish identity, has engaged in various military and political actions to secure and expand its borders. Since its establishment, the state has been involved in conflicts with neighboring countries, including Egypt, Syria, Lebanon, and Jordan, resulting in periods of territorial expansion. These actions have been part of broader regional dynamics and complex historical circumstances involving territorial disputes and security concerns. [75]

The total area of Israel is 22,145 square kilometers (21,671 square miles). (The country is essentially long and narrow, with the longest distance from north to south is about 290 miles (470 km) and the widest distance from east to west is 85 miles (135 km). The country borders Lebanon to the north, Syria to the northeast, Jordan to the east, Egypt to the

[71] Rodman (n 14) 71.
[72] Horowitz (n 12) 11; Merom (n 13) 418.
[73] Rodman (n 14) 71.
[74] Yaakov Amidror, 'Israel's National Security Doctrine' (*JISS*, 2021) <https://jiss.org.il/en/amidror-israels-national-security-doctrine/> accessed 19 March 2024.
[75] Israel's aggression against the people of Gaza as of October 7, 2024 is beyond the scope of this study and is therefore not discussed in detail.

southwest, and the Mediterranean Sea to the west.[76] Israel's economic, financial, technological, and demographic center is heavily concentrated along the Mediterranean seacoast on a narrow strip of just 100 km between Haifa and Ashdod". [77]

By land size, Israel ranks 154th in the world. Despite its small land area and relatively small population, it has significantly influenced international politics and the historical process of the Middle East's geography.

Since its establishment in 1948, Israel has fought six major wars, all of them against its Arab neighbors in the Middle East. The War of Independence in 1948-1949, the Sinai War in 1956, the Six Day War in 1967, the War of Attrition in 1969, the Yom Kippur War in 1973, and the Lebanese Civil War from 1975 to 1990. Also, essential events in Israel's history are the First and Second Intifada, the Palestinian uprising against Israeli occupation; the month-long war with Lebanon's Hezbollah in 2006; and the conflicts with the Palestinian political party Hamas in 2008, 2014, 2021, and most recently in October 2023. In addition, in the 1991 Gulf War, Iraq, led by Saddam Hussein, struck Israeli territory with ballistic missiles, but Israel did not retaliate. These large-scale and other medium and small-scale conflicts are the main, but not the only, problem of Israel's national security. Israel lacks strategic depth due to its geopolitical position.[78] The Arab states of different religions and ethnicities surrounding it, the conflict with the Palestinian people, and its geographical location in a narrow area deprive Israel of strategic depth.[79]

In 1948, the government and authorities in Israel, a newly emerged state from the war, were aware that the ceasefire was not a peace agreement and that there would be a second round. IDF officials, therefore, demanded that the government put all resources under the control of the army and prepare for a second Arab attack, which was seen as the most

[76] 'Coğrafya ve İklim' <https://embassies.gov.il/ankara/AboutIsrael/history/Pages/cografyaveiklim.aspx> accessed 20 March 2024.

[77] SA Cohen and A Klieman, *Routledge Handbook on Israeli Security* (Taylor & Francis 2018) 81 <https://books.google.com.tr/books?id=2tNyDwAAQBAJ>.

[78] Gil Merom, "Israel's National Security and the Myth of Exceptionalism," *Political Science Quarterly* 114, no. 3 (1999): 413, https://doi.org/10.2307/2658204;

Gadi Eisenkot and Gabi Siboni, "Guidelines for Israel's National Security Strategy | The Washington Institute," Policy Focus (Washington DC: The Washington Institute for Near East Policy, October 2019), 43, https://www.washingtoninstitute.org/policy-analysis/guidelines-israels-national-security-strategy.

[79] William Wunderle and Andre Briere, 'U.S. Foreign Policy and Israel's Qualitative Military Edge' [2008] Policy Focus 1; *The Oxford Handbook of Israeli Politics and Society* (Oxford University Press 2018) 109–112 <https://academic.oup.com/edited-volume/34274> accessed 19 March 2024.

imminent threat.[80] However, then Prime Minister David Ben Gurion argued that the main existential threat to the state was not only Arab aggression but that social, economic, and industrial development was as vital as any other threat. This was interpreted as a departure from the security criteria of a newly formed state fresh from war, and IDF officials objected. However, Ben Gurion believed that even if the next battle were won, the state would collapse for other internal reasons if the necessary measures were not taken. Economically, providing jobs for its citizens, industrial development to solve the country's infrastructure and other construction problems, encouraging diaspora Jews to immigrate to Israel and settling new settlers in the occupied territories, and maintaining national education, another critical issue, were the main issues that Ben Gurion considered vital for Israel's national security.[81]

At the same time, the Prime Minister did not ignore his country's short-term military threats and military objectives. Still, at the same time, in the long term, Israel's survival depended on the fulfillment of these requirements. A National Security doctrine was needed to define Israel's policies in this context. Some senior IDF officials presented the government with a request to temporarily transfer the country's budget and control entirely to them. Ben Gurion played an essential role in shaping Israel's national security policy. Under Ben-Gurion's leadership, Israel developed security strategies in the economic, social, and diplomatic spheres, as well as in the use of military force. These strategies were based on various policies and practices to counter threats in Israel's environment and to ensure the security of the state. Therefore, it is possible to find the determinants of Ben-Gurion's national security policy not in a series of official documents but in the policies and practices under his leadership. The national security doctrine drafted by Prime Minister David Ben Gurion and read in parliament was Israel's first recorded national security document. However, this text was read as a declaration by Ben Gurion in the Israeli parliament. A national security declaration as we know it today has not been officially announced publicly.

Rodman broadly defines national security doctrine as the totality of a state's military, diplomatic, economic, and social policies in the context of its national security interests.[82] According to Deror, a state's national security is not just a document. National security is represented in its behavior and practices. To understand Israel's national security doctrine,

[80] Fried (n 15) 136–137.
[81] ibid 137.
[82] Rodman (n 14) 72.

understanding, and framework, it is necessary to examine its military, political, and security policies and practices. Consistent and repeatedly emphasized statements reveal a pattern of "national security in action."[83]

Israel's national security challenge has transcended the boundaries of the traditional battlefield - and continues to have implications beyond those boundaries. Despite the absence of a formal national security doctrine, the combined effects of the state's environment and experiences have persuaded Israeli defense planners to develop core security concepts. These concepts respond to the geographic, diplomatic, and resource environment required for Israel's survival while at the same time being influenced by the state's wartime and peacetime experiences.[84]

Despite its practical security approach, the State of Israel has no approved official National Security declaration or text, except for one.[85] In the autumn of 2019, former IDF Chief-of-Sta Lt. Gen. (res.) Gadi Eizenkot and his colleague Dr. Gabi Siboni published a detailed document that outlines the problems Israel faces and ways to address them. However, even this document did not meet the requirements of an official security document. Because no official authority had approved it, it could only be validated through Israel's security policies in practice. As a counter-example, in the US, according to the Goldwater-Nichols Act of 1986, every incoming President must annually declare a National Security Strategy report. In practice, however, it is published every four years.[86]

In many Western states, it has become the norm for the incoming government to publish a National Security Strategy or Doctrine document intended to serve as a reference point for the country's economic, political, military, and humanitarian policies. National Security Strategies shed light on the country's security needs, interests, and limitations for current and future decision-makers in their decisions and policy-making.[87]

Israel's unique security environment and challenges have led to the absence of an official national security strategy document. The obstructive attitude of Israel's political and

[83] Dror (n 67) 37.
[84] Stuart A Cohen, 'DAVID RODMAN'S "ISRAEL'S NATIONAL SECURITY DOCTRINE":' (2001) 5 71.
[85] Amidror (n 74).
[86] Daniel Ackerman, 'From Ben-Gurion to Netanyahu: The Evolution of Israel's National Security Strategy' [2019] FDD 1 <https://www.fdd.org/analysis/2019/05/13/from-ben-gurion-to-netanyahu-the-evolution-of-israels-national-security-strategy/> accessed 19 March 2024.
[87] Fried (n 15) 127.

bureaucratic structure, ad hoc strategic thinking, the volatility created by an ever-changing environment of threats and interests, and the lack of coordination and power sharing among the state's security services are among the reasons for this. These issues pose serious problems for Israel's defense capabilities. They may limit their ability to adapt quickly and actively to dynamic security challenges, as well as to long-term planning and optimal use of resources, which are the main structural inputs of defense. [88] Freilich stated that Israel, as a country with limited defense capabilities under these conditions, should develop a comprehensive and renewable strategy in its unique security environment.[89]

The understanding of national security, which has developed and evolved since the establishment of the State of Israel, initially encompassed state-to-state struggles but later changed with the emergence of local and regional non-state actors. Although Israel has defined non-state actors such as Hamas and Hezbollah as terrorist organizations, this definition has not been accepted by all countries. Although the actors Israel considers threats to have diversified, it has remained faithful to the basic principles of national defense shaped by the first prime minister, Ben Gurion.

2.4. Basic Principles of Israel's National Security Strategy

2.4.1. Iron Wall Doctrine and Ze'ev Jabotinsky

"*There can be no voluntary agreement between ourselves and the Palestine Arabs. Not now, nor in the prospective future."*[90]

The "Iron Wall" doctrine, formulated by Ze'ev Jabotinsky in 1923, is a cornerstone of Israel's security policies and its approach to relations with the Arab world. This strategy is based on the belief that Israel's military strength must be used to force the Arabs to negotiate, ultimately leading to long-term peace.

[88] Chuck Freilich, 'Israel's National Security Policy' in Reuven Y Hazan and others (eds), *The Oxford Handbook of Israeli Politics and Society* (Oxford University Press 2021) 427 <https://doi.org/10.1093/oxfordhb/9780190675585.013.25> accessed 19 March 2024.

[89] ibid 428.

[90] Jabotinsky (n 90) 2.

Ze'ev Jabotinsky (1880-1940), an influential figure in Jewish nationalism and the founder of Revisionist Zionism, emphasized the importance of the territorial integrity of Eretz Israel and the immediate establishment of Jewish sovereignty. [91]

He was an important figure of Jewish nationalism and the founder of Revisionist Zionism. Born in Odessa, Jabotinsky became a journalist and worked for Zionist ideology for the rest of his life. During World War I, he helped organize Jewish volunteer units within the British army and served in the Zion Mule Corps. Elected to the Zionist Executive Committee in 1921, Jabotinsky soon disagreed with Chaim Weizmann over policies he believed would jeopardize the Zionist goal. He resigned in 1923 and founded the World Revisionist Zionist Union and the youth movement Betar. He later became the leader of the New Zionist Organization and the militant Irgun group, opposing the partition of Palestine. [92]

In his pivotal article "The Iron Wall," Jabotinsky argued that Jewish settlement in Palestine would inevitably face Arab resistance and therefore required military protection. He famously stated, “There can be no voluntary agreement between ourselves and the Palestine Arabs. Not now, nor in the prospective future.” According to Jabotinsky, any voluntary agreement with the Arabs was unlikely, necessitating the use of military force to secure a Jewish state. [93]

The Iron Wall doctrine reflects Jabotinsky’s belief that the Arabs would never willingly accept the establishment of an Israeli state in Palestine. [94] To ensure the security of Israel and compel Arab states to negotiate, a powerful and impenetrable military force was essential. This strategic doctrine has played a vital role in shaping Israel's military and diplomatic strategies, aimed at safeguarding its independence and ensuring its security in the region.

2.4.2. Military Power Supremacy on the Road of Peace

Ze'ev Jabotinsky argued that the Zionist movement should build an “iron wall” military force that the Arabs could not overcome. According to him, this solid and impenetrable

[91] ibid 129.
[92] Avi Shlaim, *The Iron Wall: Israel and the Arab World* (Penguin 2015) 128.
[93] Avi Shlaim, *The Iron Wall: Israel and the Arab World* (Penguin 2015) 128.
[94] Shlaim (n 91) 133.

military force would make the Arabs realize the futility of their resistance and force them to negotiate. Jabotinsky's vision is not limited to building military power but also states that this power is a means to create a situation in which the Arabs accept defeat. The Iron Wall is not an end but a means to create a situation where the Arabs accept defeat.[95]

This strategy is vital in Israel's understanding of security and its relations with the Arab world. According to Jabotinsky's thinking, the fact that the Arabs will never voluntarily accept a Jewish state in Palestine necessitates the creation of an impenetrable military force to ensure Israel's security. This military force would serve as a deterrent to force the Arabs to accept Israel's existence and legitimacy. The Iron Wall doctrine has been central to Israel's military and diplomatic strategies. As envisioned by Jabotinsky, it was intended to create a strong line of defense so that the Arab world would accept Israel's existence and begin peace negotiations.[96] This strategy reflected Israel's determination to preserve its independence and security

2.4.3. Iron Wall in Israel's Security Doctrine

David Ben-Gurion, Israel's first Prime Minister, adopted the Iron Wall strategy, emphasizing that military power was vital to the existence and security of Israel. [97]Despite his public statements seeking peace, Ben-Gurion believed that only overwhelming military superiority would lead to Arab acceptance of Israel. The 1967 Six-Day War led to Israel's invasion of the Egypt's Sinai Peninsula, the West Bank, and the Golan Heights. It was seen as a validation of the Iron Wall strategy, demonstrating Israel's military superiority.[98]

Khalili argues that the Iron Wall doctrine perpetuates a cycle of violence and hinders genuine peace efforts.[99] The reliance on military power has superseded diplomatic initiatives. In his assessment of Israeli policies, Avi Shlaim noted that the Iron Wall strategy was intended to lead to negotiations ultimately. Still, successive Israeli governments have ignored mainly the stage of entering into meaningful negotiations with the Palestinians.[100]

---

[95] ibid 83.
[96] ibid; Laleh Khalili, 'The Iron Wall' [2006] Feminist Review 2, 2.
[97] Shlaim (n 97) 84.
[98] Ben Dor A and Dr Uri Milstein, 'The Iron Wall' [2023] The Iron Wall of Jabotinski 2 <https://www.academia.edu/108287725/The_Iron_Wall> accessed 11 June 2024; Shlaim (n 97) 87.
[99] Khalili (n 99) 1–2.
[100] Shlaim (n 97) 80.

2.4.4. The Iron Wall Doctrine in Contemporary Israeli Politics

The "Iron Wall" concept is still relevant in contemporary Israeli security policy, with leaders such as Benjamin Netanyahu adopting a hard-line stance in line with Iron Wall principles.[101] This approach has been criticized for increasing tensions and undermining hopes for a two-state solution.[102] In this context, the "Iron Wall" policy can be defined as a strategy of strong defense and deterrence against Israel's Arab neighbors.[103] Israel's security concerns and the instability in the region play an important role in sustaining this policy.

Israel has developed a security strategy centered around the following: A decisive numerical disadvantage, a lack of strategic depth, a climate of constant regional mobility and conflict, an unresolved and deepening Arab-Israeli conflict, and self-reliance in terms of defense[104] The basic principles of Israel's national security strategy can be listed as follows:

a. Building qualitative superiority against numerical superiority[105]

Diaspora Jews founded Israel brought together by the ideology of Zionism and suffered from numerical inferiority during its establishment. By 1948, the Jewish population in Israel was around 650,000.[106] The Arab countries were home to nearly 90 million people. Today, this figure is 6.5 million for Israel and about 400 million for the Arab states.[107] Today, the total GDP of the Arab countries neighboring Israel in the Middle East as of 2023 is 3.37 trillion dollars. In contrast, Israel's 2023 GDP is around 540 billion dollars.[108] Israel has fought wars and conflicts with many of these countries in the last 75 years, both major and minor. Therefore, Israel has pursued a determined strategy of gaining a qualitative advantage

[101] ibid 91–95; A and Milstein (n 101) 1–2.
[102] Shlaim (n 97) 95.
[103] ibid 86; A and Milstein (n 101) 2–6.
[104] Tabansky (n 32) 46.
[105] Amidror (n 74); Dan Meridor and Ron Eldadi, 'Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later' (Institute for National Security Studies 2019) Memorandum 187 <https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf> accessed 7 August 2024; Ehud Eilam, *Israel's Military Doctrine* (Lexington Books 2018).
[106] EN Luttwak and E Shamir, *The Art of Military Innovation: Lessons from the Israel Defense Forces* (Harvard University Press 2023) 57 <https://books.google.com.tr/books?id=y9agzwEACAAJ>.
[107] From Systemic Reform to Dissolution, 'Demography in the Middle East: Population Growth Slowing, Women's Situation Unresolved | The Washington Institute' <https://www.washingtoninstitute.org/policy-analysis/demography-middle-east-population-growth-slowing-womens-situation-unresolved> accessed 22 March 2024.
[108] 'World Economic Outlook (October 2023) - GDP, Current Prices' <https://www.imf.org/external/datamapper/NGDPD@WEO> accessed 22 March 2024.

to solve the problem of numerical inferiority, especially in terms of population, economic, military, and finding allies. Regarding military power, Israel had to rely on its national strength.[109] Therefore, while designing its military doctrine, it has tried to strengthen its army with advanced training tactics and state-of-the-art ammunition to counter many numerical forces. As of 2023, Israel is the leader country in R&D as a percentage of GDP.[110] As a principle of national security strategy in the post-1948 period, Israel's rapidly increasing R&D activities and continuous investments in science-technology paid off in the following years. Again, it developed a qualitative edge in cooperation with great powers such as the USA and France against the Arab countries, which supported the USSR against it and won victories in the field against Arab countries that were numerically superior.[111]

b. Early warning for compensating strategic depth[112]

Israel's small surface area, the constant struggle for liberation of the Palestinians in the territories it occupies, its relative weakness in terms of numbers, and the negative social, political, and economic impact of every soldier who dies due to the compulsory military service rule have pushed Israel to take measures in this regard.[113] Therefore, Israel had to establish intelligence superiority against possible attacks. Since every possible attack that the country faced could lead Israel to total destruction, Israel needed to gain dominance over its enemies through early warning.[114]

c. Deterrence as a tool for preventing a disastrous war:

Israel has lived with war since its inception, and both civilian and state actors have placed the threat of war as central to their existence. Having fought large-scale wars since the First Arab-Israeli War in 1948, the Israeli authorities were aware that any war situation could potentially bring total destruction to Israel. Because of its population, economy, and military power, Israel wanted to postpone and, if possible, avoid engaging in and sustaining

[109] Rodman (n 14) 79.

[110] 'Research and Development (R&D) - Gross Domestic Spending on R&D - OECD Data' (*theOECD*) <http://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm> accessed 27 June 2024.

[111] Rodman (n 14) 81–82.

[112] Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford University Press 2010) 112.

[113] Ackerman (n 86).

[114] Gadi Eisenkot, 'Deterring Terror - How Israel Confronts the Next Generation of Threats' (Belfer Center for Science and International Affairs 2016) 4 <https://www.belfercenter.org/israel-defense-forces-strategy-document> accessed 19 March 2024.

a large-scale war. This was of vital importance for a newly established state. On the one hand, Israel was in the process of settling Diaspora Jews in Israel and settling those who came to Israel in the occupied territories while at the same time needing time and material resources for infrastructure, education, industrial development, and providing jobs for the population. In such a situation, it would have been too risky to engage in an all-out war and would have disrupted the state-building efforts in Israel. Although this situation does not pose as much of a strategic threat as it used to, thanks to Israel's modernized army and economy and its agreements with the United States, avoiding war is still part of its military doctrine. Thus, Israel seeks to build deterrent capabilities against attacks on its occupied territories and its population, which would allow it to avert suburban threats. This includes maintaining superiority in military and strategy over all enemies as state or non-state actors. The principle of deterring enemies from war has been pursued through efforts to build technological and strategic superiority in the military domain.[115]

d. Building an alliance with a global superpower

On May 15, 1948, after the withdrawal of the British forces from the mandate in Palestine, the power vacuum created resulted in the birth of the State of Israel. In 1917, in the letter of the Balfour Declaration, Britain expressed its open support for the Zionist forces in Palestine, leaving two hostile peoples without state status in the territories from which it withdrew. Following the power vacuum in the region, the state of Israel declared its establishment, and the First Arab-Israeli War (the War of Independence for the Israeli people) took place and ended with an armistice. Precisely 11 minutes after the declaration of Israel's establishment, it was de facto recognized by US President Truman, making the US the first country to recognize Israel.[116]

The State of Israel, lacking strategic depth, lacking sophisticated and adequate munitions, and being very weak against the Arab states regarding demographic and economic parameters, needed a superpower to protect it. Ben Gurion expressed this as a principle: “Israel must always establish a close relationship with at least one great power.”[117]

[115] Amidror (n 74).
[116] Karaoğlu and Elhan (n 56) 201.
[117] Rodman (n 14) 81.

Addressing his commanders during this period, Prime Minister Ben Gurion commented on the power struggle in the Middle East as follows:

"If a war breaks out between the Arabs and us and the Arabs win, no one will touch them because everyone is courting them. We saw this at the last Security Council meeting. There is nothing more natural than for America and Russia together to cultivate Arab friendship, and there is no guarantee that they would impose any sanctions on them. On the other hand, there is a severe threat that even after they attack us, and we give them hell in return and don't give up until we prevail against them, [the US and the USSR] would use extreme measures against us. (Ben-Gurion, 1980, p. 215)"

Israel acquired weapons from different states throughout the 20th century. It was subjected to embargoes in different periods during the wars with Arab countries. Different states such as Czechoslovakia, the United Kingdom, France, the United States, and Czechoslovakia sold arms to Israel and it received aid from some of them. At the time of its establishment, the UN Security Council imposed an arms embargo on the Palestinian territories. This embargo aimed to prevent possible conflicts and tensions in the region. The UK and the US complied with this embargo and stopped arms shipments to the region. Israel, on the other hand, bypassed this embargo with the weapons it obtained from Czechoslovakia, thereby increasing its military capacity in the period leading up to the First Arab-Israeli War and reaching a level of resistance.[118]

In 1956, due to the Suez Crisis, Britain and France acted jointly against Egypt, and Israel acquired weapons and ammunition from these two countries during this crisis.[119] In the same crisis, the USSR supported Egypt.[120] During the Cold War, the US and the USSR tried to influence the conflicts in the region by providing arms to their allies. Especially after the Six-Day War in 1967, the USSR provided large amounts of military aid to Egypt and Syria in an effort to increase their military capacities. In response to the USSR's support, the US provided Israel with large amounts of military aid and increased its defense capacity in order to maintain the balance of power in the region.[121] During this period, Israel received

[118] Avi Kober, 'Arms Races and the Arab–Israeli Conflict' in Thomas Mahnken, Joseph Maiolo and David Stevenson (eds), *Arms Races in International Politics: From the Nineteenth to the Twenty-First Century* (Oxford University Press 2016) 209 <https://doi.org/10.1093/acprof:oso/9780198735267.003.0010> accessed 8 July 2024.

[119] ibid 209–210.

[120] ibid 210.

[121] Fahir Armaoğlu, *20. Yüzyıl Siyasi Tarihi 1914-1995* (Kronik Kitap 2019) 530–537.

modern weapons from the US, such as Skyhawk and Phantom fighter jets, heavy attack helicopters and Patton tanks.[122] This military aid helped Israel succeed in the 1973 Yom Kippur War. At the same time, it further accelerated the arms race in the region and undermined the peace process.[123]

During the arms embargo on Israel, not only France, but also Britain and the United States imposed similar restrictions. In 1969, Britain and France imposed an embargo on the supply of tanks, fighter jets and warships to Israel. Until the Six-Day War, Israel received only rhetorical and economic support from the United States, but its main ally was France.[124] Charles de Gaulle, the leader of France in 1967, decided imposing an military embargo on Israel during the Six-Day War. This decision was a reflection of changes in France's Middle East policy. Unlike previous governments, de Gaulle tended to establish closer relations with Arab countries and wanted to increase his influence in the Arab world. Therefore, restricting or halting arms sales to Israel was part of France's efforts to alter the balance in the Middle East. This decision was a significant turning point in France's relations with Israel and led to a decline in military cooperation between Israel and France.[125]

To replace the embargoed British Chieftain tank, Israel expanded its inventory by developing the powerful Merkava tank.[126] In addition, the US threatened to halt arms deliveries in order to secure a ceasefire during the Yom Kippur War and to limit the invasion of Lebanon in 1982. These embargoes led Israel to take important steps to develop its own defense industry and to decrease its dependence on American weapons in particular.[127] The Arab states also became militarily dependent on the USSR for a certain period of time, as they chose the USSR as their strategic partner against the US and Israeli forces.[128] These embargoes, which indirectly affected the Arab-Israeli wars in the Middle East, limited Israel's military power and restricted its operations. However, these embargoes also contributed to the development of Israel's defense industry and the reduction of its foreign dependence.[129] Arms purchases and subsidies, especially from the United States, supported

[122] Kober (n 121) 210.
[123] Armaoğlu (n 124) 539–546.
[124] Eytan Gilboa, 'American Contributions to Israel's National Security' (2020) 23 18, 24.
[125] 'Jews, Arabs, and French Diplomacy: A Special Report' (*Commentary Magazine*, 1 May 2005) <https://www.commentary.org/articles/pryce-jones/jews-arabs-and-french-diplomacy-a-special-report/> accessed 24 March 2024.
[126] 'Israel Has Seen Arms Embargoes Before' *The Economist* <https://www.economist.com/middle-east-and-africa/2024/05/16/israel-has-seen-arms-embargoes-before> accessed 7 August 2024.
[127] ibid.
[128] Armaoğlu (n 124) 530–537.
[129] 'Israel Has Seen Arms Embargoes Before' (n 129).

Israel's efforts to maintain military balance in the region. This process led Israel to invest in its own arms industry.

Following the Six-Day War, US-Israeli relations maintained to enhance. The allied relations of the Arab countries with the USSR and the arms trade led the US to establish an alliance with Israel as a balancing factor in the Middle East.[130]

e. US Aid to Israel

Economic, military, and political aid provided to specific regions by different powers can contribute to shaping that region and even global politics. During the establishment period of the State of Israel, the long-term struggle between the superpowers during the early stages of the Cold War had direct or indirect effects on the countries in the Middle East. The superpowers leading the two rival blocs of the time, the United States and the Soviet Union, occasionally provided geopolitical and ideologically-based aid to different countries.[131] This aid was not only economic, military, and political but also extended to other areas such as education. The aid provided by the United States to European states and peripheral countries, which were economically struggling after World War II, as well as the aid provided by the Soviet Union to its satellite states, continued later on with the aim of attracting, persuading, and gaining supporters from other countries.[132] After the First Arab-Israeli War, the states in the region received varying amounts of aid at different times. In this section of the thesis, the aid provided by the United States to the MENA (Middle East and North Africa) region will be examined, followed by a detailed analysis of the aid provided by the United States to Israel.

U.S. Aid to the Middle East and North Africa Region

[130] Yaacov Bar-Siman-Tov, 'The United States and Israel since 1948: A "Special Relationship"?' (1998) 22 Diplomatic History 231, 234.

[131] David Kinsella, 'Conflict in Context: Arms Transfers and Third World Rivalries during the Cold War' (1994) 38 American Journal of Political Science 557, 561.

[132] Armaoğlu (n 124) 525–530.

Since 1946, the United States has provided varying amounts of aid to different regions around the world. The estimated total aid to the MENA region is $372.6 billion.[133] As shown in the graph below, the U.S. provided the most aid to the MENA region in the context of foreign assistance between 1946 and 2020.

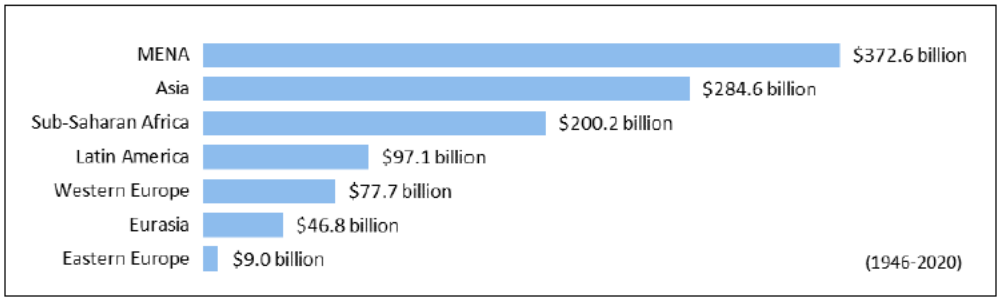

Figure 1. U.S. Foreign Aid by Region: FY1946-FY2020 (Adopted from U.S. Foreign Assitance Report)[134]

When examining the details of the aid given to this region, it is evident that Israel, Egypt, and Iraq are the top three recipients.[135]

[133] 'U.S. Foreign Assistance to the Middle East: Historical, Recent Trends, and the FY2024 Background Request' (Congressional Research Service 2023) R46344 2 <https://sgp.fas.org/crs/mideast/R46344.pdf> accessed 7 August 2024.
[134] ibid.
[135] ibid.

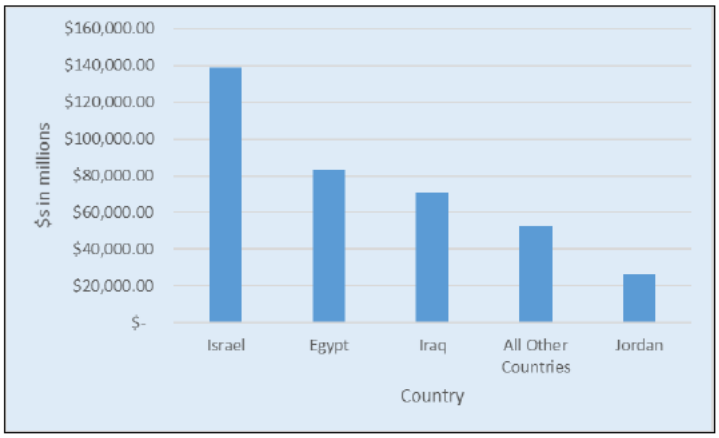

Figure 2. U.S. Foreign Aid to MENA Countries: FY 1946-FY2020 (Adopted from US Foreign Assistance Report)[136]

The majority of direct aid to Israel from the U.S. has been in the form of military assistance and missile defense funding, amounting to approximately $158 billion.[137] With the 'Memorandum of Understanding' approved by the U.S. Congress in 2016, it was pledged that Israel would receive a military aid package worth $38 billion for the fiscal years 2019-2028.[138]

Another MENA country that has benefited from this aid is Egypt. Despite being in conflict with Israel for many years in the region and at times aligning with the Soviet Union, which conflicted with U.S. geopolitical interests, U.S. aid to Egypt increased following the 1979 Egypt-Israel peace agreement.[139] Since 1946, the United States has provided Egypt with $87 billion in economic and military aid.[140] U.S. administrations have argued that these aid packages are vital for regional stability and have continued to support Egypt accordingly.

Additionally, countries such as Iraq, Jordan, Palestine, and various other MENA nations have received varying amounts of aid.[141] While the U.S. has given special consideration to aid for Israel, it is essential to consider the assistance provided to other regional states. Although there has been debate over the conditions under which these aid

[136] ibid 3.
[137] ibid 5.
[138] ibid.
[139] ibid 7–8.
[140] ibid 7.
[141] ibid 3.

packages are used, the U.S. has continued its military and economic assistance to regional countries since World War II.

Since its inception, Israel has been aware that the principle of "self-reliance" would be inadequate in certain situations, even though it has relied on its national resources for developing military personnel and ammunition.[142] Therefore, in different periods, it has taken steps to establish good relations with other great powers as patronage. The US acceptance of Israel as an ally against the Arab states supported by the USSR as a balancing factor in the Middle East is critical in terms of the economic and military development that Israel has achieved. The US aid for Israel's security is inevitable for Israel to maintain its existence and sovereignty.[143] These aids can be divided into "hard and soft elements." The soft elements in the US-Israel relationship can be listed as the common Judeo-Christian roots of the two societies, being a state founded on immigration, liberal democratic values, and the Jews in the US. The most important help in the soft elements is the public justification and justification of Israel's policies and wars by a superpower like the United States all over the world.[144] President Truman, who not only defended Jewish identity within the framework of Zionism but also took it as a cause, said the following in his speech in the opening session of the 45th National Convention of Hadassah:

"I had faith in Israel before it was established; I have faith in it now. I believe it has a glorious future before it - not just another sovereign nation, but as an embodiment of the great ideals of our civilization."[145]

The U.S. support for Israel has been shaped primarily by national security, military, and economic aid. The US aid to Israel was aimed at deterring the attacks of the Arab countries, thus trying to break the influence of the USSR in the region. A strong Israel was aimed to protect its presence in the region against the Arab countries, which the USSR constantly supported. The aid started with Hawk anti-aircraft missiles and then focused on the provision and co-production of modern weapons such as the latest generation fighter jets like the F-35 and many other military munitions. The central theme of this assistance is

[142] Cohen and Klieman (n 77) 75.
[143] Gilboa (n 127) 18–19.
[144] ibid 19.
[145] 'Remarks by the President at AIPAC Policy Conference' (*whitehouse.gov*, 4 March 2012) <https://obamawhitehouse.archives.gov/the-press-office/2012/03/04/remarks-president-aipac-policy-conference-0> accessed 23 March 2024.

"Qualitative Military Edge."[146] The QME has been the main starting point for US aid to Israel. Officially defined by a 2008 Congressional resolution, the QME is stated as follows:

"The term 'qualitative military edge' means the ability to counter and defeat any credible conventional military threat from any individual state or possible coalition of states or from non-state actors, while sustaining minimal damages and casualties, through the use of superior military means, possessed in sufficient quantity, including weapons, command, control, communication, intelligence, surveillance, and reconnaissance capabilities that in their technical characteristics are superior in capability to those of such other individual or possible coalition of states or non-state actors."".[147]

That is, to make the Israeli army well-trained and equipped with state-of-the-art weaponry against enemy states that are numerically outnumbered, armed, and militarily powerful. According to this law, the US will not sell weapons to other Middle Eastern countries that could threaten Israel. The weapons and military equipment sold to Israel must be technologically better than those sold to other Arab countries. This would increase Israel's deterrence. [148]

In the 1990s, these aid programs took on a more formalized format thanks to mutual agreements between Israel and the US. These agreements, which are renewed every ten years, have continued even under presidents such as Barack Obama, who did not want this level of support for Israel.[149] Since its inception, Israel has obtained around 300 billion dollars (adjusted for inflation) in different groups (economic, military)—Table 1 below lists the countries that received the most assistance from the US from 1946 to 2023.

[146] Patrick Scott, 'Israel's Qualitative Military Edge: U.S. Arms Transfer Policy' International Relations 7.
[147] NAVAL VESSEL TRANSFER AUTHORITY 2008 (Public Law) 3.
[148] ibid.
[149] Dennis Ross, *Doomed to Succeed: The U.S.-Israel Relationship from Truman to Obama* (First edition, Farrar, Straus and Giroux 2015) 173–174; ibid 399–400.

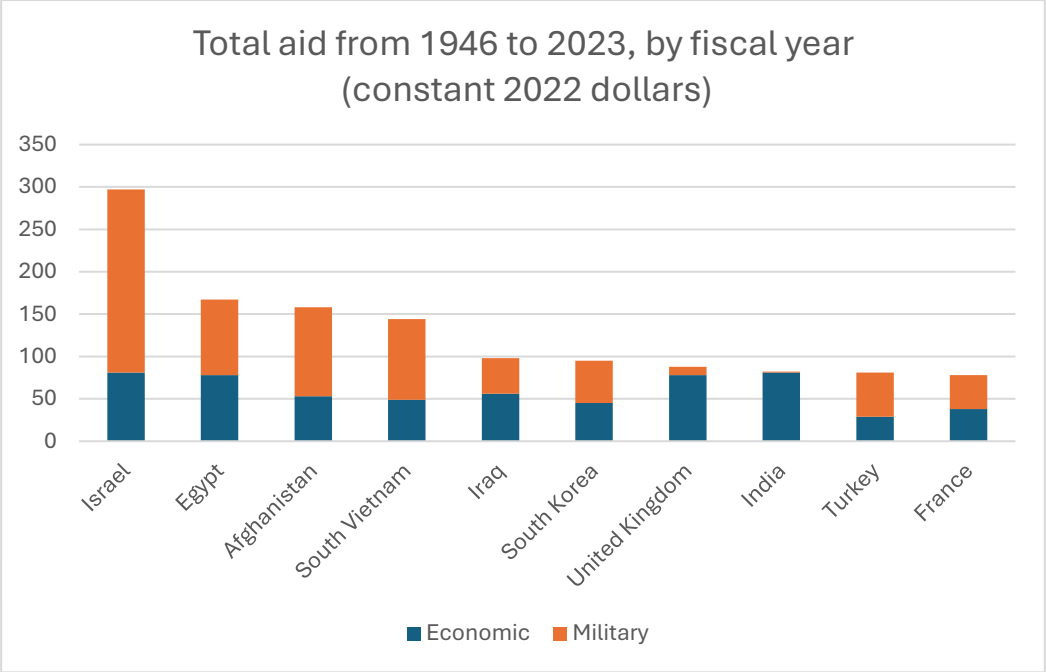

Figure 3. Total aid from 1946 to 2023, by fiscal year (USAID)[150]

Table 2 presents a graph of US military aid to Israel since 1970. As can be seen, Israel stopped receiving economic aid as of 2007 but continues to receive military aid. Through a new "memorandum of understanding," the US promises Israel $4 billion in annual aid until 2028.[151]

[150] 'U.S. Overseas Loans and Grants (Greenbook) -- Data | Development Data Library' <https://data.usaid.gov/Administration-and-Oversight/U-S-Overseas-Loans-and-Grants-Greenbook-Data/7cnw-pw8v/about_data> accessed 24 March 2024.

[151] 'U.S. Aid to Israel in Four Charts' (*Council on Foreign Relations*) <https://www.cfr.org/article/us-aid-israel-four-charts> accessed 23 March 2024.

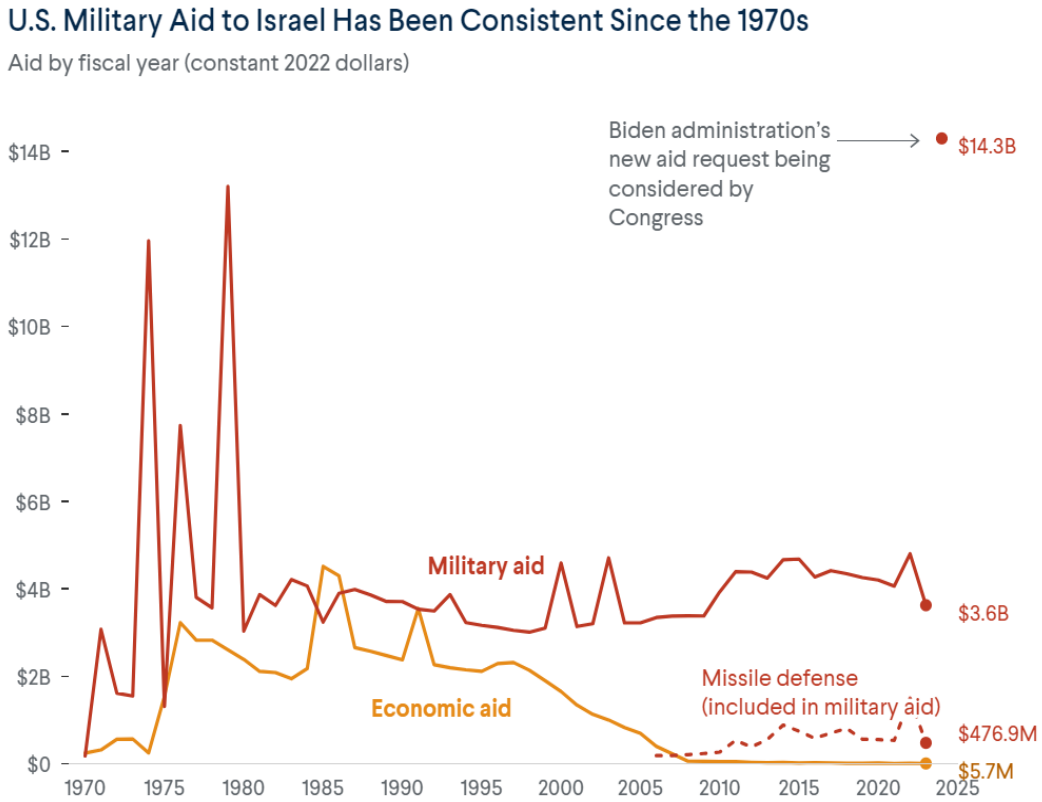

Figure 4. U.S. Aid to Israel – 1970 – 2025 (U.S. Aid to Israel in Four Charts," Council on Foreign Relations)[152]

It is also essential to look at US defense industry investments in Israel. This data sheds light on one of the factors behind Israel's establishment of a high-tech defense industry.Table 3 shows which defense industry projects the US has invested in Israel.

[152] ibid.

Characteristic	David's Sling (Short-range)	Arrow II	Arrow III (High Altitude)	Iron Dome
2006	10	122.87	-	-
2007	20.4	117.49	-	-
2008	37	98.57	20	-
2009	72.9	74.34	30	-
2010	80.09	72.31	50.04	-
2011	84.72	66.43	58.97	205
2012	110.53	58.96	66.22	70
2013*	137.5	40.8	74.7	194
2014	149.71	44.36	74.71	460.31
2015	137.93	56.2	74.71	350.97
2016	286.53	56.52	89.55	55
2017	266.51	67.33	204.89	62
2018	221.5	82.3	310	92
2019	187	163	80	70
2020	191	159	55	95
2021	177	173	77	73
2022	157	173	62	1,108

Figure 5. Defense Budget Appropriations for U.S.-Israeli Missile Defense From FY 2006 to FY 2022, (in billion U.S. dollars)[153]

As a result, since its establishment, Israel has always adopted the principle of being in a relationship with a great power. Israel, under the mandate of the United Kingdom, established an alliance with France after its establishment and developed an alliance with the United States in response to the French embargo after the Six-Day War. The U.S. characterized this alliance as a "special relationship."[154] In addition to economic and military aid, US assistance has been indispensable in national security, technology transfer, and

[153] 'U.S.-Israeli Missile Defense Budget Appropriations' (*Statista*) <https://www.statista.com/statistics/209369/defense-budget-appropriations-for-us-israeli-missile-defense-by-system-type/> accessed 24 March 2024.

[154] Steven L Spiegel, *The Other Arab-Israeli Conflict: Making America's Middle East Policy, from Truman to Reagan* (University of Chicago Press 1986) 106 <https://press.uchicago.edu/ucp/books/book/chicago/O/bo5953649.html> accessed 24 March 2024.

education. The aid budget, which has totaled 300 billion dollars to date, has been guaranteed by agreements for the future.

2.5. Development of Science and Technology in Israel

a. Impact of Culture

According to Adamsky, cultural anthropology researches shown that Israelis see their culture as decisive, flexible, and spontaneous in taking action.[155] According to Freilich, creativity in Israel is synonymous with improvisatory. He states that Israelis do not look for solutions in books and are interested in finding quick solutions in times of crisis.[156] Even if this sometimes requires a complete overhaul of the current process, Israelis maintain their stance. Historically, based on the exiles and other problems that the Israeli people have faced, it is argued that being able to organize quickly, not getting stuck on an idea, exercising personal judgment, and taking the initiative have been some of the traits that have been glorified.[157] In the IDF's military culture, army officers must be adventurous, innovative, and flexible.[158] However, these characteristics have led to a lack of intellectual heritage. The belief in solving every crisis and problem with the decisions taken at the time did not favor intellectual knowledge and problem-solving approaches. In a way, Israelis preferred to be doers rather than talkers. This is why a sophisticated and innovative defense industry was established, as the military was focused on quick, short-term solutions. [159] Behind the defense industry, which has developed much faster and more in-depth than in other fields, is the IDF's focus on quick solutions, which makes it impatient with long-term issues.[160]

b. Scientific Landscape Before the Founding of Israel

Israel's founding national security policy placed great emphasis on science. In the background of these policies is the desire to be a secular reflection of Zionist ideology, a secular reflection of being “chosen” in the real world. Theodor Herzl, one of the intellectual leaders of Zionism, believed that science and technology would play a vital role in the

[155] Adamsky, *The Culture of Military Innovation* (n 115) 132.
[156] Charles D Freilich, ‘National Security Decision-Making in Israel: Processes, Pathologies, and Strengths’ (2006) 60 Middle East Journal 635, 644.
[157] Edward N Luttwak and Daniel Horowitz, *The Israeli Army, 1948-1973*, p 87.
[158] Reuvan Gal, *A Portrait of the Israeli Soldier:* (Praeger 1986) 115.
[159] Adamsky, *The Culture of Military Innovation* (n 115) 134.
[160] ibid 140–141.

establishment of the State of Israel.[161] Believing that they are God's "Chosen Nation," Israelis need to be militarily, technically, and technologically superior to their neighbors and other enemies. For this reason, Zionist society, both before and after the founding of Israel, placed a high value on science.[162] So much so that Albert Einstein was the first name considered for the state's presidency at the founding of Israel. When Einstein rejected this offer, another scientist, chemist Chaim Weizmann, assumed this position.[163] In a society where science was so important, scientific development, technological clusters, and universities, which were the centers of scientific education, were also considered very important. Israeli politicians, especially David Ben-Gurion, also recognized the importance of science. In Israeli society, science was seen as a way out and a way of salvation. At this point, among those who immigrated to the Palestinian territories were scientists who had worked in Europe and different countries. [164]

As a newly established state with limited resources and manpower, it was limited in what it could do against the relatively more powerful Arab states that were armed and had made the region their home for thousands of years. Scientific activity provided a chance for Israeli society and the state, which were weak in quantity, to overcome this disadvantage by adding quality.[165] The so-called Qualitative Edge strategic approach was recognized as one of the indispensable pillars of Israeli national security. It was one of the critical principles of military doctrine to import advanced weapons against enemy armies, either of its production or from allied and friendly countries. Otherwise, there was no population power or strategic partner to fill the gap. The principle of qualitative edge was a combination of two elements: moral (human) and material.[166] In material terms, it was supported by the United Kingdom, France, and then the United States, which continues to this day. In the process, it synthesized material support with educated human resources and made advances in high technology and science.[167] They derived moral and cultural understanding from the philosophy of Zionism. Because of their historical problems, the Israelis could not enter into a relationship of mutual trust with any nation. Self-reliance was almost a religious principle in Israeli security. Self-sufficiency in the production of weapons and military technology became nearly an

[161] Nurit Kirsh, 'The Foundations of Israel's Ongoing Love Affair with Science' (2022) 46 Endeavour 100837, 1.
[162] ibid.
[163] ibid 2.
[164] ibid.
[165] Adamsky, *The Culture of Military Innovation* (n 115) 128.
[166] Gil Baram and Isaac Ben-Israel, 'The Academic Reserve' (2019) 34 Israel Studies Review 75, 7–8.
[167] Wunderle and Briere (n 79) 1.

obsession for Israel.[168] For Israel, being strong in technology and science was not only to increase its chances of winning wars militarily but also to tip the balance of power in its favor against its enemies. This meant gaining superiority in intelligence, deterrence, early warning, offense, and defense. At the very beginning of Israel's establishment, there was a belief that the only way to overcome the problems created by limited resources was through scientific and technological superiority. One of the reasons for this belief was that the politicians of the newly established state were composed of both military and civilian followers of World War II, which ended in 1948. The technological and scientific superiority of the United States, which changed the course of the war with its support for the European states and ended the war with two nuclear bombs dropped on Japan, increased Jewish politicians' belief in science. [169]

Science and technology were considered necessary by the first Jewish settlers in Palestine. Thinking that science and technology were the most critical factors for progress in agriculture and industry, the pioneers also realized a brain drain from their countries. Biology and chemistry were emphasized to increase agricultural production. Investments were made in physics and engineering to build essential sectors such as the defense industry. The history of today's leading Israeli universities predates Israel. When Technion University was founded, the Palestinian territories were under Ottoman rule. The Hebrew University in Jerusalem was founded in 1918. The Daniel Sieff Research Institute, which is today's Weizmann Institute of Science, was founded under the Mandate in 1934. Moreover, since the first Arab-Israeli war, the new state was in constant search for security, and this search continued in the scientific field. In this way, science and technology in Israel were mutually developed in a civil-military framework. A year before the war outbreak, David Ben-Gurion met with Professor Yochanan Ratner of Technion University. Ben-Gurion asked Professor Ratner to head the scientific work of *Hagana* (meaning Defense), which would later become the Israel Defense Forces. According to Ben-Gurion, scientists were crucial to the country's defense and should be recruited into the army. In this way, scientists could work to find the materials and devices that the *Hagana* needed or provide alternatives. During this period, *Hagana* scientists worked under constant security threats, and a year later, they served in the First Arab-Israeli War. The young scientists acquired skills not easily acquired in everyday life, such as finding quick solutions to the complex problems of war and developing practical

[168] Adamsky, *The Culture of Military Innovation* (n 115) 128.
[169] Kirsh (n 164) 11.

tools and technologies despite shortcomings. They became the pioneers of scientific endeavors in the newly established state of Israel.[170] During the war, scientists from the Sieff Institute (later the Weizmann Institute), the Hebrew University, the Technion, and Jewish scientists from the West worked under the leadership of the scientist Ernst Bergmann. The purpose of this committee was to conduct research for producing weapons, explosives, and biochemical weapons.[171] Israel's first Air Force technicians were trained at the Technion, and broken airplanes and engines were brought here for repair. The Technion was heavily guarded, as security studies were carried out there. It functioned as one of Israel's military bases. The director of the Sieff Institute, chemist Ernst David Bergmann, proudly stated that they worked non-stop during the war.[172] The words of Dr. Shlomo Kaplansky, President of the Technion, about the impact of scientific studies and efforts on the course of the war are essential**:**

"The War of Independence underscores all too well our dependence upon aviation and maritime transport. Our backs are to the sea, and transport and air defense are as essential to us as oxygen."[173]

For Kaplansky, science could create a Western state in the heart of the Middle East. The emphasis on science could dramatically boost agriculture, industry, construction, transportation, and education.[174] Kaplansky put it this way:

"Only our quality advantage up until now in science and technology can explain the miracle of the victory of the few over the many of our successfully defending our young nation of 750,000 Jews from the armies of five Arab countries whose populations total 25 million."[175]

In conclusion, the Palestinian territories were a vibrant place for scientific endeavors and technology even before the establishment of Israel. There were institutions established

[170] ibid 3.

[171] Sylvia Flowers, *The History and Development of the Weizmann Institute of Science* (University of London 1975) 42–44.

[172] Milton Orchin, Henry Fenichel and William B Jensen, *Scientist in the Service of Israel: The Life and Times of Ernst David Bergmann* (Magnes Press,Israel 2011) 136.

[173] Kirsh (n 164) 9.

[174] Derek J Penslar, *Zionism and Technocracy: The Engineering of Jewish Settlement in Palestine, 1870-1918* (Indiana University Press 1991) 116.

[175] Kirsh (n 164) 10.

during the Ottoman Empire and scientific endeavors during the British Mandate. Along with Jewish immigration, scientists from Europe and other countries studied many fields, especially agriculture. Even before Israel was founded, founding leader Ben-Gurion stated that science would transform Jewish society and recognized it as a cornerstone of the Zionist ideology. They contributed to the production of products such as weapons and explosives needed by militaries such as *Hagana*, which was established before the start of the First Arab-Israeli War. Nobel Prize-winning Jewish scientists were invited, scientific committees were established, and studies were carried out for the security of the future of Israel. These studies, which took place before the establishment of Israel, continued to increase during the war period. Science and technology remained important in post-war Israel.

2.6.Academic Reserve and its Impact on Israel's Cybersecurity Development

Israel's ascent to the forefront of global cybersecurity is a testament to its strategic initiatives and programs that foster technological innovation and expertise. Among these, the Academic Reserve (Atuda) program stands out for its pivotal role in the country's high-tech and cybersecurity development. In this section, the use of the term 'Academic Reserve' for the system originally called Atuda is based on the work of Baram and Ben-Israel.[176] This section delves into the Academic Reserve's significant contributions to Israel's cybersecurity, tracing its impact from its inception to the present and exploring its symbiotic relationship with military and academic institutions.

2.6.1. Israel's Reserve System and Swiss Reserve Forces

The Israeli Defense Forces (IDF) reserve system draws heavily from the Swiss armed forces. The structure of the IDF was shaped by military leaders, particularly Yigal Yadin, who studied the Swiss model and attempted to implement it. Yadin and Mordechai Makleff combined the Swiss model with the lessons from the Yishuv. Switzerland and Israel adopted the 'nation in arms' concept, including military service and mandatory reserve duty for demobilized soldiers. However, due to Israel's distinct security threats, the IDF maintains a

[176] Baram and Ben-Israel (n 169).

small regular army and reserve forces to ensure constant combat readiness, in contrast to the Swiss model of a militia army consisting of reserve forces and a small regular core army.[177]

Taking into account the economic constraints Israel faced compared to its neighboring countries, David Ben-Gurion proposed the concept of the "working army," which envisages the integration of military personnel into the workforce during peacetime[178]:

"Every man and woman under the age of 50 or 55 will be obligated to provide emergency defense services without disruption to their civilian life during times of peace, except for brief annual training, generally along the lines of the system practiced in Switzerland, adjusted for the special circumstances of the State of Israel."

However, as the security situation in Israel began to take a different turn, Ben-Gurion turned to the concepts of a "fighting nation" and a "people's army" that favored a small, highly trained regular force and a substantial reserve system.[179] The IDF's reserves are organized regionally, similar to the Swiss model, to ensure rapid mobilization and efficient use of resources. The system of storing reserve soldiers' equipment at home was also inspired by Swiss practice. The salary system for reservists, introduced in 1952, was modeled on the Swiss system, considering family status and civilian wages.[180] While the Swiss armed forces provided an essential model for the IDF's reserve system, the security threats posed to Israel itself required adjustments to the Swiss model. The structure of the IDF reflects a mixture of Swiss influence and the need for a solid, regular army to ensure Israel's defense preparedness.

2.6.2. Academic Reserve (Atuda) System in Israel

The Academic Reserve (Atuda) program is one of the critical elements behind Israel's success in cybersecurity. This program allows young talents to be discovered early[181]

[177] Yitzhak Greenberg, 'The Swiss Armed Forces as a Model for the IDF Reserve System—Indeed?' (2013) 18 Israel Studies 95, 109.
[178] ibid 101.
[179] ibid 108.
[180] ibid.
[181] Tabansky and Ben Israel (n 35) 19.

and enables them to specialize in high technology.[182] Upon graduation, students who continue their academic studies while receiving military training join the IDF as high-tech professionals. In this sense, Atuda serves as a bridge between the army and educational worlds. Annually, 1,000 exceptional high school graduates, making up 1% of the 100,000 conscripted yearly, are chosen to earn university degrees in areas critical to the IDF. They complete 32 months of mandatory service plus an extra three years. Nearly 25% of IDF officers possess academic degrees.[183] The program's influence extends beyond individual achievements, having shaped Israel's high-tech and cybersecurity landscape.[184] Atuda graduates have contributed to the invention of many innovative solutions and new technologies recognized nationally and internationally for their achievements in their fields of study. These innovations have consolidated Israel's global leadership in cybersecurity and increased the country's competitiveness in this field.[185] Most notable graduates include figures like Gil Shwed, founder of Check Point; Yoel Gat from Gilat; Shlomo Dovrat; Eyal Herzog, co-founder of Metacafe; Avishai Abrahami, co-founder of Wix; Retired Brig. Gen. Hanan Gefen; Retired Brig. Gen. Yair Cohen, vice president at Elron; and Retired Col. Nir Lampert, CEO of Dapei Zahav Group.[186]

2.6.3. Historical Background

The Academic Reserve program was established in the 1950s as part of Israel's vision to build a technologically advanced defense force. The program's primary purpose is to identify successful high school students from across the country and enable them to combine their military service with their academic education.[187] This Israeli program ensures that the Israel Defense Forces (IDF) benefit from highly educated and skilled personnel, especially in science and technology.[188]

2.6.4. Integration of Education and Compulsory Military Service

[182] Deganit Paikowsky and Isaac Ben Israel, 'Science and Technology for National Development: The Case of Israel's Space Program' (2009) 65 Acta Astronautica 1462, 1466.
[183] Tabansky and Ben Israel (n 35) 19.
[184] Baram and Ben-Israel (n 169) 80–85.
[185] ibid.
[186] 'The Unit' (*Forbes*) <https://www.forbes.com/2007/02/07/israel-military-unit-ventures-biz-cx_gk_0208israel.html> accessed 30 September 2024.
[187] ibid 75–77.
[188] ibid 76.

The Academic Reserve is intended to allow students to acquire advanced knowledge and skills in their chosen fields and to serve Israel's military in their specialized fields throughout the process. It has been particularly effective in cyber security, where elite units of the IDF have become incubators for technological innovation.

2.6.5. Structure and Working System of the Academic Reserve

The Academic Reserve system consists of several processes, ranging from the identification of successful students to their service in the elite units of the Israeli army. These processes can be listed as follows:

Selection Process: Successful high school students are screened based on their academic performance during high school, followed by aptitude tests and interviews conducted by IDF. Prospective students are assessed on their mathematics and physics achievements and abilities, such as group leadership skills. Every year, thousands of students apply to be part of this system. The IDF accepts 1000 students annually, but only 50 are accepted into the Talpiot program. Accepted applicants commit themselves to 9 years of intensive academic and military training, which they know will be very intense and which they can adapt to. During the selection process, the authorities evaluate not only the academic performance of these students but also their ability to combine this training with military service.[189]

Academic Education: Selected students enroll in leading universities to pursue degrees in fields related to national security and technological advancement. Students earn a dual bachelor's degree in physics and mathematics at the Hebrew University in their first three years. However, about 20 percent of students drop out early due to the program's difficulty. Typical fields of study include computer science, engineering, and cybersecurity.[190]

Military Training: Students undergo basic military training while completing their academic studies. In the first three years of their academic education, they spend their

[189] ibid 77.
[190] Paikowsky and Ben Israel (n 185) 1466.

vacation time in military training. After completing their academic education, they are commissioned as officers in the army and participate in R&D studies. [191]

2.6.6. Academic Reserve Programs

Within the Academic Reserve system, there are different training programs. These programs focus on various fields and aim to personally train well-trained military units to serve at a high level. In addition to Talpiot, Psagot, and Havatzalot, there are also programs in the social sciences.

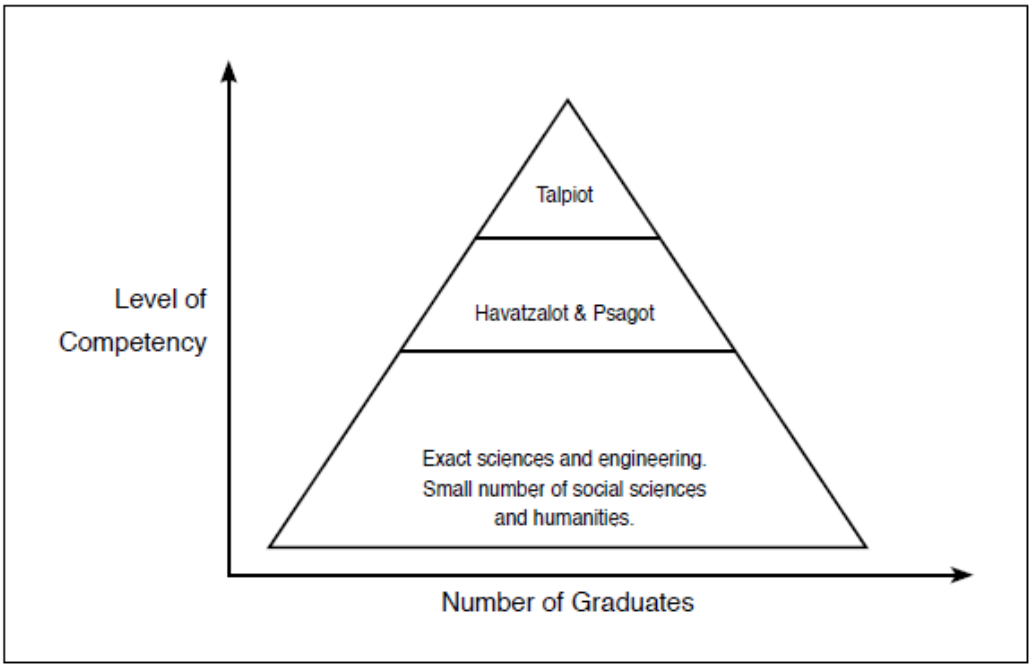

Figure 6. Academic Reserve Programs[192]

a. Talpiot Program

The Talpiot Program was initiated by the Israel Defense Forces (IDF) in 1979 and provided advanced training in engineering, mathematics, and physics.[193] The program aims to train soldiers to serve the army in the field of high technology. Participants in the Talpiot program undergo a rigorous three-year academic program designed to develop multi-

[191] ibid 1465.
[192] Baram and Ben-Israel (n 169).
[193] Jason Gewirtz, *Israel's Edge: The Story of The IDF's Most Elite Unit - Talpiot* (Independently published 2016).

disciplinary skills, followed by six years of military service. During this time, participants receive in-depth mathematics, computer science, engineering, and physics training.[194]

The Talpiot Program allows participants to develop theoretical knowledge and practical application skills. Graduates of the program play critical roles in the IDF's research and development (R&D) units and are employed by the military to develop innovative solutions.[195] Talpiot graduates have contributed significantly to cybersecurity and are among the founders of many successful cybersecurity initiatives. For example, Ben-Israel, a General in the IDF, was appointed as a cyber advisor to Prime Minister Benjamin Netanyahu. One of Ben-Israel's first acts upon taking office was establishing the Israeli National Cyber Bureau on August 7, 2011, and appointing Talpiot graduate Eviatar Matania as its head. The purpose of the INCB is to advise the prime minister and carry out tasks in this new and critical field, both offensive and defensive.[196] Mobileye, a technology company founded by Amnon Shashua, another graduate of the Talpiot programs, was acquired by Intel in 2017 for $15.3 billion.[197]

b. Havatzalot Program

The Havatzalot program is another part of Israel's Academic Reserve program and aims to develop technological support and strategic expertise for the military intelligence field. Participants earn a bachelor's degree in Middle Eastern studies or another discipline; during their academic studies, they receive military training, as in the Talpiot program. Graduates join Israel's various intelligence services and apply their educational training and army experience in this field.[198] This program is an example of Israel investing in Israel's younger generations to prepare the country for security threats effectively. The process equips participants with the ability to conduct in-depth analysis and make quick decisions to protect and advance Israel's strategic interests. Havatzalot stands out as a program that reinforces Israel's leadership in intelligence and security.

c. Psagot Program

[194] ibid 47–49.
[195] Baram and Ben-Israel (n 169) 84.
[196] Gewirtz (n 195) 66.
[197] 'Intel's $15 Billion Purchase of Mobileye Shakes up Driverless Car Sector | Reuters' <https://www.reuters.com/article/idUSKBN16K0Z4/> accessed 11 June 2024.
[198] Baram and Ben-Israel (n 169) 84–86.

The Psagot Program aims to train gifted students in physics and electronic engineering. Graduates receive a dual bachelor's degree in physics and electronics engineering. Students receive their education at Technion University. The program provides participants with advanced academic training and military training. Graduates of the Psagot Program are expected to serve in the engineering units of the IDF. Participants gain in-depth knowledge in engineering and technology during their academic studies and apply this knowledge to create solutions in their military service.[199]

The Talpiot and Psagot programs may appear to offer a similar level of education. Still, the Talpiot program is the most elite program and includes the 1 percent who participate in the Academic Reserve program. The Talpiot program offers a broader education, while the Psagot program focuses on electronic engineering and physics.

d. Social Sciences and Humanities

Although Academic Reserve programs focus on technical fields, they also accept students in the social sciences. These participants contribute to the IDF by gaining expertise in human behavior, cultural studies, and strategic thinking, essential for comprehensive security planning.[200]

2.7. Evaluation

Israel's understanding of national security has been shaped and continuously evolved in line with the challenges and threats it has faced since its establishment. Despite its small population and limited resources, Israel has achieved military and technological superiority through a “Quality versus Quantity” approach. This strategy was grounded in the leadership of Israel's founding prime minister, David Ben Gurion, and supported by the country's investments in education, conscription, and high-tech industries. Israel's national security strategy aims to be strong in economic, social, and technological fields in addition to military power. In this context, programs such as the Academic Reserve have enabled young talents

[199] ibid.
[200] ibid 84.

to be discovered early and specialize in cyber security, high technology, and engineering. These programs have been one of the critical factors behind Israel's success in cyber security.

Israel's national security strategy focuses on maintaining qualitative military superiority, compensating for its limited strategic depth through early warning systems and deterrence policies, and building alliances with global powers. The strategic partnership with the United States has played a significant role in enhancing Israel's military and economic capabilities. As a result, Israel's emphasis on technology and security has positioned it as a leader in cybersecurity and high-tech industries.

3. CYBER SECURITY

3.1. Introduction

Information has been one of history's most essential elements of power and warfare. However, there is a big difference between the importance of information and knowledge in today's society and the society of the pre-modern era. In the post-industrial revolution society, information has become one of the main elements rather than a side element. As of the late 20th century, digitalization, which started globally, has enabled the free circulation of information, thus making information security even more critical. With the spread of digital technologies, information security has become a factor that must be ensured in disciplines such as economics, politics, and international relations. The role of information in production, economy, politics, and power acquisition has affected actors who want to gain power. Information technologies have transformed knowledge into data and facilitated its circulation. This knowledge in the form of data has become the fundamental element of cybersecurity.[201]

The cyber incidents analyzed in this thesis—such as Stuxnet, Pegasus, Operation Orchard, and the Estonia Cyber Attack—have been selected based on specific criteria to ensure a systematic and impartial approach.Systematic examination of the data will enable the identification of relevant trends and patterns, thereby offering a more holistic and critical perspective. These criteria include:

Impact on National Security: Incidents that have significant implications for national security, either for Israel or other nations, have been prioritized to understand the security dynamics involved. Significance in the Context of International Law: Cases that present substantial legal considerations under international law have been chosen to explore the legal responsibilities and challenges associated with cyber operations.

Influence on Israel's Cybersecurity Strategy: Incidents that have affected or reshaped Israel's cybersecurity policies and strategies have been included to assess the evolution of its cyber defense mechanisms. These criteria ensure that the selected cases align with the

[201] Collins (n 54) 363.

objectives of the study and allow the research to be conducted in a more systematic and unbiased manner.

3.2. Cyberspace

Cyberspace is a complex digital environment where information, interaction, and transactions occur, and it has become an indispensable part of modern society. Although this concept may seem separate from the physical world, it profoundly affects the physical world through digital networks and systems. Cyberspace can be defined as a global space consisting of interdependent networks of international information technology infrastructures. According to the National Institute of Standards and Technology (NIST), cyberspace is "The global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Doyle[202] defines cyberspace as combining all communication networks, databases, and information sources to form a comprehensive, complex, and diverse electronic mass of mutual communication.

Cyber is a broad term that covers everything related to computer networks and digital technologies. It includes issues such as protection of information systems, security of digital infrastructures, and defense against cyber attacks. According to the definition by the National Institute of Standards and Technology (NIST), cyber is defined as "The complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

Cyberspace needs a definition of security in its own right. The nature of cyberspace should be understood not only as a technological construct but also as a space where states can exert power and influence.[203] It has become a critical security space where states and non-state actors engage in various forms of conflict and cooperation. Ensuring security in cyberspace is a common challenge for all nations due to the complexities arising from the

[202] DYSON (n 18) 296–297.

[203] David J Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower* (1st edition, Routledge 2011) 9–12.

global nature of this space and the interdependence of digital infrastructures.[204] Moreover, cyberspace governance involves a complex political, technological, and economic interplay. These factors shape the rules and norms of digital interactions. Thus, the governance of cyberspace has significant implications for global order.

3.3. History of Cyberspace

The history of cyberspace is closely linked to the development of computer technology and the Internet, which has gone through several important milestones. In the 1960s, the Advanced Research Projects Agency Network (ARPANET), established by the US Department of Defense, is considered the Internet's forerunner. ARPANET was developed to enable data sharing and communication between various universities and research centers.[205] 1969, the first successful message was sent from the University of California Los Angeles (UCLA) to the Stanford Research Institute (SRI). This point in time is seen as the genesis of the Internet.

In 1971, Ray Tomlinson laid the foundation of electronic mail by sending the first e-mail on ARPANET. Work on protocols and standards used in inter-computer communication accelerated during this period. In the late 1970s, the TCP/IP protocol, developed by Vint Cerf and Bob Kahn, became the basic communication protocol of the Internet. TCP/IP laid the foundation for today's Internet by enabling the secure and organized transmission of data packets.[206] In the 1980s, the Internet's infrastructure developed further, increasing the number of users. In 1983, the Domain Name System (DNS) was introduced. DNS allowed the use of more user-friendly domain names instead of IP addresses.[207] This development made the use of the Internet more accessible. Around the same time, the first computer viruses appeared. In 1986, two Pakistani brothers wrote a virus called “Brain,” which targeted MS-DOS computers. This virus is considered one of the first major threats to computer security.

[204] Will Goodman, ‘Cyber Deterrence: Tougher in Theory than in Practice?’ (2010) 4 Strategic Studies Quarterly 102, 121.

[205] Collins (n 54) 363.

[206] PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford Univ Press 2014) 30.

[207] ibid 33–34.

The 1990s saw an explosion in the use of the internet. In 1991, the World Wide Web (WWW), developed by Tim Berners-Lee, made the Internet widely available.[208] The WWW facilitated access to information through hyperlinks and made the Internet more user-friendly. In the mid-1990s, the first large-scale cyber-attacks and security breaches began to occur. In 1998, the "Morris Worm," created by Cornell University student Robert Tappan Morris, infected thousands of computers, raising severe concerns about Internet security.[209] In the early 2000s, the emergence of social media platforms radically changed the use of cyberspace. Facebook, Twitter, and other social media platforms have transformed how people communicate and share information online. During this period, cyber-attacks and cybersecurity incidents have also increased. In 2007, cyber-attacks on Estonia went down in history as one of the most significant cyber-attacks on a country. These attacks are considered the beginning of state-sponsored cyber attacks and cyber warfare.[210]

In the 2010s, cloud computing technologies revolutionized data storage and processing power. Cloud computing allows users to store and process their data over the internet. In the same period, mobile internet use increased with the widespread use of smartphones. In recent years, technologies such as the Internet of Things (IoT) and artificial intelligence have accelerated the evolution of cyberspace. IoT has enabled devices used in daily life to communicate with each other over the internet. This technology is used in many areas, from smart homes to industrial automation. Artificial intelligence has revolutionized many areas, from cyber security to data analytics. Technological developments have shaped cyberspace and have evolved continuously. This process has increased the importance of the Internet and computer technologies.

3.4. Introduction to Cyber Security

Cybersecurity has emerged as a critical area of study and practice with the widespread integration of digital technologies into every aspect of modern life. The term "cybersecurity" encompasses a broad range of activities, strategies, and measures to protect digital systems, networks, and data from unauthorized access, attacks, and damage. Despite

[208] ibid 32.

[209] Jeffrey Hunker, 'Cyber War and Cyber Power: Issues for NATO Doctrine' (NATO Defense College 2010) 6 <https://www.jstor.org/stable/resrep10354> accessed 4 June 2024.

[210] Betz and Stevens (n 205) 29.

its widespread use, the definition of cybersecurity is broad and often context-dependent, reflecting the multifaceted nature of the field.

Cyber security is the security of data/information. According to this definition, cyber security is the production, preservation, processing, dissemination, and access of information, as well as all the qualities of information in all these processes and stages, without any manipulation of its content by unauthorized persons.

Dictionary definitions often express cybersecurity simply and straightforwardly. For example, the Merriam-Webster dictionary defines cybersecurity as "the protection of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks."[211] The Oxford Dictionary defines cybersecurity as "the protection of computer systems and networks from unauthorized access or attack." [212]

NATO's definition of cybersecurity offers a broader perspective and emphasizes its importance in the context of international security. NATO defines cybersecurity as "the set of policies, strategies, and measures necessary to ensure the security of information and communication technologies." This definition reveals that cybersecurity is not only a technical issue but also has a strategic and political dimension.

Definitions from global technology companies that are essential actors in cyberspace today also emphasize different aspects of cybersecurity. For example, Cisco's official website defines cybersecurity as "the practice of protecting computer systems, networks and data from digital attacks". It highlights three main components of cybersecurity: information security, network security, and operational security.[213] IBM defines cybersecurity as "Any technology, measure or practice for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect individuals and organizations' systems, applications, computing devices, sensitive data, and financial assets against computer viruses, sophisticated and costly ransomware attacks, and more." It emphasizes the importance of cybersecurity for both individuals and businesses. IBM's definition highlights the broad

[211] 'Cybersecurity Definition & Meaning - Merriam-Webster' (n 22).
[212] Collins (n 54).
[213] 'What Is Cybersecurity? - Cisco' <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html> accessed 4 June 2024.

scope of cybersecurity and the various assets that need to be protected.[214] Microsoft's definition similarly emphasizes the broad scope of cybersecurity. Microsoft defines cybersecurity as "A set of processes, best practices, and technology solutions that help protect your critical systems and network from digital attacks. As data has increased and more people work and connect from anywhere, bad actors have responded by developing sophisticated methods for gaining access to your resources and stealing data, sabotaging your business, or extorting money. Every year, the number of attacks increases, and adversaries develop new methods of evading detection. An effective cybersecurity program includes people, processes, and technology solutions that reduce the risk of business disruption, financial loss, and reputational damage from an attack." It also points out that cybersecurity is a constantly evolving field. [215]

These definitions reveal cyber security's different components and dimensions, showing how broad and complex the field is. Cyber security is a multifaceted field not only limited to technical measures but also includes strategic, political, and organizational dimensions. The scope of cyber security, which is perceived differently by different disciplines and actors, has naturally expanded continuously, especially in the 21st century, not only in the technical dimension but also in political, economic, social, and cultural fields.[216]

In recent years, scholars have attempted to develop more comprehensive definitions to understand cybersecurity's complexity and interdisciplinary nature better. For example, Craigen, Diakun-Thibault, and Purse argue that cybersecurity is "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from de facto deviations from de jure property rights."[217] This definition emphasizes the need for a holistic approach that integrates technical, organizational, and human factors.

The evolution of the term "cybersecurity" can be traced back to early discussions of "computer security" and "information security." As Schatz, Bashroush, and Wall note, terms

[214] 'Enterprise Security Solutions | IBM' <https://www.ibm.com/security> accessed 4 June 2024.
[215] 'What Is Cybersecurity? | Microsoft Security' <https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity> accessed 4 June 2024.
[216] Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik* (2018) 107.
[217] Dan Craigen, Nadia Diakun-Thibault and Randy Purse, 'Defining Cybersecurity' 13, 13–14.

such as “Computer Security,” “IT Security,” and “Information Security” were commonly used before the term “cybersecurity” became commonplace.[218] The shift to “cybersecurity” reflects the broader scope of threats and challenges posed by the digital age and the protection of critical infrastructure, personal data, and national security. Cybersecurity is a product of the anarchic nature of cyberspace. While it can involve the struggle of many actors simultaneously, it is not the case that only one or one actor achieves absolute dominance.[219]

Morten Bay addresses the theoretical aspects of cybersecurity, arguing that it is a multifaceted phenomenon that needs to be analyzed from various angles, including critical security studies and critical theory.[220] Bay emphasizes the importance of distinguishing cybersecurity from related concepts such as information security and computer security and proposes a classification to clarify these distinctions. He notes that the term is often used to mean protection against malware and hacker attacks but that a deeper theoretical examination is necessary.

Yang Lu presents a systematic review of empirical research on cybersecurity and divides the studies into three levels: individual (non-work environment), employee (work environment), and organizational (policy/regulatory environment). Lu's review highlights the various factors that influence end-users' behavior and decision-making processes in cybersecurity and states that a comprehensive understanding of these dynamics is essential for developing effective security measures.[221] Lu argues that cybersecurity needs to be addressed not only from technical perspectives but also from behavioral and organizational perspectives.

The International Telecommunication Union (ITU) defines cybersecurity as “the collection of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organizational and user assets.”[222] This definition emphasizes the comprehensive nature of cybersecurity and covers a broad range of activities and measures to protect digital environments.

---

[218] Schatz, Bashroush and Wall (n 24) 53–54.

[219] Fulya KÖKSOY (ed), *Yeni Küresel Tehdit Siber Saldirilar: Siber Güvenlik ve Politika Uygulamalari* (Nobel Akademik Yayincilik 2020) 5.

[220] Bay (n 23) 1–3.

[221] Lu (n 26) 1–2.

[222] ‘Cybersecurity’ (*ITU*) <https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx> accessed 4 June 2024.

The interdisciplinary nature of cybersecurity is further emphasized by the need to address both its technical and human dimensions. Fredrick Chang, former Director of Research at the United States National Security Agency, explains that cybersecurity involves hostile actions, leading to the involvement of many different disciplines. Cybersecurity results from hostile interactions, and humans strive to defend machines when machines attack them. [223]

According to the US cyberspace policy document, cybersecurity policy is defined as "Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." This definition is as comprehensive as the other technical definitions but also emphasizes international relations, politics, and international cooperation.

3.5. Overview

Cybersecurity is emerging as a wide-ranging field developed to counter the complex and multifaceted threats of the digital age. It includes protecting computer systems, networks, mobile devices, electronic systems, and data. However, cybersecurity is not limited to technical measures; it also encompasses organizational, strategic, and human factors.

The definition of cybersecurity is evolving with the involvement of different disciplines. In technical terms, cyber security aims to protect computer systems and networks from malicious attacks. Sub-components such as information security, network security, and operational security play an important role in this context. Cyber security policies and strategies aim to protect the digital assets of organizations and individuals.

[223] Frederick Chang (ed), 'Building a National Program for Cybersecurity Science' (2012) 19 The Next Wave 2 <https://www.govinfo.gov/content/pkg/GPO-TNW-19-4-2012/pdf/GPO-TNW-19-4-2012.pdf> accessed 7 August 2024.

From an organizational perspective, cybersecurity is the organization of resources and measures necessary to secure organizations' processes and structures. This is not limited to technical measures but includes elements such as training employees in cyberspace, risk management in this area, and crisis management in problematic situations. In this context, cybersecurity is the attempt to help actors in cyberspace manage their presence in the digital world in a sustainable and secure manner.

From a strategic perspective, cybersecurity plays a critical role in ensuring security at the national and international levels. International organizations such as NATO and the EU define cybersecurity as a set of policies, strategies, and measures necessary to ensure the security of information and communication technologies. This approach emphasizes that cybersecurity is an area that requires international cooperation and coordination.

In terms of the human factor, cybersecurity significantly impacts user behavior and decision-making processes. Cybersecurity awareness and training of individuals and employees increase the effectiveness of measures against cyber threats. Therefore, cybersecurity strategies should consider the human factor along with technical measures.

3.6.Cyber Attacks

Cyberattacks are as difficult to explain as cybersecurity, cyber deterrence, and cyber policy, which all take place in cyberspace. Cyberattacks can be technical or social in nature, such as social engineering or fraud. Physical attacks on cyber infrastructures can also be considered cyber attacks. To understand cyber attacks, it is useful to understand the fragile structure of cyberspace. In this way, it will be easier to understand how attacks are carried out and for what purposes.

3.7. Insecurity of Computer Systems and Networks

Although many factors contribute to computer systems and networks' vulnerability to cyber-attacks, the ARPANET mentioned above was the turning point. Considered the ancestor of the internet we use today, ARPANET was the pioneer of the transition from a

static system to a dynamic and accessible system. This accessibility has become more complex over time and has created today's cyberspace. Today, it is possible to explain cyberspace with four components. These are the user, information (online), software such as programs, codes, protocols, and physical hardware such as computers, cables, servers, and satellites. [224] Three factors make today's information systems so insecure or vulnerable to interference: network technology (poorly structured security), the democratization of technology, which has made it smaller and more open, and the democratization of technology, which has resulted in the creation of comprehensive network systems.[225] In addition, the Internet has become an arena of economic activity, one of the main branches of commercial activity. This has made it insecure. Another problem with cyber systems is that they are constantly evolving and changing. Security problems arise again with the development of a system that has been updated in its latest form and whose security vulnerabilities have been closed or with the development of the attacked system. Considering that billions of individual and corporate users are also actively in cyberspace, the security problem continues in a cycle. In short, as information systems become more complex, the security problem deepens.[226]

3.8.What is a Cyber Attack

In the contemporary digital age, cyber-attacks have become a significant threat to individuals, organizations, and nations. A cyber attack is explaned as “any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to or make unauthorized use of an asset”.[227] These attacks could be advanced and are generally performed by individuals or groups with hostile intent, including hackers, criminals, and state-backed actors.[228] This section explores the nature of cyber attacks, their types, impacts, and the strategies used for prevention and mitigation, drawing on insights from various academic sources.

A cyber attack is a malicious act carried out in the cyberspace that threatens information security, confidentiality, integrity, and availability. These attacks can range from email scams to large-scale attacks with various political, economic and security goals, as

[224] KÖKSOY (n 221) 11.
[225] Collins (n 54) 363.
[226] ibid.
[227] ‘What Is a Cyberattack? | IBM’ (15 August 2021) <https://www.ibm.com/topics/cyber-attack> accessed 25 June 2024.
[228] KÖKSOY (n 221) 10–11.

achieving unauthorized access to private information, disrupting or destroying IT systems, and resulting in physical damage to industrial systems.[229] Cyber attacks can be directed against one or more IT systems, typically targeting IT security, confidentiality, integrity, and availability.[230] These attacks are carried out in an organized and/or pre-planned manner with the intent to damage computer systems. They are referred to as cyber espionage when directed by foreign intelligence services and cyber sabotage when directed against the integrity and availability of IT systems.[231]

According to Khalid Walid Mahmoud, cyberspace has become a critical battlefield where sophisticated cyber-attacks occur by states, groups, and individuals. Mahmoud emphasizes that since the 1990s, cyberspace has become a vital space for both civilian and military operations, noting the increasing use of the internet for various productive, intangible, and information services.[232]

Mahmoud states that these threats are complex to monitor and deter due to the complexity and anonymity of cyber attacks. Therefore, he argues that states need to develop comprehensive strategies and mechanisms to protect their cyber infrastructure and national security interests.[233] Taking the Israeli case in particular, he emphasizes the strategic importance of cyberspace and the necessity of strong cyber defenses. By detailing Israel's cyber capabilities and the economic and security implications of cyberattacks against the country, Mahmoud argues that cyberattacks are a new dimension of warfare and that this threat is strategically essential.[234]

3.9.Types of Cyber Attacks

Cyber attacks can be categorized into several types based on their methods and objectives. Common types include:

[229] Chandrika Nath, 'Cyber Security in the UK' 1 <https://post.parliament.uk/research-briefings/post-pn-389/> accessed 6 June 2024.

[230] Kissel (n 19) 57.

[231] 'Cyber Security Strategy for Germany' (*Federal Ministry of the Interior and Community*) 14–15 <https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-artikel.html;jsessionid=CBA5C6A6A1FE88917BAC7ED12F5703E1.live892?nn=16825398> accessed 6 June 2024.

[232] Mahmoud (n 30) 1–3.

[233] ibid 4–6.

[234] ibid 7.

Malware Attacks: Malware attacks involve malicious software such as viruses, worms, trojans, and ransomware that can damage or disable systems, steal data, or disrupt operations. Malware can be introduced through email attachments, downloads, or vulnerabilities in software. As noted by Mahmoud, malware has become a critical tool in the arsenal of cyber attackers, allowing them to infiltrate and compromise systems with relative ease. This kind of software, known as viruses, spyware, ransomware, etc., attaches itself to legitimate code and propagates autonomously. Malware can access private networks, disrupt operations, and steal sensitive information to profit from the target illicitly. Modern malware often targets business or financial data rather than personal credentials.[235] Common types of malware include:

Virus: Virus software is malicious software that replicates the systems it infiltrates within a specific program. It is known as the oldest and most dangerous malware.[236] The most essential feature of viruses is that they tend to spread. Viruses need a triggering action to spread because they cannot spread independently.[237] An example in this regard is Stuxnet, which damaged the centrifuges of the nuclear power plant in Iran.

Worms: The most important difference between computer worms and viruses is their ability to spread independently. They do not need a triggering action like viruses and can spread systematically without carrier devices (such as USB sticks). At this point, it should be emphasized that the human factor is not a factor. An example is Stuxnet, which damaged centrifuges in Iranian nuclear power plants. However, there are also opinions stating that Stuxnet is a virus.

Spyware: Spyware monitors user activity without approval and reports to the attacker.[238] This type of spyware comes ready-made in a software package. When the software installed in the spyware is installed, the spyware is integrated into the system, and personal information is collected in different ways. An example is Pegasus, a spyware installed on devices using phishing and zero-click methods. Pegasus software was developed by NSO Group, an Israel-based company, to obtain data on target audiences.

---

[235] Biju, Gopal and Prakash (n 28) 3.

[236] Samet Refik and Aslan Ömer, 'Kötü Amaçlı Yazılımlar ve Analizi' [2018] Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık 227, 228.

[237] Andhika Pratama and Fauzi Adi Rafrastara, 'Computer Worm Classification' (2012) 10 International Journal of Computer Science and Information Security 21, 21.

[238] Biju, Gopal and Prakash (n 28) 3.

Phishing Attacks: A phishing attack occurs by sending fake emails that appear to come from trusted sources, and the target person opens links redirected through this attack. The main goal of such attacks is to obtain personal information, passwords, or important secrets known to the person.[239] A phishing attack is a form of social engineering different from other attacks. It is usually designed in the form of emails or SMS containing links that install malware on computer systems. Phishing attacks use various media, messages, calls, etc., to obtain sensitive data. Spear-phishing sends social engineering messages to trick the user into performing a specific action. [240] RSA, a security firm, sent an email titled "2011 Recruitment Plan" to some of its employees containing an Excel file allowing hackers to infiltrate the system. Attackers accessed the company's system through employees who clicked on this link. [241]

Denial-of-Service (DoS) Attacks: A denial-of-service (DoS) attack is an attack method that disrupts a user's access to a computer network for malicious purposes.[242] It causes certain actors' websites or computer systems to overwork their resources, making them unresponsive to service requests. The bandwidth capacities of computer systems and networks and distributing services can simultaneously respond to a certain number of transactions.[243] Different types of DoS and DDoS attacks include TCP-SYN (Transmission Control Protocol (TCP)-Synchronize) flood attacks, teardrop attacks, smurf attacks, ping-of-death attacks, and botnets.

Table 1. Typical Cyber Attack Events From Years 2010 to Present[244]

[239] Rid and Buchanan (n 50) 15–16.
[240] ibid.
[241] ibid 16.
[242] Gil Baram, 'Israeli Defense in the Age of Cyber War' (2017) 24 Middle East Quarterly 1–2.
[243] KÖKSOY (n 221) 13.
[244] Wenli Duo, MengChu Zhou and Abdullah Abusorrah, 'A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges' (2022) 9 IEEE/CAA Journal of Automatica Sinica 784, 785.

Year	Country/Institution	Details
2010	Iran	Stuxnet attack destroying core controllers of industries
2015	Ukraine	BlackEnergy attack on power grid, leading to massive power outage
2017	Russia, Ukraine, India, China	WannaCry attack aiming to encrypt data and demand ransom payments
2020	Brno University Hospital, Czech Republic	A cyber attack that shut down IT network of a Czech hospital
2020	US Dept. Health & Human Services	Unspecified attack on servers
2021	Colonial Pipeline, US	A ransomware attack on a US fuel pipeline, leading to shutdown of a critical fuel network

Infrastructure is necessary for nearly all malevolent actions. In the case of a denial-of-service (DoS) attack, which depends on overruning the target computer with clusters of irrelevant information, the infrastructure actually performs the attack. Other activities, infrastructure is often used as a jumping-off point or to instruct code on compromised machines. To maximize the severity of attacks and reduce their cost, attackers can use the systems they disable to attack other networks.[245]

DoS attacks are very difficult to prevent because it is difficult to distinguish between normally functioning network traffic and maliciously generated traffic requests by attackers, which use the same ports and protocols. To protect systems against denial-of-service attacks, it is important to ensure that the system is equipped with Intrusion Detection Systems (IDS) and DDoS protection products. It is also necessary to have extra bandwidth available on an organization's internet connection. Having a large bandwidth for service traffic requests provides protection against low-scale DDoS attacks.[246]

Man-in-the-Middle (MitM) Attacks: A MitM attack occurs when a third party enters the communication between a client and a server. This third party impersonates both the client and the server, gaining access to information between them. This type of attack allows attacker actors to intercept and distribute data on systems. MitM attacks exploit the real-time processing of transactions, communications, or other information exchanges. [247]

[245] Rid and Buchanan (n 50) 17.
[246] Biju, Gopal and Prakash (n 28) 4849.
[247] ibid 4850.

Zero-day Attacks: A zero-day vulnerability is a software or network flaw that hackers exploit as soon as it becomes known. The term "zero" signifies the immediate exploitation window. A zero-day attack happens when this vulnerability is used by hackers, who scan for flaws, develop exploit code, infiltrate the system, and deploy malicious code. The growth of technology has increased zero-day attacks, often driven by nation-states or regions with significant cybercrime networks.[248] Zero-day vulnerabilities surged to 58 in 2021, up from 25 in 2020 and 21 in 2019, reflecting escalating risks as systems interconnect. Hackers have breached Microsoft servers and deployed spyware on smartphones, targeting journalists, politicians, and activists, highlighting the growing threat landscape.[249]

3.10. Impacts of Cyber Attacks

Cyber attacks can negatively impact the lives of many organizations and individuals. These impacts can lead to losses in the lives of actors. These losses can be economic, social and security. These harmful consequences can be expressed as physical or digital damage, reputational damage to individuals or organizations, and negative social consequences.

Physical or Digital Harm: This includes damaging or destroying digital assets, systems, and data. An example is the Stuxnet worm, which targeted Iran's nuclear facilities, causing physical damage to centrifuges used in uranium enrichment.[250]

Economic Harm: Cyber-attacks can cause significant economic damage to individuals, businesses, and economies in general. The financial consequences of these attacks are multifaceted and can manifest as direct financial losses, increased operational costs, and long-term economic impacts. One of the most critical consequences of cyber-attacks is the direct financial losses actors suffer. Cybercriminals can cause financial damage by gaining unauthorized access to bank accounts, conducting fraudulent transactions, or stealing money through ransomware.[251] For example, the 2014 attack on Sony Pictures resulted in losses of approximately $171 million, including investigations, remediation, and

[248] Splunk (n 29) 100.

[249] 'Hackers Exploited Record "Zero-Day" Flaws in 2021, Google Researchers Say - Bloomberg' <https://www.bloomberg.com/news/articles/2022-04-19/google-caught-record-number-of-zero-day-hacks-in-2021> accessed 9 June 2024.

[250] A detailed chapter on this issue will follow.

[251] Shinichi Kamiya and others, 'What Is the Impact of Successful Cyberattacks on Target Firms?' (National Bureau of Economic Research, March 2018) 2–4 <https://www.nber.org/papers/w24409> accessed 6 June 2024.

opportunity costs during and after the attack.[252] Cyberattacks can disrupt companies' operations, causing significant downtime or reduced productivity. When critical infrastructure systems are compromised, businesses may be unable to perform their core functions, resulting in delayed services, missed deadlines, and lost revenue.

Reputational Harm: Organizations can suffer long-term damage to their reputation, leading to loss of customer trust and business opportunities.[253] In late 2013, the well-known American retail chain Target suffered a large-scale incident.[254] This cybersecurity issue resulted in malware compromising Target's branch systems and exposing the personal and financial data of millions of customers to cybercriminals. As a result, Target's profits fell by 46% in the last quarter of 2013. By January 2014, the proportion of US households shopping at Target had fallen to 33%, down from 43% a year earlier. This resulted in the resignation of the longtime CEO and chief information officer in 2014, paving the way for significant management changes.[255]

Social and Societal Harm: Cyber attacks can disrupt societal functions and services, affecting large populations. The 2015 cyber attack on Ukraine's power grid, which caused widespread power outages, is a stark example of how cyber attacks can impact society at large.[256] The fear and stress caused by cyber attacks can have significant psychological effects on individuals and communities.

3.11. Cyber Diplomacy

Cyber diplomacy is the use of diplomatic efforts and strategies to address issues such as cybersecurity, cyber governance and cyber conflict prevention. It involves the negotiation and implementation of international agreements and norms and aims to ensure a stable,

---

[252] 'PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher | PCMag' <https://www.pcmag.com/archive/playstation-hack-to-cost-sony-171m-quake-costs-far-higher-264796> accessed 6 June 2024.

[253] 'The White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009. Unclassified. | National Security Archive' 19 <https://nsarchive.gwu.edu/document/21424-document-28> accessed 5 June 2024.

[254] 'Target Cyber Attack | Columbia SIPA' <https://www.sipa.columbia.edu/sipa-education/picker-center-executive-education/case-collection/target-cyber-attack> accessed 25 June 2024.

[255] Kelli Young, 'Cyber Case Study: Target Data Breach' (*CoverLink Insurance - Ohio Insurance Agency*, 13 September 2021) <https://coverlink.com/cyber-responsibility-insurance/target-data-breach/> accessed 6 June 2024.

[256] 'New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction | WIRED' <https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/> accessed 6 June 2024; L Lindstrom and M Signoretti, '12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020' (CCDCOE 2020) 202 <https://ccdcoe.org/library/publications/12th-international-conference-on-cyber-conflict-20-20-vision-the-next-decade-proceedings-2020/> accessed 6 June 2024.

secure and open digital environment.[257] Cyber diplomacy aims to influence the behavior of states in cyberspace, to hold states accountable in cyberspace, to increase cooperation of state actors in cyberspace, and to prevent conflicts. It aims to replace the cost-benefit approach of state actors when considering coercive cyber operations with a stability and peace approach.[258] As cyber threats become increasingly intertwined with geopolitical competition and instability, cyber diplomacy becomes critical to ensuring international security. It addresses the strategic, tactical and operational dimensions of cyber operations and aims to provide a framework for regulating state behavior.

The Netherlands' cyber diplomacy, for example, is shaped by long-term and short-term goals.[259] Long-term goals include promoting the development of an international normative framework to regulate cyber operations. These efforts aim to raise the political, moral and legal costs of engaging in unlawful cyber activities and to establish a form of deterrence similar to nuclear, biological and chemical arms control processes.[260] Short-term objectives include using cyber diplomacy to prevent, deter and retaliate against coercive cyber operations. The Netherlands also demands that cyber diplomacy is compatible with NATO and EU initiatives. The EU's 'Cyber Diplomacy Toolbox' is an example of a coordinated European Union cybersecurity mechanism against cyber incidents.[261]

As another case study, Russia's cyber diplomacy has been increasingly active since the late 1990s, with initiatives focused on conflict prevention and curbing the cyber arms race. It has introduced resolutions on cybersecurity at the UN General Assembly and promoted the concept of 'international information security'. Russia has signed bilateral agreements on cyber cooperation with countries such as the US, China and India. It also promotes cyber diplomacy initiatives in regional organizations such as the Shanghai Cooperation Organization (SCO) and the Collective Security Treaty Organization (CSTO).[262]

---

[257] Rutger van Marissing, 'The Role of Cyber Diplomacy in Dutch Security Policy: Long Term and Short Term Responses to Coercive Cyber Operations' (2017) 41 Atlantisch Perspectief 29, 29–32.

[258] Russell Buchan and Joe Devanny, 'South African Cyber Diplomacy and Cyber Governance' (Carnegie Endowment for International Peace 2024) <https://www.jstor.org/stable/resrep57025.7> accessed 4 June 2024.

[259] van Marissing (n 259) 30.

[260] ibid.

[261] ibid 31.

[262] Elena Chernenko and others, 'Russia's Cyber Diplomacy' (European Union Institute for Security Studies (EUISS) 2018) 45–46 <https://www.jstor.org/stable/resrep21140.8> accessed 4 June 2024.

Cyber diplomacy is a vital tool for managing and mitigating cyber threats in an increasingly digitalized world. By promoting international norms, enhancing cooperation and preventing conflict, cyber diplomacy helps ensure global stability and security. The Dutch and Russian examples illustrate different approaches and priorities in cyber diplomacy, reflecting the geopolitical contexts and strategic interests of each.

3.12. Cyber Power

Cyber power encompasses the capacity of states to gain strategic advantage through the use of disruptive cyber offensive capabilities and goes beyond cyber warfare.[263] While traditional cyber warfare involves direct and serious attacks on another nation's cyberspace and is considered a use of force, cyber power can involve the use, threat or potential use of such capabilities and includes the capacity to influence and control events without engaging in direct conflict. Cyber power is defined as "the ability to use cyberspace to create advantages and influence events across various operational environments and instruments of power".[264]

Cyberpower refers to a nation's capacity to use digital technology for surveillance, exploitation, sabotage and coercive force in international conflicts. Unlike traditional military domains such as land, sea and air, cyber power operates in the virtual environment of cyberspace, and its specific characteristics differ from kinetic power.[265]

One of the key characteristics of cyberspace is the low barriers to entry, which is due to the cheap and accessible nature of cyber capabilities relative to the cost of conventional operations. A wide pool of actors, including non-state actors, have easy access to these technologies. For example, commercially available distributed denial of service (DDoS) attack tools can be purchased for a few hundred dollars, allowing even technologically underdeveloped countries to engage in significant cyber activities. [266] This democratization of cyber tools could complicate traditional balance of power models, allowing new actors to

[263] Hunker (n 211) 4.

[264] Daniel T.Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem' in Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security* (University of Nebraska Press 2011) 38 <http://www.jstor.org/stable/10.2307/j.ctt1djmhj1> accessed 6 June 2024.

[265] Ralph Langner, 'Cyber Power: An Emerging Factor in National and International Security' [2016] Horizons: Journal of International Relations and Sustainable Development 206, 207.

[266] ibid.

emerge on the scene and eroding the power of powerful states in the cyber domain.[267] In this context, cybersecurity strategies should be considered from a broader perspective, involving not only inter-state but also non-state actors.

The strategic use of cyber power involves a variety of tactics, including espionage, sabotage and information warfare. For example, cyber espionage may involve the theft of sensitive data without disrupting targeted systems, while sabotage may aim to disrupt critical infrastructure, for example energy grids or communication networks.[268] Information warfare focuses on manipulating public opinion and spreading disinformation.[269]

States can use cyberpower in a variety of ways, whether in conjunction with kinetic military operations, covert operations without an explicit link, or as part of a broader military-diplomatic strategy. This multi-pronged approach allows nations to achieve their objectives without engaging in direct conflict. However, it is important to note that passive cyber activities such as espionage, while important, do not constitute cyber power in the traditional sense.[270] While such activities are valuable for gathering information and gaining strategic advantage, they do not represent an active and effective use of cyber power. Therefore, the full exercise of cyber power requires a comprehensive strategy that includes both active offensive capabilities and defensive capabilities.[271]

The unique nature of cyberspace significantly affects the use of cyber power by actors. Cyberspace is a dynamic and rapidly evolving environment where technological and systemic changes occur at an extraordinary pace. This volatility means that cyber weapons, once used, often lose their effectiveness because vulnerabilities are quickly patched. However, some attack methods, such as Distributed Denial of Service (DDoS) attacks, remain effective due to the lack of robust defenses against such attacks. This means that cyberspace requires constantly innovative and adaptive strategies, as the race between offensive and defensive mechanisms is the fundamental dynamic of the cybersecurity domain.[272]

---

[267] Dave Weinstein, 'Snowden and U.S. Cyber Power' [2014] Georgetown Journal of International Affairs 4, 5.
[268] Hunker (n 211) 3.
[269] Cathy Downes, "Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns," *The Cyber Defense Review* 3, no. 1 (2018): 80.
[270] Hunker (n 211) 4.
[271] ibid.
[272] ibid 4–5.

Another critical aspect of cyber power is the advantage that offensive operations create. While the attacked party has to close all potential vulnerabilities, the attackers only need to exploit a single weak point. This imbalance suggests that offensive cyber operations will maintain the upper hand for the foreseeable future.[273] Moreover, cyber operations happen very quickly and often involve multiple actors, directly or indirectly. This complexity can hide the true source of an attack, making it difficult to attribute and respond. Cybersecurity strategies must therefore be constantly innovative and flexible to balance this imbalance.[274]

Another critical feature of cyberspace is limited traceability. Anonymity makes it difficult to quickly and effectively identify the source of cyber-attacks, which hinders cyber deterrence. Anonymity allows actors to avoid responsibility and creates confusion among states about which actor to strategize against. [275]

An effective cyber power doctrine must address several challenges, such as the difficulties of technically identifying the source of an attack. Because the architecture of the Internet was designed without robust security measures, it allows attackers to easily anonymize source addresses, which increases the potential for false attribution.[276] The rapid execution of cyberattacks exacerbates this problem, leaving governments uncertain about the level of evidence required to justify a response. The effects of cyber-attacks can be highly unpredictable, with tools such as worms and viruses being widespread and causing different types of damage.[277]

The strategic use of cyber power also faces legal and diplomatic challenges. Article 2(4) of the United Nations Charter[278] prohibits the use or threat of force, which prevents cyber threats and unlawful attacks from gaining legitimacy. Deterrence in cyberspace is still an undeveloped concept as the principles of nuclear deterrence are not directly applicable. While openly declaring how many nuclear warheads and missiles there are in terms of

[273] ibid.
[274] ibid.
[275] Weinstein (n 269) 5.
[276] Collins (n 54) 363–365.
[277] Hunker (n 211) 5–6.
[278] United Nations, 'United Nations Charter (Full Text)' (*United Nations*) <https://www.un.org/en/about-us/un-charter/full-text> accessed 6 June 2024.

nuclear weapons is beneficial for nuclear deterrence, openly declaring cyber power contradicts the theory of cyber deterrence. This is because such an action may cause attackers to detect vulnerabilities. Therefore, cyber strategies should be carefully considered in the context of both legal frameworks and diplomatic relations.[279]

Although cyberpower operates under different conditions compared to traditional forms of power such as air power or naval power, it is fundamentally similar to power operations in other domains. The importance of cyber power in strategic communication and public diplomacy is increasingly emphasized. In this context, the effective use of cyberpower plays a critical role in national security strategies and international relations, with a broad day-to-day reach in both military and civilian domains.[280] In modern warfare, military cyber power plays a critical role, and an army without strong cyber capabilities is likely to be at a serious disadvantage against an enemy that possesses this technology.[281]

To overcome these challenges, there are several key areas that policymakers should focus on. First, it is necessary to ensure transparency on cyber policy issues while maintaining operational anonymity in cyberspace. This dual approach can rebuild credibility at home and abroad.[282] Taking US cybersecurity policy as an example, creative deterrence strategies should be developed to account for the offensive cyber advantage of adversaries. Establishing clear boundaries for the use of force in cyberspace and declaring the response to attacks in these areas can enhance cyber deterrence.[283]

In conclusion, this study demonstrates that cyberpower is a critical component of modern statecraft. In particular, effectively managing cyberattacks requires addressing technical, legal, and strategic challenges. As cyberspace continues to evolve, the doctrines and strategies governing the use of cyberpower must evolve as well.

[279] Hunker (n 211) 7–8.
[280] Betz and Stevens (n 205) 44.
[281] Michael Barnett and Raymond Duvall, 'Power in International Politics' (2005) 59 International Organization 39, 52–55.
[282] Weinstein (n 269) 9–10.
[283] ibid 10.

3.13. Cyber Deterrence

3.13.1. Deterrence

Deterrence is critical in strategies of countrires, essential for maintaining stability and preventing conflict. The Department of Defense Joint Publication 3-0 defines it as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits".[284] On the other hand, Frank Zagare views deterrence as a strategy where states, assumed to be rational actors, make decisions based on cost-benefit analyses to avoid actions that would result in unacceptable consequences.[285] Joseph Nye adds another perspective by defining deterrence as "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit".[286] Nye's definition focuses on the psychological aspect, altering an adversary's perception to prevent undesirable actions.

According to Chen, effective deterrence relies on three critical factors: capability, credibility, and communication.[287] Capability refers to the ability to inflict significant damage, making the cost of an attack prohibitive. Credibility is established through the demonstrable willingness to use such capabilities, and communication ensures these capabilities and resolve are clearly conveyed to potential adversaries.[288]

Deterrence can be divided into two primary strategies: deterrence by denial and deterrence by punishment.[289] Deterrence by denial makes it so difficult for an adversary to achieve their objectives that they are dissuaded from even attempting an attack. This involves robust defenses and resilience measures for rapid recovery from breaches.[290] Deterrence by

[284] United States Government US Army, *Joint Publication JP 3-0 Joint Operations 11 August 2011* (CreateSpace Independent Publishing Platform 2012) GL-9.

[285] Frank C Zagare, 'Reconciling Rationality with Deterrence: A Re-Examination of the Logical Foundations of Deterrence Theory' (2004) 16 Journal of Theoretical Politics 107, 109.

[286] Joseph S Nye Jr, 'Deterrence and Dissuasion in Cyberspace' (2017) 41 International Security 44, 45.

[287] Jim Chen, 'Cyber Deterrence by Engagement and Surprise' (2017) 7 PRISM 100, 101.

[288] ibid.

[289] Erica D Borghard and Shawn W Lonergan, 'Deterrence by Denial in Cyberspace' (2023) 46 Journal of Strategic Studies 534, 11.

[290] ibid.

punishment focuses on retaliating against adversaries to impose costs that outweigh the benefits of their actions.[291]

3.13.2. Cyber Deterrence

The cyber domain presents unique challenges for deterrence. The nature of cyberspace is characterized by anonymity, asymmetry, and the potential.[292] One significant issue is attribution; identifying the perpetrator of a cyberattack can be complex, complicating timely and targeted retaliation.[293] Cyber deterrence has become a critical component of national security strategies globally, reflecting the increasing significance of cyberspace in modern conflict.[294] Unlike nuclear or conventional weapons, cyber weapons do not cause massive physical destruction but can target critical infrastructure[295] and cause substantial economic damage, as seen in the 2007 cyberattack on Estonia.[296] The 2007 Estonia cyberattacks demonstrate that cyber deterrence has become a critical component of national security strategies. Effective retaliation in cyberspace must be swift, leveraging the unique capabilities of cyber weapons to surprise and disrupt adversaries.[297] However, the limitations in scale and capacity of cyber weapons mean that cyber deterrence often requires a combination of strategies, including legal prosecution, economic sanctions, and diplomatic isolation.[298]

The success of deterrence by punishment during the Cold War has significantly influenced contemporary strategies for managing cyber threats. Public dialogue on national security policies often emphasizes retaliation, reflecting the historical reliance on punitive measures to maintain deterrence.[299] Cyber deterrence by punishment can involve various responses, such as "cyber or kinetic retaliation, legal actions, economic sanctions, and

[291] 'Hybrid CoE Paper 8: Cyber Deterrence: A Case Study on Estonia's Policies and Practice - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats' 8 <https://www.hybridcoe.fi/publications/hybrid-coe-paper-8-cyber-deterrence-a-case-study-on-estonias-policies-and-practice/> accessed 7 June 2024.

[292] Goodman (n 206) 111.

[293] Chen (n 291) 103–104.

[294] Liam Nevill and Zoe Hawkins, 'Cyber Deterrence' (Australian Strategic Policy Institute 2016) 7 <https://www.jstor.org/stable/resrep04232.6> accessed 4 June 2024.

[295] Chen (n 291) 103–104.

[296] Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia' *The New York Times* (29 May 2007) <https://www.nytimes.com/2007/05/29/technology/29estonia.html> accessed 8 June 2024.

[297] Chen (n 291) 103–104.

[298] Joe Burton, 'Cyber Deterrence: A Comprehensive Approach?' <https://ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/> accessed 7 June 2024.

[299] Nevill and Hawkins (n 298) 7.

diplomatic efforts".[300] Norms and international agreements also play a crucial role in establishing a deterrent framework by setting expectations and standards for state behavior in cyberspace. This legal framework will be held in next sections in detail.

Deterrence remains vital in the cybersecurity strategies, evolving to address the unique challenges posed by the digital domain. By combining robust defenses with credible threats of retaliation, states can effectively dissuade adversaries from engaging in cyber operations. As cyber threats continue to evolve, so too must the strategies and policies designed to counter them, ensuring that deterrence remains a cornerstone of national and international security.

3.13.3. Strategies for Effective Cyber Deterrence

Despite the challenges, several strategies can enhance the effectiveness of cyber deterrence. One approach is to bolster defensive capabilities, making it more difficult for attackers to achieve their objectives.

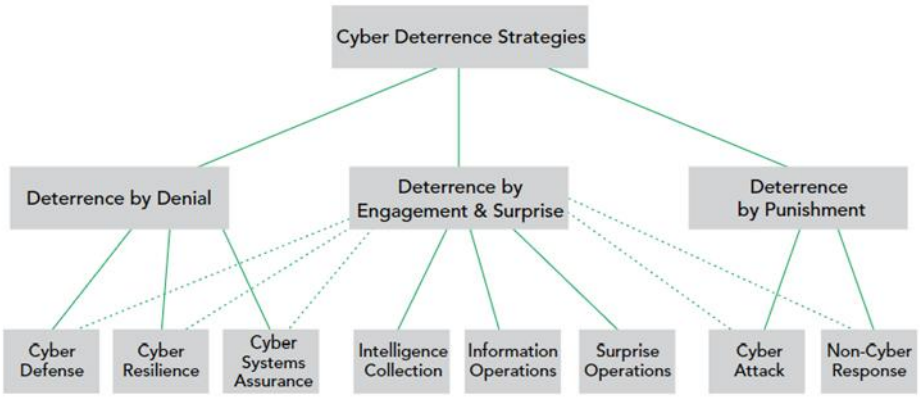

Figure 7. Deterrence by Engagement and Surprise[301]

[300] Burton (n 302).
[301] Chen (n 291).

This strategy, known as deterrence by denial, involves implementing robust cybersecurity measures to protect critical infrastructure and recover quickly from attacks .[302] The U.S. Department of Defense emphasizes the importance of securing its networks against attacks and maintaining the resilience of its systems. [303]Another strategy is to develop offensive cyber capabilities that can be used to retaliate against adversaries, thereby deterring them through the threat of punishment. For instance, the U.S. Cyber Command has highlighted the role of enhanced offensive capabilities in deterring or defeating adversaries in cyberspace.[304] However, the effectiveness of this approach depends on the ability to credibly threaten retaliation, which is often hindered by the attribution problem.

3.13.4. The Role of International Cooperation

International cooperation plays a crucial role in enhancing cyber deterrence. By working together, nations can improve their attribution capabilities, share intelligence, and coordinate responses to cyber threats. For example, NATO's efforts to develop a comprehensive cyber defense strategy and establish partnerships with key private entities can help create a more resilient and secure cyber environment.[305] Additionally, establishing norms and legal frameworks for acceptable behavior in cyberspace can provide reassurance and reduce the likelihood of conflicts. [306]

3.13.5. International Laws and Norms

The United Nations Office on Drugs and Crime (UNODC) carries out important work on combating cybercrime and capacity building in this field. UNODC provides support to member states on legal frameworks and practices related to cybercrime, thus enabling them to build the necessary infrastructure to effectively combat cybercrime. This support includes a variety of activities, such as training and technical assistance, as well as legal frameworks. UNODC's efforts aim to prevent and control cybercrime on a global scale.[307]

---

[302] Nevill and Hawkins (n 298) 8.
[303] ibid.
[304] Franklin D Kramer, Robert J Butler and Catherine Lotrionte, 'Cyber, Extended Deterrence, and NATO' (Atlantic Council 2016) 2 <https://www.jstor.org/stable/resrep03464> accessed 7 June 2024.
[305] ibid 6.
[306] Goodman (n 206) 120.
[307] 'Cybercrime' (*United Nations : UNODC ROMENA*) <https://www.unodc.org/romena/en/cybercrime.html> accessed 8 June 2024.

On the other hand, the International Telecommunication Union (ITU) promotes international cooperation on cybersecurity by setting global telecommunication and information technology standards.[308] ITU develops and supports the implementation of cybersecurity strategies through initiatives such as the Global Cybersecurity Agenda (GCA). The GCA provides a framework for cybersecurity policy-making, technical cooperation, capacity building and information sharing.

The United Nations Development Program (UNDP) carries out capacity building projects on digital development and cybersecurity.[309] UNDP helps developing countries increase their capacity for digital transformation and cybersecurity. The UN has adopted several resolutions and agreements promoting international cooperation and legal frameworks on cybersecurity and information security.

The Budapest Convention on Cybercrime, drafted by the Council of Europe and supported by the UN, is an important treaty promoting international cooperation in the fight against cybercrime. It is published in ETS No. 185 (2001)[310] and promotes international cooperation in combating crimes committed over the Internet and other computer networks.

As a conclusion, cyber deterrence is a complex and evolving field that requires a multifaceted approach. While traditional deterrence theories provide a useful foundation, they must be adapted to address the unique challenges of cyberspace. By enhancing defensive capabilities, developing credible offensive options, and fostering international cooperation, nations can better deter cyber threats and maintain stability in the digital domain.

3.14. Cyber Attacks on Estonia

3.14.1. Introduction

[308] 'ITU Cybersecurity Activities' (*ITU*) <https://www.itu.int:443/en/action/cybersecurity/Pages/default.aspx> accessed 8 June 2024.

[309] 'Ensuring Equitable Digital Futures for Everyone' (*UNDP*) <https://www.undp.org/turkiye/press-releases/ensuring-equitable-digital-futures-everyone> accessed 6 June 2024.

[310] 'Council of Europe – Convention on Cybercrime (ETS No. 185) – Translations - Treaty Office - Www.Coe.Int' (*Treaty Office*) <https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations> accessed 8 June 2024.

Estonia has a population of 1.35 million people and a GDP of close to 30 billion US Dollars.[311] Located in the east of Europe and bordering Russia, Estonia is one of the smallest countries in Europe in terms of population and economic power, as well as area. Estonia, which is advanced in the use of network technologies, has established good relations with the Western bloc after gaining its independence as part of the Soviet Union and became a member of the NATO pact with the NATO enlargement in 2004.[312] In 1991, Estonia, which was not in a very good position in terms of technological infrastructure, closed these gaps over time and made gains in the context of digital technology. So much so that Estonia provided its citizens with the possibility of electronic voting in 2005, a date that could be considered early for other countries. According to the data, 60 percent of the Estonian people are active users of the internet, while 96 percent of the banking transactions have taken place over the internet.[313] While Estonia has such a presence in cyberspace, as a result of the attacks in 2007, it was revealed that it was not at an advanced level in terms of cyber security.

3.14.2. Background of the Incident

In April 2007, Estonia was the target of a series of unprecedented cyber-attacks that made history as one of the first incidents in which a nation-state was the target of coordinated, large-scale cyber-warfare. These attacks took place after the government of Estonia decided to move a Soviet-era war memorial (Bronze Soldier Monument).[314] These events exposed the vulnerabilities of digitized societies and clearly demonstrated the potential for cyber operations to be used as tools of political repression. Estonia, a Baltic country known for its advanced digital infrastructure and e-government[315] applications, faced significant unrest in April 2007 after the government's decision to move the Soviet World War II monument “The Bronze Soldier” from the center of Tallinn to a military cemetery. The decision sparked riots among the Russian-speaking minority and triggered a series of cyber attacks targeting Estonia's critical infrastructure.[316] The relocation of the

[311] “World Bank Open Data - Estonia,” World Bank Open Data, accessed June 8, 2024, https://data.worldbank.org.

[312] dhojnacki, “NATO Enlargement at Twenty-Five: How We Got There and What It Achieved,” *Atlantic Council* (blog), March 6, 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-enlargement-at-twenty-five/.

[313] “Digital 2023: Estonia - DataReportal - Global Digital Insights,” accessed June 8, 2024, https://datareportal.com/reports/digital-2023-estonia.

[314] Vincent Joubert, “Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?” (NATO Defense College, 2012), 1, https://www.jstor.org/stable/resrep10366.

[315] “E-Estonia - We Have Built a Digital Society & We Can Show You How,” accessed June 8, 2024, https://e-estonia.com/.

[316] Stephen Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,” *Journal of Strategic Security* 4 (June 9, 2011): 50-51, https://doi.org/10.5038/1944-0472.4.2.3.

Bronze Soldier was seen by the Russian-speaking community as an attack on their historical narrative and cultural identity.[317][318] The controversy around the relocation of the monument provided a pretext for the cyberattacks, which were perceived as political retaliation. Geopolitical tensions between Estonia and Russia exacerbated the situation and highlighted the complex relationship between national identity, historical memory and cyber warfare.[319]

3.14.3. Method of Attacks

The cyber attacks against Estonia were multi-pronged, involving a variety of methods such as Distributed Denial of Service (DDoS) attacks, website defacement, email spamming and targeted attacks on critical infrastructure. These attacks overwhelmed servers with traffic, altered website content to display political messages, disrupted communication channels and targeted Domain Name Servers (DNS), international routers and major telecommunications providers.[320] DDoS attacks were the main method used, overwhelming websites and servers with large amounts of traffic, causing them to crash. The main targets included government websites, media organizations and financial institutions.[321] The attackers used botnets - networks of compromised computers - to generate the high volume of traffic needed to disable the targeted servers.[322] DDoS attacks were the main method used, overwhelming websites and servers with large amounts of traffic, causing them to crash. The main targets included government websites, media organizations and financial institutions.

The attackers utilized botnets—networks of compromised computers—to generate the high volume of traffic needed to disable the targeted servers. [323] DDoS attacks were the primary method employed, overwhelming websites and servers with large amounts of traffic and causing them to crash. More sophisticated attacks targeted critical infrastructure components, such as DNS servers and international routers, and aimed to disrupt the core operations of Estonia's digital ecosystem.[324] The main targets included government websites,

[317] Herzog, 51.

[318] "BBCTurkish.Com | News | Cyber Attack on Estonia," accessed June 8, 2024, https://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml.

[319] Piret Pernik et al., "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine," HACKS, LEAKS AND DISRUPTIONS: (European Union Institute for Security Studies (EUISS), 2018), https://www.jstor.org/stable/resrep21140.9; Joubert, "Five Years after Estonia's Cyber Attacks."

[320] Pernik et al., "The Early Days of Cyberattacks," 55-56.

[321] Hunker, "Cyber War and Cyber Power," 52.

[322] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," January 29, 2008, 7.

[323] Wilson, 7.

[324] Pernik et al., "The Early Days of Cyberattacks," 56.

media organizations, and financial institutions. These botnets were under the control of the attackers, allowing them to execute large-scale operations without the users' knowledge.

The attackers used botnets, i.e. compromised computer networks, to generate the high volume of traffic needed to disable the targeted servers.[325] These targeted attacks demonstrated a high level of coordination and technical expertise, suggesting the involvement of skilled cyber operators.

3.14.4. Impact and Consequences of Attacks

The cyber-attacks had significant but varied impacts across different sectors of Estonian society. Government websites, including ministries and political parties, were taken offline, hampering communication and service delivery. These attacks severely hampered the authorities' ability to communicate with the public and respond to the crisis.[326] In the financial sector, online banking services were disrupted, leading to major inconveniences and financial losses.[327] The financial damage caused by the cyber-attack was estimated at around six and a half million Estonian crowns (approximately €415,000), including remedial measures taken in the public sector. Hansapank's cybersecurity expert stated that the costs faced by Estonia's largest bank at the time could range from ten million to one billion Estonian crowns (approximately €640,000 to €6.5 million).[328] This highlights how vulnerable financial institutions are to cyber threats. The media sector also suffered its share of attacks, with news portals targeted and information dissemination severely affected. The disruption of media outlets halted the flow of information and caused public confusion and uncertainty.[329] . According to Pernik, the attacks also had a major impact on public perception; they created a sense of vulnerability in society and brought the importance of cybersecurity back into the spotlight. Widespread outages and the authorities' inability to immediately counter the attacks led to a decline in public trust in digital services.

---

[325] Wilson, 7.
[326] Herzog, "Revisiting the Estonian Cyber Attacks," 52.
[327] Pernik et al., "The Early Days of Cyberattacks," 55-57.
[328] "TÄISMAHUS: Jaan Priisalu: küberrünnakutest sai Hansapank kahju kuni miljard krooni," Eesti Päevaleht, accessed June 8, 2024, https://epl.delfi.ee/artikkel/64309855/taismahus-jaan-priisalu-kuberrunnakutest-sai-hansapank-kahju-kuni-miljard-krooni.
[329] Pernik et al., "The Early Days of Cyberattacks," 56; "Web War I: The Cyberattack That Changed the World," accessed June 8, 2024, https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/.

While direct attribution to the Russian government has not been conclusively proven, the attacks were believed to have been organized by Russian nationalist groups and possibly carried out with the implicit support of the Russian state. The government of Estonia responded by increasing cybersecurity measures and calling for stronger international cooperation on cyber defense, with the support of international allies such as NATO and the European Union.[330]

The attacks led to a reassessment of cyber defense strategies within NATO and the European Union, resulting in increased cooperation and the establishment of new cybersecurity initiatives. Estonia's experience highlighted the need for a coordinated international response to cyber threats.[331] However, it was also observed that NATO's response capacity was insufficient during the attacks and could not take adequate measures quickly. This highlighted the need to improve NATO's cyber defense capabilities. [332] The establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn resulted from the attacks and aimed at improving the Alliance's cyber defense capabilities.[333] It conducts training, research, and cooperation activities to enable NATO to be better prepared and more effective in responding to cyber threats.[334]

These attacks, which are claimed to be carried out by Russia, have led to groundbreaking changes in the field of cybersecurity. In this context, Ali Burak Darıcılı draws the following conclusions from the attacks: [335] :

These were the first large-scale cyber attacks attributed to Russia and targeting the neighboring country. Russia has not refrained from using cyberattacks as a means of political retribution. Subsequent cyberattacks on Georgia and Lithuania (2008), Kyrgyzstan (2009), Ukraine (2014-2022), and Turkey (2015) have been claimed to have been carried out by Russia. [336] The DDoS attack method appeared in many incidents afterward and has started

[330] Ali Burak Daricili Darıcılı, "Estonia's Cybersecurity Policy," in *Yeni Küresel Tehdit Siber Saldirilar: Siber Güvenlik ve Politika Uygulamalari*, by Ali Burak Daricili Adem Yilmaz (Nobel Akademik Yayincilik, 2020), 190.

[331] Joubert, "Five Years after Estonia's Cyber Attacks," 2.

[332] Ali Burak Daricili Darıcılı, "ANALYSIS OF NATO'S CYBER SECURITY STRATEGY," 413-15, accessed June 8, 2024, https://www.researchgate.net/publication/323689206_NATO'NUN_SIBER_GUVENLIK_STRATEJISI'NIN_ANALIZI.

[333] Pernik et al., "The Early Days of Cyberattacks," 54-55; Darıcılı, "Estonia's Cyber Security Policy," 191.

[334] "About Us," accessed June 8, 2024, https://ccdcoe.org/about-us/.

[335] Darıcılı, "Estonia's Cyber Security Policy," 191.

[336] "ANALYSIS OF CYBER ATTACKS ALLEGEDLY SOURCED FROM THE RUSSIAN FEDERATION," 1-2, accessed June 8, 2024,

to be used implicitly by other countries as a cyber warfare tool. The attack on Estonia served as a warning to other countries, which recognized the need to take measures in cybersecurity and began to invest in the necessary infrastructure, training, and military investments. The "Patriotic Hacker" has emerged as a new actor. Individuals and groups that attack other countries out of a sense of patriotic defense, independent of state control, have emerged. This has made it difficult to identify the power behind cyber-attacks.

It has become clear that increased investment in the Internet and digital technologies will also create vulnerability. States need to take security measures simultaneously with the systems created.

Furthermore, the "Tallinn Manual on the International Law Applicable to Cyber Warfare" was developed following these attacks. The Tallinn Manual is a comprehensive guide explaining how to apply international law to cyber warfare and cyber operations. This work is recognized as an essential step towards defining the legal framework for cyber conflicts and contributes to the international community's better preparedness against cyber threats. [337]

3.15. Stuxnet Attacks on Iran

Stuxnet is a sophisticated and unprecedented piece of malware that has significantly impacted cybersecurity and international relations. It was first discovered in June 2010 by a Belarusian antivirus company, VirusBlokAda, after a client reported that their machines were rebooting repeatedly. This led to the identification of a highly sophisticated worm, unlike any other malware. Kushner defines Stuxnet as: " This worm was an unprecedentedly masterful and malicious piece of code…"[338]

https://www.researchgate.net/publication/325674833_RUSYA_FEDERASYONU_KAYNAKLI_OLDUGU_IDDIA_EDILEN_SIBER_SALDIRILARIN_ANALIZI.

[337] "The Tallinn Manual," accessed June 8, 2024, https://ccdcoe.org/research/tallinn-manual/.

[338] 'The Real Story of Stuxnet - IEEE Spectrum' <https://spectrum.ieee.org/the-real-story-of-stuxnet> accessed 9 June 2024.

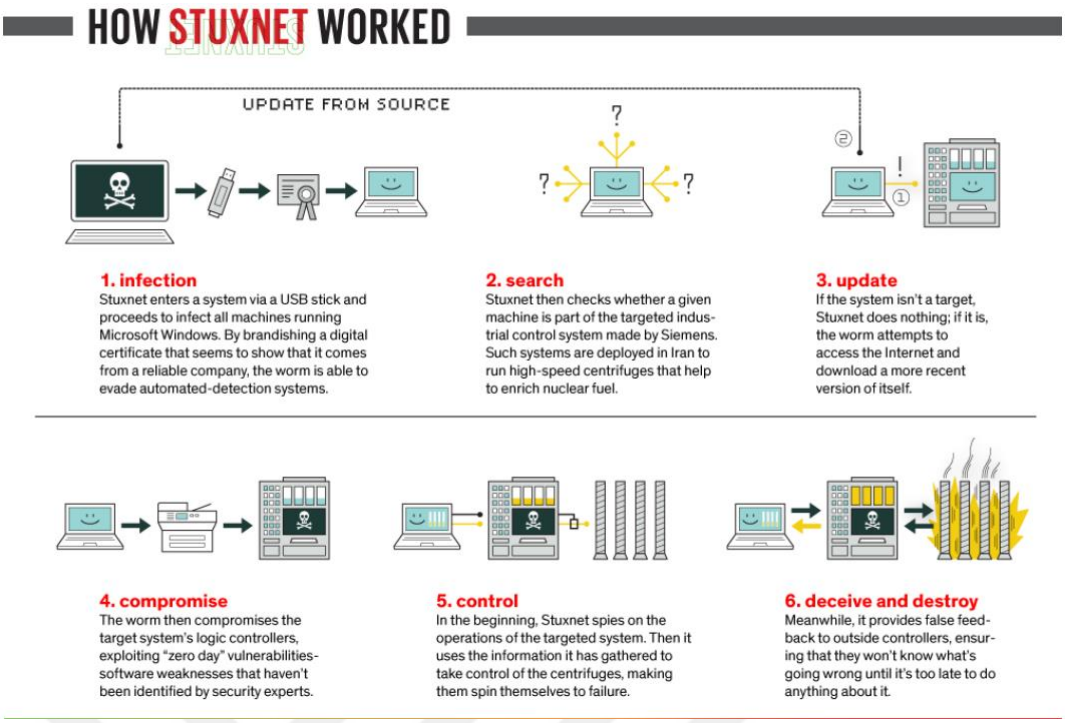

Figure 8. How Stuxnet Worked[339]

3.15.1. Technical Composition and Spread

Stuxnet is notable for its complexity and the use of multiple zero-day exploits-vulnerabilities previously unknown and unpatched.[340] A zero-day is a security vulnerability unknown to the software vendor, with no available patch. Such vulnerabilities can be exploited by attackers immediately upon discovery.

[339] ibid.
[340] ibid.

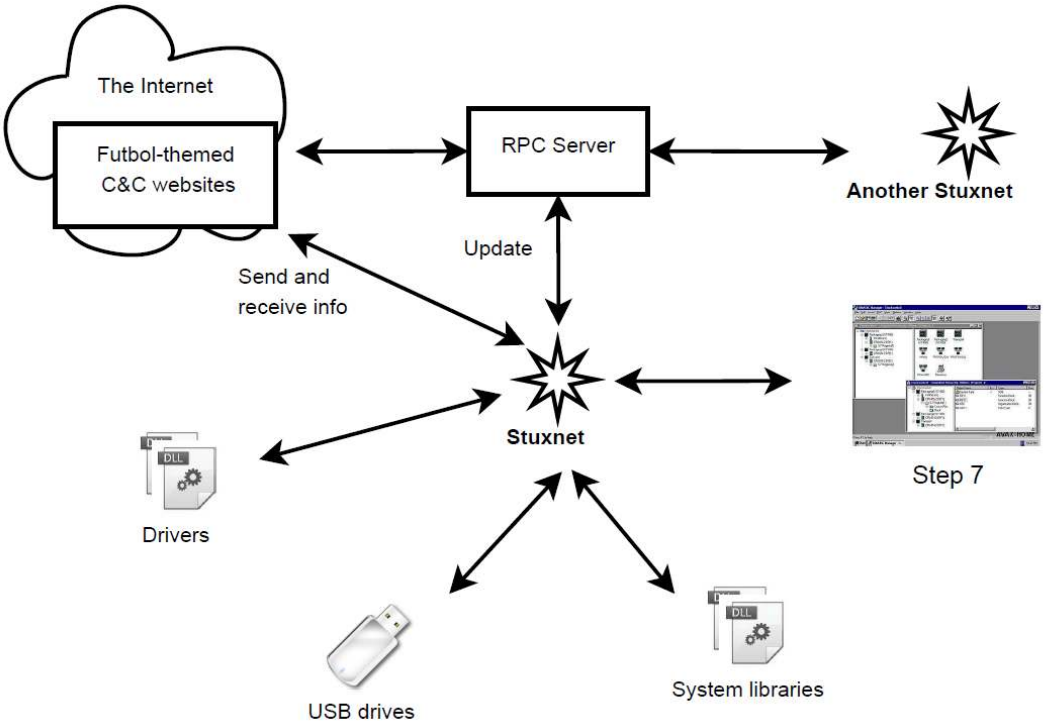

Figure 9. Stuxnet's Various Components[341]

It utilized four zero-day vulnerabilities to spread and execute its payload, unprecedented in the history of malware.[342] The worm (or virus) spreads through several vectors:

USB Flash Drives[343] : Stuxnet could propagate via infected USB drives, exploiting the LNK vulnerability (CVE-2010-2568) to execute its code when the drive was viewed in Windows Explorer.

Network Shares and Print Spooler Vulnerability[344] : It could spread over local networks by exploiting the MS10-061 print spooler vulnerability and using shared folders.

[341] ibid.
[342] Jon R Lindsay, 'Stuxnet and the Limits of Cyber Warfare' (2013) 22 Security Studies 365, 383.
[343] Marie Baezner and Patrice Robin, *Stuxnet* (2018) 4.
[344] P Mueller, 'The Stuxnet Worm' (2012) 5 <https://www.semanticscholar.org/paper/The-Stuxnet-Worm-Mueller/1501b8b7da65c8fc15846bd67765db735b23cda8> accessed 9 June 2024.

Siemens WinCC and Step7 Software[345] : Stuxnet specifically targeted Siemens WinCC software, which is used to control industrial processes. It used hardcoded passwords to access the system and upload itself. Its difference from other worms is shown in a table:

Table 2. Differences between Stuxnet and other malicious software (Adapted from Collins and McCombie)[346]

Stuxnet's Characteristics		
Aspect	**Common Malware**	**Stuxnet**
Targeting	Indiscriminate	Extremely Selective
Type of Target	Computers	Industrial control systems
Size	Less than 1 Mbyte	500 Kbytes
Probable initial infection vector	Internet and other networks	Removable Flash Drive and other ways
Exploits	Possibly one zero-day	Four zero-days

3.15.2. Target and Operation

Stuxnet was designed to target Siemens SCADA (Supervisory Control and Data Acquisition) systems , particularly those controlling the centrifuges at Iran's Natanz uranium enrichment facility. The worm was highly selective, infecting only systems that matched specific criteria related to the centrifuges' configuration. [347]

[345] ibid; Nicolas Falliere, Liam O. Murchu and Eric Chien, 'Nicolas Falliere, Liam O. Murchu, and Eric Chien, Symantec, W 32. Stuxnet Dossier, Version 1.4, February 2011. Not Classified.' (2011) 33 <https://nsarchive.gwu.edu/document/21440-document-44> accessed 7 August 2024.

[346] Sean Collins and Stephen McCombie, 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications' (2012) 7 Journal of Policing, Intelligence and Counter Terrorism 80.

[347] ibid 85.

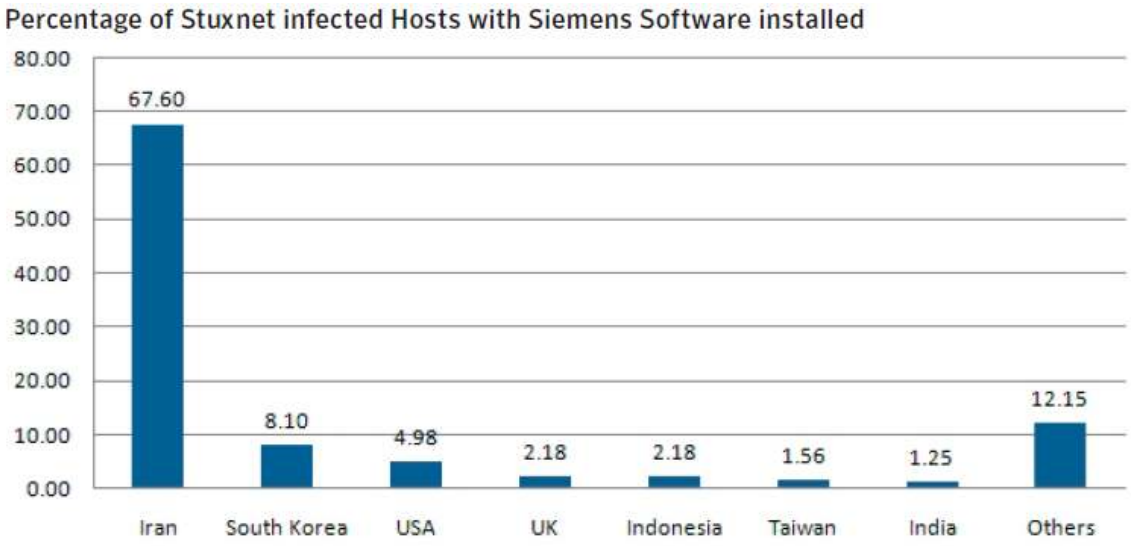

Figure 10. Percentage of Stuxnet infected Hosts with Siemens Software Installed[348]

Once inside the system, Stuxnet modified the PLCs (Programmable Logic Controllers) to alter the speed of the centrifuges, causing them to spin at speeds that would damage or destroy them.[349] This was done while sending average operating values to the monitoring systems, thus preventing detection by the plant operators. The immediate effect of Stuxnet was the physical destruction of about 1,000 centrifuges[350] (according to Albright[351] , the total number of destroyed centrifuges was 984) at the Natanz facility, which was approximately 10% of Iran's installed centrifuges at the time. This significantly delayed Iran's nuclear enrichment program and caused considerable economic and technical setbacks.[352]

[348] Liam O. Murchu and Eric Chien (n 348) 6.

[349] Jānis Jansons, 'Was Stuxnet an Act of War?' (2017) 1 Security Forum 109, 115; 'Was Stuxnet Built to Attack Iran's Nuclear Program? | InfoWorld' <https://www.infoworld.com/article/2626198/was-stuxnet-built-to-attack-iran-s-nuclear-program-.html> accessed 9 June 2024.

[350] Baezner and Robin (n 346) 9; Mueller (n 347) 10; David P Fidler, 'Was Stuxnet an Act of War? Decoding a Cyberattack' (2011) 9 IEEE Security & Privacy 56, 56.

[351] Robert Avag, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security' <https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant> accessed 9 June 2024.

[352] 'The Real Story of Stuxnet - IEEE Spectrum' (n 341); Baezner and Robin (n 346) 8.

Table 3. Stuxnet Technical Process Timeline (Adopted from W32.Stuxnet Dossier Report)[353]

Stuxnet Technical Process Timeline	
Date	**Event**
November 20, 2008	Trojan.Zlob variant exploited the LNK vulnerability, later identified in Stuxnet.
April, 2009	Hakin9 magazine reveals a remote code execution vulnerability in the Printer Spooler service, later identified as **MS10-061**.
June, 2009	The earliest Stuxnet sample observed does not **exploit MS10-046** and lacks signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate from Realtek Semiconductor Corp.
March, 2010	First Stuxnet variant to exploit **MS10-046**.
June 17, 2010	Virusblokada (a Belarus-based security software company) reports W32.Stuxnet (RootkitTmphider) using a vulnerability in shortcut/.lnk file processing to propagate, later identified as **MS10-046**.
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory **2286198** for a Windows Shell vulnerability in shortcut/.lnk file processing. Verisign revokes Realtek Semiconductor Corp's certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, now signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens reports investigating malware infections in WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues **MS10-046**, which patches the Windows Shell shortcut vulnerability.

[353] Liam O. Murchu and Eric Chien (n 348).

August 6, 2010	Symantec reports that Stuxnet can inject and hide code on a PLC, affecting industrial control systems.
September 14, 2010	Microsoft releases **MS10-061** to patch the Printer Spooler vulnerability identified by Symantec in August and reports two other privilege escalation vulnerabilities identified by Symantec.
September 30, 2010	Symantec presents at Virus Bulletin and releases a comprehensive analysis of Stuxnet.

3.15.3. Attribution and Implications

Stuxnet's attribution and its broader implications are complex and multifaceted, reflecting the intersection of cybersecurity, geopolitics, and international relations. The complexity and sophistication of Stuxnet indicated that it was beyond the capabilities of typical cybercriminals or hacktivists.[354] It required extensive resources, including financial backing, technical expertise, and detailed knowledge of the target systems. Experts estimated that developing Stuxnet would have required a team of 5 to 10 programmers working full-time for at least six months. [355]

Stuxnet utilized four zero-day vulnerabilities, which are extremely rare and valuable. The developers' use of multiple zero-days suggests that they had access to significant resources and intelligence capabilities. [356] The worm used stolen digital certificates from RealTek and JMicron, which allowed it to appear as legitimate software and avoid detection.[357] It was very advanced work for a cybercriminal group or hacktivists.

3.15.4. Geopolitical Background of the Stuxnet Attack

a. Operation Olympic Games

[354] Lindsay (n 345) 366.
[355] Thomas M Chen and Saeed Abu-Nimeh, 'Lessons from Stuxnet' (2011) 44 Computer 91, 92.
[356] ibid.
[357] Mueller (n 347) 8.

David E. Sanger from The New York Times discussed a secretive U.S. cyber-operation called Operation Olympic Games, which targeted Iranian nuclear facilities. Stuxnet, a significant malware, was part of this initiative. The operation began around 2006 during the Bush administration and was expanded under President Obama.[358] This operation aimed to delay or disrupt Iran's nuclear program without resorting to military action. [359]

b. Israel's Role and Impact on Iran's Nuclear Program

Preventing Iran From Getting Nuclear Weapons: Israel has consistently viewed a nuclear-armed Iran as a significant existential threat. The development and deployment of Stuxnet were aligned with Israel's strategic objective of delaying or disrupting Iran's nuclear capabilities without resorting to direct military action. The immediate impact of Stuxnet was the destruction of approximately 1,000 IR-1 centrifuges, significantly setting back Iran's uranium enrichment efforts by about a year. [360]

Stuxnet specifically targeted Iran's nuclear enrichment facilities at Natanz. The geopolitical context of the time involved significant international tension over Iran's nuclear ambitions. The United States and Israel were particularly concerned about Iran developing nuclear weapons capabilities. Mueller says:

"Israel and the U.S. are the leading suspects as Stuxnet's creators. Neither are friends of Iran's current leadership (to put it mildly), and both, especially Israel, fear a nuclear-armed Iran."[361]

The US and Israel have long viewed Iran's nuclear program as a threat to regional and global security.[362] The US-based Institute for Science and International Security (ISIS) confirmed that Stuxnet was programmed to target the Natanz centrifuges. This incident

---

[358] 'Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon' (*Cybersecurity & Digital Trust*, 6 February 2021) <https://icdt.osu.edu/countdown-zero-day-stuxnet-and-launch-worlds-first-digital-weapon> accessed 9 June 2024.

[359] Marco De Falco, 'Stuxnet Facts Report. A Technical and Strategic Analysis' 40–54 <https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/> accessed 9 June 2024.

[360] David Albright and others, 'Preventing Iran From Getting Nuclear Weapons: Constraining Its Future Nuclear Options' (2012) 15 <https://dissem.in/p/37253385/preventing-iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-march-2012> accessed 7 August 2024.

[361] Mueller (n 347) 3.

[362] 'George Bush and the Axis of Evil' *The Economist* <https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil> accessed 9 June 2024.

exacerbates the existing political tensions between the US and Iran and shows that cyber warfare has taken on a new dimension.[363] Iran's nuclear program has been a significant concern for the United States and Israel in particular, and the Stuxnet attack demonstrates how far these concerns can be taken. To understand the background of the process, it is helpful to look at the following picture.

Table 4. Part I - Chronology of Events and Political Background (Adapted from Baezner and Patrick)[364]

Chronology of Events (Political Background)	
Date	**Event**
29.01.2002	George Bush, in his State of the Union address to Congress, labels North Korea, Iran, and Iraq as an "Axis of Evil" for pursuing weapons of mass destruction.[365]
08.2002	An Iranian dissident group discloses that the government is enriching uranium at the Natanz nuclear facility. The USA responds by alleging that Iran is seeking to develop nuclear weapons.
02.2003	Iran acknowledges enriching uranium at Natanz, leading to the first visit by international inspectors from the International Atomic Energy Agency (IAEA). These inspections will continue regularly thereafter.
2006	The international community initiates diplomatic talks to persuade Iran to halt its nuclear program. However, Iran refuses to stop, leading to new international sanctions that further escalate tensions between the USA and Iran.[366]
06.2010	VirusBlockAda, a Belarus-based antivirus company, discovers the Stuxnet worm. They received a malware sample causing a computer in Iran to reboot repeatedly. This malware surprises specialists due to its use of a zero-day exploit, which is uncommon for a computer

[363] Lindsay (n 345) 380.
[364] Baezner and Robin (n 346) 6–7.
[365] 'George Bush and the Axis of Evil' (n 365).
[366] 'Fact Sheets: Iran | Arms Control Association' <https://www.armscontrol.org/factsheets/IranProliferation> accessed 9 June 2024.

	worm.[367] Typically, worms exploit flaws in web pages or bugs in legitimate software to infect computers.

Table 5. Part II - Chronology of Events and Political Background (Adapted from Baezner and Patrick)[368]

12.07.2010	News of the discovery of a computer worm using a zero-day exploit goes public, prompting the antivirus and technology communities to reverse-engineer and investigate this unusual malware. At this time, Stuxnet is believed to be an industrial spying tool. Its sophistication indicates that substantial resources were invested in its development.[369]
08.2010	Symantec reveals that Stuxnet's goal is sabotage rather than espionage.[370] Notably, 60% of infected computers are in Iran, suggesting the worm originated there.[371] Experts trace the infection back to five Iranian organizations, confirming Iran as the likely target.[372] During this time, Stuxnet's C&C servers lose connection with Iranian computers, indicating Iran's attempts to contain the worm.[373] Meanwhile, the Bushehr power plant's nuclear section launch is delayed due to a technical issue.[374]
09.2010	Iranian officials acknowledge that a computer virus infects some employees' personal computers at the Bushehr nuclear plant. They blame Western countries for the attack. [375]

[367] 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | WIRED' <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/> accessed 9 June 2024.

[368] Baezner and Robin (n 346) 6–7.

[369] 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | WIRED' (n 370).

[370] ibid.

[371] Aleksandr Matrosov and others, 'Stuxnet under the Microscope' (2010) 6 ESET LLC (September 2010) 15 <http://ca-apac.com/image/ITR%201.pdf> accessed 9 June 2024.

[372] Lindsay (n 345) 380.

[373] 'Stuxnet Timeline Shows Correlation Among Events | WIRED' <https://www.wired.com/2011/07/stuxnet-timeline/> accessed 9 June 2024.

[374] Collins and McCombie (n 349) 85.

[375] James Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War' (2011) 53 Survival 23, 25.

11.2010	Iran halts uranium enrichment at the Natanz nuclear plant without explanation.[376] It is later assumed they are attempting to remove Stuxnet from the facility. Subsequently, the head of Iran's Atomic Energy Organization and acting Foreign Minister admits that a computer virus has infected Iranian nuclear installations.[377]
12.2010	The Institute for Science and International Security (ISIS), a US-based non-profit monitoring Iran's nuclear program since the 1990s, confirms that the Stuxnet worm is designed to target elements configured like Natanz's centrifuges.

3.15.5. Indicators and Inferences

Code Analysis

Security researchers found several indicators within the code that hinted at its origins. For instance, the word "Myrtus" in the code was speculated to reference the Hebrew word for Myrtle, which could be linked to the biblical story of Esther saving the Jews from a Persian massacre.[378]

Nationality and Expertise

The detailed knowledge about the Siemens systems and the specific configuration of the Iranian centrifuges suggested that the developers had access to classified information, likely from intelligence agencies.[379] Although no country officially claimed responsibility for Stuxnet, leaks and statements from officials in the United States and Israel strongly suggested their involvement. For example, a video shown at the retirement party of Israeli

[376] Farwell and Rohozinski (n 378).
[377] Avag (n 354).
[378] De Falco (n 362); Liam O. Murchu and Eric Chien (n 348) 24.
[379] 'The Real Story of Stuxnet - IEEE Spectrum' (n 341).

Defense Forces' Lieutenant General Gabi Ashkenazi included Stuxnet among his achievements, indirectly acknowledging Israel's role.[380]

Furthermore, the psychological impact of Stuxnet should not be understated.[381] The attack demonstrated that Iran's nuclear program was not impervious to external interference, thereby increasing the regime's anxiety about future cyber threats. This heightened state of alert potentially diverted resources and attention away from the advancement of their nuclear capabilities.[382] The discovery of the Duqu malware in 2011, which shares components with Stuxnet, indicates ongoing efforts to gather intelligence and prepare for subsequent attacks.[383]

Stuxnet's deployment marked a significant escalation in using cyber tools to achieve strategic military objectives. By effectively disrupting Iran's nuclear program, Stuxnet delayed Iran's progress and exposed the vulnerabilities inherent in relying on digital infrastructure. The ongoing threat of similar cyber-attacks continues to shape the strategic landscape, compelling nations to bolster their cyber defenses and reconsider the implications of cyber warfare in modern conflict.

[380] Mueller (n 347) 3; 'Israeli Security Chief Celebrates Stuxnet Cyber Attack' (*The Telegraph*, 16 February 2011) <https://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html> accessed 9 June 2024.

[381] Albright and others (n 363) 30.

[382] ibid 15.

[383] ibid.

4. ISRAEL'S CYBER SECURITY

A comprehensive analysis of the institutional and political structure behind Israel's success in cybersecurity is essential for understanding the country's cybersecurity strategies and practices. In previous sections, the basic cybersecurity concepts and the historical background of Israel's development in this field were discussed in detail. This section will analyze the main elements of Israel's cybersecurity ecosystem, its significant institutions and companies, and their roles.

The Israel Defense Forces (IDF), especially military intelligence units such as Unit 8200, the National Cyber Directorate (INCD), and intelligence agencies such as the Mossad and Shin Bet, play a critical role in shaping Israel's cyber security strategy.[384] In addition to these institutions, Israel's dynamic technology companies and start-up ecosystem also make significant contributions to cybersecurity. Globally recognized companies such as Check Point, CyberArk, and Palo Alto Networks have a significant stake in developing Israel's cybersecurity capacity.[385]

This chapter will also examine the technical aspects of Israel's cyber security strategy. The structuring of the cybersecurity infrastructure, the technologies used, the solutions developed against cyber threats, and the deterrence methods will be discussed in detail. The threats that Israel faces in cyberspace, the source and nature of these threats, the defense mechanisms developed, and strategic approaches will also be evaluated. In addition, Israel's solutions and deterrence methods will be examined, taking into account the threats, potentials, and threats posed by Israel in cyberspace.

4.1.A Brief Overview of Israel's Innovation Economy

To understand Israel's cyber security structure, it is necessary to understand the innovation economy, which is an essential factor for the cyber ecosystem. The concept of innovation economy describes an economic model in which innovation is the critical

[384] Frei (n 38).
[385] Cordey (n 39) 4.

determinant of economic growth, competitiveness, and social welfare. This approach emphasizes the essential role of knowledge, technology, entrepreneurship, and creativity in driving economic development. As Asher Tishler and Naama Halevi-Davidov note, "The interest in innovation activities within mainstream economics and management is clearly attributable to the recognition of the sustained and positive impact of technical progress on productivity."[386] In other words, the main reason for the growing interest in innovation activities is the widespread recognition of technological progress's sustained and positive impact on productivity. Innovation and human capital development can be considered as critical elements of knowledge. The OECD defines knowledge as the sum of R&D expenditures, educational investments, and software costs.[387]

Despite its strategic location in the Middle East, Israel is a relatively small country. According to the armistice agreements signed in 1949, Israel has an area of 20,770 square kilometers and a population of approximately 9.5 million.[388] (data from the Turkish Ministry of Foreign Affairs). Nevertheless, the Israeli economy has undergone a remarkable transformation over time and has positively differentiated itself from other countries in the region.

While Israel's economy was agriculture-based in its early years of establishment and was not rich in underground resources, it has become one of the most prosperous countries in the region with a skilled workforce.[389] Israel's adoption of an export-led growth model, investment in technology and high-tech fields, and encouragement of entrepreneurship, innovation, and research and development (R&D) culture are behind this success.[390]

Today, Israel ranks in the high-income group in terms of per capita income and is characterized as a high-tech country. Given the regional dynamics and geopolitical challenges, the country's economic transformation and success are all the more remarkable.[391]

---

[386] Naama Halevi-Davidov and Asher Tishler, 'Innovation in Israel: Facts and Measures' 2.

[387] Roberto Mangabeira Unger, 'THE KNOWLEDGE ECONOMY' 11.

[388] 'Ülke Künyesi / T.C. Dışişleri Bakanlığı' <https://www.mfa.gov.tr/israil-kunyesi.tr.mfa> accessed 25 June 2024.

[389] Dan Breznitz, 'Industrial R&D as a National Policy: Horizontal Technology Policies and Industry-State Co-Evolution in the Growth of the Israeli Software Industry' (2007) 36 Research Policy 1465, 1473.

[390] J Avidor, *Building an Innovation Economy: Public Policy Lessons from Israel* (SSRN 2014) 37 <https://ssrn.com/abstract=1856603> accessed 7 August 2024.

[391] Dan Peled, 'Defense R&D and Economic Growth in Israel: A Research Agenda' [2001] Science 5.

Due to geopolitical problems and the difficulties arising from the occupation of the Palestinian territories, the Israeli economy has had to place great emphasis on overseas trade. Given the profitability of export and import activities, the country's limited domestic market, and political tensions with countries in the region, this economic model has become a necessity. Israel's economic adventure started with agricultural products in Kibbutzes during its foundation period but underwent a significant transformation.[392] The country turned to defense industry products, jewelry trade, and health and pharmaceutical sectors in the following years. With the digitalization era, it focused on the export of high-tech products. Today, these sectors form the basis of Israel's export markets.[393]

Despite having a population of 9.5 million, Israel's economic performance is remarkable. The country's gross domestic product (GDP) is 502.3 billion dollars.[394] This figure shows that Israel's per capita income is 51,990 dollars. The Israeli economy grew by 6.5% in 2022, by an average of 4.4% in 2018-2022. The unemployment rate in the country was 5%, and the inflation rate (CPI) was 4.4%. Moreover, foreign direct investment inflows to Israel amounted to USD 27.8 billion, while public debt stood at 60.7% of GDP.[395]

According to the OECD report on higher education in 2022, Israel is among the top 10 countries in the world in terms of the proportion of the population with a higher education degree.[396] Research shows that 50.12% of Israel's population has a higher education degree, well above the OECD average of 39%.[397]

Countries with the most educated populations share some common characteristics. Israel shares these characteristics, including a low unemployment rate, high investment in higher education, and high levels of happiness among citizens. Israel's unemployment rate is 5.05%, which is relatively low compared to other countries on the list. Regarding

[392] Tamar Almor, 'Born Global: The Case of Small and Medium Sized, Knowledge Intensive, Israeli Firms' (2000) 1.

[393] Tabansky and Ben Israel (n 35) 21–22.

[394] 'Israel GDP' (*World Bank Open Data*) <https://data.worldbank.org> accessed 25 June 2024.

[395] The Heritage Foundation, 'Index of Economic Freedom: Israel | The Heritage Foundation' (*Index of Economic Freedom | The Heritage Foundation*) <https://www.heritage.org/index> accessed 12 June 2024.

[396] OECD, *Education at a Glance 2022: OECD Indicators* (Organisation for Economic Co-operation and Development 2022) <https://www.oecd-ilibrary.org/education/education-at-a-glance-2022_3197152b-en> accessed 25 June 2024.

[397] ibid.

investments in higher education, Israel spends USD 12,336 per student. Although this figure is low compared to other countries, it is above the world average. [398]

4.2.Defense Industry and Economy: Israel's Strategy for Sustainable Growth

Israel's leadership in the high-tech sector is mainly due to the adaptation of military and defense technologies for civilian use. The country's strength in the defense industry is based on the effective use of high technology in the defense industry, rather than on factors such as the number of troops, the abundance of natural resources, or their balanced distribution.[399]

The Israeli economy has been structured to adapt to the ongoing conflict since the country's founding.[400] To survive under prolonged war conditions, it has become imperative for Israel to have dynamic, fast-decision-making individuals, companies, and bureaucratic structures. This leads the Israeli economy to be considered as a war economy. Characterized as a war economy, the Israeli economy has to obtain the resources it needs, find suitable markets, and sustain all this in an aggressive environment. Under these challenging conditions, Israel has developed various strategies to maintain its economic activities. These include investing in high-tech sectors, developing human capital, promoting innovation, and strengthening international cooperation.[401]

Despite geopolitical challenges and limited natural resources, Israel has achieved remarkable success thanks to its innovation-driven economic model.[402] The country's economic transformation is based on an export-led growth strategy, investments in technology and high-tech fields, promoting an entrepreneurial culture, and the importance of R&D activities.[403] Israel's strength in the defense industry also stems from the effective use of high technology, and the adaptation of military technologies for civilian use contributes to the country's economic development. In conclusion, Israel's innovation economy model stands out as the key to sustainable growth and global competitiveness.

---

[398] ibid.

[399] Karaoğlu and Elhan (n 56) 314.

[400] Mark Broude, Saadet Deger and Somnath Sen, 'Defence, innovation and development: the case of Israel' (2013) 12 Journal of Innovation Economics & Management 37, 38.

[401] Baram and Ben-Israel (n 169) 87.

[402] Tabansky and Ben Israel (n 35) 15.

[403] ibid 15–16.

4.3.Israel's Security Forces and Defense Industry

Israel's innovation economy and high technology are closely linked to its military power. Israel stands out with its high-tech military equipment and cyber power units. Therefore, it is important to examine Israel's military power, defense industry and leading companies in this field in order to understand the country's technological success and regional influence.

The country's geopolitical position and security needs require the continuous modernization of its defense industry. Numerous defense industry companies, cooperating with the Israeli Ministry of Defense and the private sector, develop and produce advanced technology products in various fields such as electronic warfare systems, unmanned aerial vehicles, electro-optical systems, aviation, space technologies, land and naval platforms.[404] Therefore, it is necessary to examine Israel's military and defense industrial system to understand the country's cybersecurity actors before explaining them.

4.4.Historical Background

Since its independence in 1948, Israel has always treated security issues as a priority due to its geopolitical position in the Middle East and conflicts with neighboring countries. Security forces and issues play a decisive role in the political and social life of the country.

Since its establishment, Israel has been involved in several major conflicts, including the 1948 Arab-Israeli War, the 1956 Suez Crisis, the 1967 Six-Day War, the 1973 Yom Kippur War, the 1982 Lebanon War, and the 2006 Lebanon War. In addition, Israel lives under a constant security threat due to the ongoing occupation of Palestinian territories and conflicts with the Palestinians. The Camp David Treaty signed with Egypt in 1978 marked the turning point in Israel's security approach to the modern era. With this agreement, which was the first time an Arab state recognized Israel, Israel's security architecture was also affected.[405]

[404] Karaoğlu and Elhan (n 56) 314.
[405] ibid.

This challenging security environment has led Israel to continuously develop and strengthen its military and intelligence capacity. The Israel Defense Forces (IDF) has become one of the country's most important institutions. Compulsory military service has created a strong bond between Israeli citizens and the military and reinforced the country's security-oriented culture. The central role of security issues in Israeli politics has also shaped the country's foreign policy. To maintain deterrence against regional threats and ensure national security, Israel continues to maintain a robust military presence and conduct cross-border operations when necessary.

4.5.Israel Defense Forces (IDF)

Israel's armed defense forces are the Israeli Defense Forces (IDF). It was founded by David Ben-Gurion on May 26, 1948, 12 days after Israel declared its independence, and has fought many wars and conflicts. In Israel, the army has a decisive role in social and political life. The ongoing security threat since 1948 has led to compulsory military service for all Israeli citizens, both men and women. A significant part of the lives of citizens who periodically serve and train as a reserve force after the end of their mandatory service is spent in or in relation to the army.

In Israel, both men and women are subject to compulsory military service. However, the length of service and reserve obligations differ depending on gender and roles in the Israel Defense Forces (IDF). Men generally serve 32 months (approximately 2 years and 8 months) of compulsory military service when they reach the age of 18, while women are obliged to serve 24 months (2 years).[406] Citizens who have completed compulsory military service must serve in reserve units until a certain age. Men usually serve in the reserve for a few weeks a year until age 40, while women are subject to this obligation until they get married or reach the age of 38. The length of reserve service may vary depending on the individual's age and unit. [407]

[406] 'Israeli Army to Extend Mandatory Service: Report' <https://www.aa.com.tr/en/middle-east/israeli-army-to-extend-mandatory-service-report/3131078> accessed 25 June 2024.

[407] Richard Weitz, 'Israel' (Strategic Studies Institute, US Army War College 2007) 98–99 <https://www.jstor.org/stable/resrep12108.14> accessed 25 June 2024.

Israel's conscription system also allows for some exceptions. For example, the Haredi sector, known as Ultra-Orthodox Jews, can be exempted from military service if they pursue full-time religious education.[408] Israeli Arab citizens are also exempt from conscription but can serve voluntarily.[409] Israel's conscription system plays a vital role, given the country's geopolitical position and security needs. However, the fairness of the system and the exemptions for certain groups are sometimes disputed in society. Despite this, conscription remains essential to Israeli society and underpins the country's defense capacity.

Military Power

As of 2022, the total number of personnel is 169,500, and the number of reserve personnel ready for call-up is 465,000.[410] The IDF comprises land, naval, air, and space forces. Israel is also claimed to be a nuclear weapons state, but this claim has not been accepted or denied by the Israeli authorities. [411]

[408] Lorenzo Tondo and Quique Kierszenbaum, 'Plan to End Ultra-Orthodox Students' Military Exemption Sparks Row in Israel' *The Guardian* (26 March 2024) <https://www.theguardian.com/world/2024/mar/26/plan-end-ultra-orthodox-students-military-exemption-row-israel> accessed 25 June 2024.

[409] Israel Policy Forum, 'The Haredi Exemption' (*Israel Policy Forum*, 2 April 2024) <https://israelpolicyforum.org/2024/04/02/the-haredi-exemption/> accessed 25 June 2024.

[410] Karaoğlu and Elhan (n 56) 314.

[411] ibid.

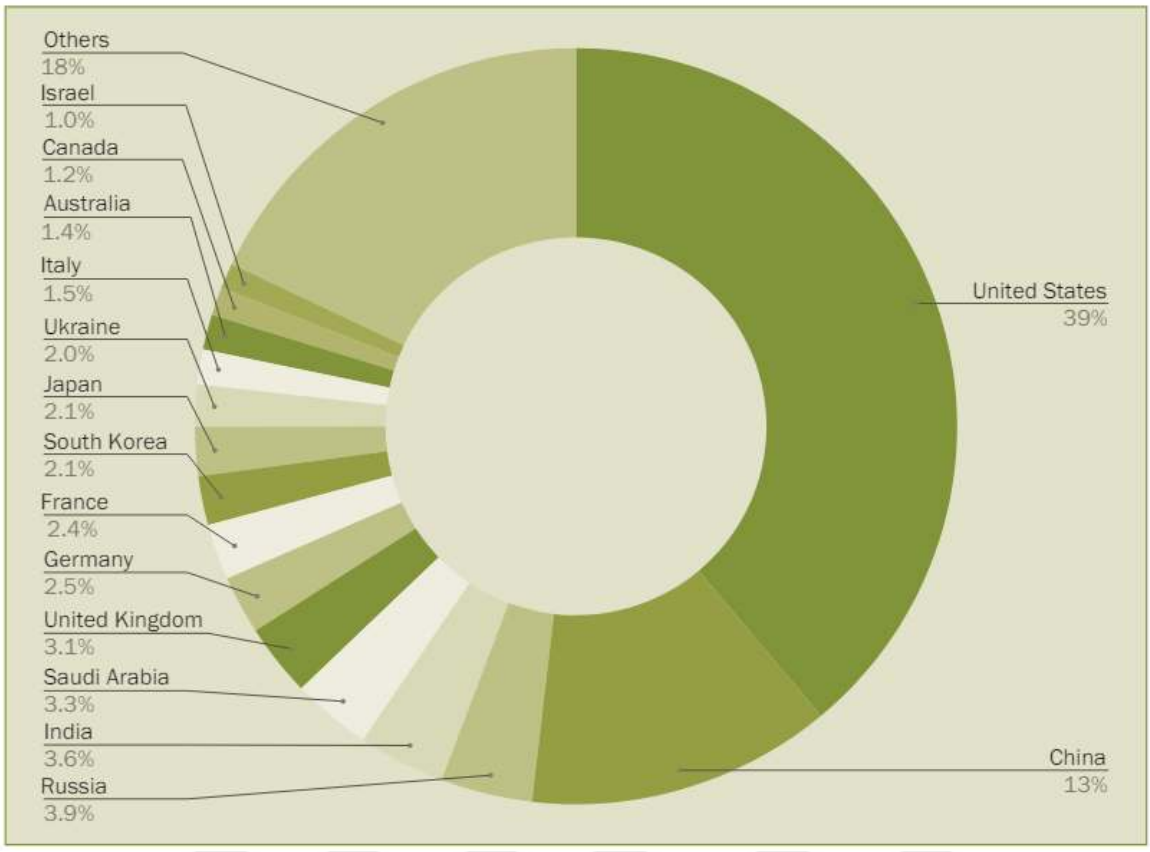

Figure 11. Countries Share of Global Military Expenditures (SIPRI 2022)[412]

If we look at Israel's military expenditures, according to the SIPRI Report, Israel's military spending in 2022 amounted to 23.4 billion dollars, which is a decrease of 4.2% compared to the previous year.[413] However, despite this decrease, Israel's military spending is still 26% higher than in 2013. This decrease, the first recorded since 2009, is noteworthy. [414] This decrease in military spending can be seen as a result of the Israeli government's efforts to reduce public spending and address the budget deficit. As of December 2022, the measures have transformed the budget deficit into a GDP surplus of 0.5%. In 2022, Israel ranked 15th in the world regarding military spending. [415] Such high Israeli military

[412] Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2022: Armaments, Disarmament and International Security* (Oxford University Press 2022) <https://www.sipri.org/yearbook/2022>.
[413] ibid.
[414] ibid.
[415] ibid.

expenditures are made tolerable by US support.[416] By 2020, an average of 18 percent of the Israeli defense budget was financed by US military aid. Annual US financial support to the Israeli defense budget is around $3.5 billion. This amount excludes project-based investments and support. With the financing and technology support for projects such as Iron Dome, Arrow Projects, David's Sling, etc., the total aid reaches around 4 billion dollars.[417]

- **IDF Ground Forces**

With 128,000 personnel, the Israeli Land Army is not a separate unit like other force commands. It is directly integrated with the IDF and divided into three main commands: North, South, and Center. [418]

- **IDF Air and Space Forces**

With 34,000 personnel, the Israel Air and Space Force has a variety of functional vehicles and ammunition, including combat aircraft, electronic warfare, and helicopters. With 348 combat aircraft, the Israeli Air Force is the most powerful air force in the Middle East.[419]

- **IDF Navy**

It is a small unit of the Israeli armed forces with approximately 9,500 personnel. [420]

4.6. Israel's Defense Industry Sector

Israel has witnessed many wars and conflicts since its establishment in 1948. This has profoundly affected the development of the country's defense industry. In the early years, the Israel Defense Forces (IDF) were equipped with weapons and equipment from the Second World War, inherited from the UK and purchased in Europe.[421] These weapons' maintenance, repair, and modification formed the basis of the Israeli defense industry. In the 1950s and 1960s, with the support of Britain and France, Israel embarked on a rapid rearmament process. Israel acquired many tanks, armored vehicles, Mystere 4 and Vatour jet fighters from France, and Centurion tanks and Meteor jet fighters from Britain. The embargo imposed by France after the Six Day War in 1967 led Israel to restructure its defense industry

[416] Karaoğlu and Elhan (n 56) 314.
[417] Jeremy M Sharp, 'U.S. Foreign Aid to Israel' 17.
[418] Karaoğlu and Elhan (n 56) 315.
[419] ibid 316–317.
[420] ibid 318.
[421] ibid 320.

not only in terms of maintenance and repair but also in terms of weapons development.[422] With the rapid growth of military relations with the United States in the 1970s and 1980s, Israel acquired many high-tech weapon systems. With technical assistance and technology transfers from the United States, the Israeli defense industry began to develop new products and platforms.[423] Indigenous defense systems such as the Kfir fighter jet, the Merkava main battle tank, and the Gabriel anti-ship missile were introduced during this period. From the 1980s onwards, great emphasis was placed on electronic warfare systems and unmanned aerial vehicles (UAVs), especially against Syria's integrated air defense system. [424] After the 1973 Yom Kippur War, UAVs were used intensively in the 1980s. These technologies led to great success against Syrian warplanes and air defense systems in the 1982 Lebanon War.[425] Due to Israel's small area and population, society, the army, the state bureaucracy, and the defense industry are intertwined. Engineers, technicians, and managers working in the defense sector gain field experience through military service.[426] This enables defense industry employees to gain experience from the end user's perspective.

4.6.1. Some Prominent Israeli Defense Industry Companies

Israel Aerospace Industries (IAI) was founded in 1953 under the name Bedek Aviation Company (BAC) on the instructions of then Defense Minister Simon Peres. As of the end of 2021, the company has 15,000 employees and a turnover of approximately 4.5 billion dollars. IAI operates in communication and sensor systems, avionics, command and control software, intelligence, early warning, and homeland security solutions. Elta Systems, one of the company's primary units, works in communication and sensor systems, avionics systems, and command and control software for the military and civilian markets. [427]

Elbit Systems was founded in 1996 as a joint venture between Elron Electronic Industries and the Israeli Ministry of Defense. As of the end of 2021, the company has approximately 18,000 employees and a turnover of around 5.3 billion dollars. Elbit Systems operates in military aircraft and helicopter systems, commercial aviation systems, UAVs,

[422] ibid.
[423] 'U.S. Aid to Israel in Four Charts' (n 154).
[424] Karaoğlu and Elhan (n 56) 320.
[425] ibid 321.
[426] Baram and Ben-Israel (n 169).
[427] 'IAI Company Profile - The Solution to Defense and Security Challenges' <https://www.iai.co.il/about/company-profile> accessed 25 June 2024.

electro-optical systems, land vehicles, military naval systems, ammunition, C4ISR systems, electronic warfare, and electronic intelligence systems. The company's key units include the Hermes UAV family, Elbit Medical Imaging, and Elbit Systems Land.[428]

Rafael Advanced Defense Systems was founded under the name HEMED by Shlomo Gur shortly after independence in 1948. As of the end of 2021, the company had over 8,000 employees and a turnover of 3 billion dollars.[429] Rafael operates in the fields of rocket and missile systems, including the Iron Dome missile defense system, the Iron Beam anti-missile laser weapon system, the Spike anti-tank missile family, the Python and Derby air-to-air missile families, and the Trophy anti-tank missile defender active protection system. [430]

Israel Weapon Industries (IWI) was founded 1933 as Israel Military Industries (IMI). In 2005, its small arms manufacturing unit, Magen, was privatized and sold to SK Group. IWI is active in the production of pistols, infantry rifles, and machine guns and in counter-terrorism and security training services for security forces.

Israel Shipyards was established in 1959 as a state-owned economic enterprise for military and civilian shipbuilding and privatized in 1998. The company operates in areas such as Saar 4-type guided missile attack boats, patrol boats, assault boats, the OPV-45 patrol ship, and the Saar S-72 corvette.[431]

4.7.Introduction to Israel's Cybersecurity Landscape

In the previous chapters, fundamental issues such as the definition of cyber security, the tools used, and the functions of these tools are discussed in detail. In addition, recent cases and important developments in cybersecurity have been analyzed. Then, the factors behind Israel's success in the field of cybersecurity were explored in depth. In light of the information obtained in this context, it is emphasized that the national security strategy, the country's unique cultural structure, and strong innovation economy are of great importance to Israel's cyber security strategy.

[428] Karaoğlu and Elhan (n 56) 326.
[429] 'Our Story' (*Rafael*) <https://www.rafael.co.il/our-story/> accessed 25 June 2024.
[430] Karaoglu and Elhan, *Israel Academic Anatomy of a Country*, 327.
[431] 'Israel Shipyards – DIMSE' <https://dimse.info/israel-shipyards/> accessed 25 June 2024.

In this section, based on the information obtained in the previous section, Israel's cyber security policy will be discussed in more detail. It will also examine how Israel interacts with state and non-state actors in the field of cybersecurity and the role and importance of these actors in its cybersecurity policy. In addition, Israel's position in cyberspace, its approach to cybersecurity developments in the international arena, and its activities in this field will also be discussed. Thus, Israel's cybersecurity policy, strategy, and the factors behind its success will be revealed from a holistic perspective.

4.8. Israel's Understanding Of National Security And Cyber Security

In the previous section, the definition of the security concept was examined, and a national security strategy or doctrine was explained. It tried to understand how Israel's national security strategy was shaped in the historical process. To summarize, Israel's national security policy has been shaped by the following basic principles since its establishment[432] :

- ❖ Building qualitative superiority against numerical superiority:

-Israel is focused on gaining a qualitative edge, as it is at a population and economic disadvantage compared to Arab countries.

-It has sought to strengthen its military by investing in advanced training tactics, state-of-the-art ammunition, and R&D.

-Aimed to achieve qualitative superiority by cooperating with great powers like the United States and France.

- ❖ Compensating for the lack of strategic depth with an early warning system:

-Israel's limited territory and constant threats have necessitated an emphasis on early warning systems.

-It aimed to be prepared for possible attacks by providing intelligence superiority.

- ❖ Using deterrence to prevent a potentially catastrophic all-out war:

-Israel, aware that a large-scale war could devastate the country, has sought to delay or prevent it.

-It aimed to deter its enemies from war by maintaining its military and strategic superiority.

[432] Tabansky and Ben Israel (n 35) 11.

❖ Building an alliance with a global superpower:

-Israel, lacking strategic depth, needed a superpower to protect it.

-Initially establishing close relations with France, Israel later developed a strong alliance with the United States.

-The economic and military aid received from the US has strengthened Israel's position in the region.

❖ US Aid to Israel:

- The US saw Israel as a counterbalance in the Middle East and accepted it as an ally against the USSR-backed Arab states.

- US aid to Israel is concentrated mainly in military and economic areas.

- The "Qualitative Military Edge" (QME) principle has formed the basis of US military aid to Israel.

- Israel has received around 300 billion dollars in aid from the US since its establishment.[433]

- The US has also made significant investments in Israel's defense industry.

Israel's national security strategy involves balancing its numerical disadvantage with qualitative superiority, compensating for its lack of strategic depth through early warning systems, preventing wars through deterrence, and building an alliance with a global superpower. The special relationship with the United States has been essential in strengthening Israel's position in the region.

4.9.The Place of Cyber Security in National Security Strategy

Today, information technologies are active in every field and have become all-encompassing. Many areas of our lives, such as weapon systems, the defense industry, and the national and international economy, are equipped with information technologies.[434] As information technologies have become democratized, their use among nation-states and individuals has become more widespread, thus creating security vulnerabilities and threats. In order to counter these threats and to be prepared for attacks and cyber wars, states have started to include cyber security strategies in their national defense doctrines.

[433] 'U.S. Aid to Israel in Four Charts' (n 154).

[434] Ilai Saltzman, 'Cyber Posturing and the Offense-Defense Balance' (2013) 34 Contemporary Security Policy 40, 43.

For the actions in cyberspace to become a problem, that is, an object of security, the subject who carries out the attack or action must benefit from this action. The elimination and deterrence of such threats in cyberspace fall within the scope of cyber security.[435] In cyberspace, "pre-emptive" strategies are pursued against attacks. Deterrence is vital at this point. Since cyberspace is open to constant updating due to its nature, threats are constantly renewed and require continuous caution. Static measures are contrary to the dynamic nature of cyberspace. Cybersecurity strategies must be multifaceted since cyberspace is not a regional structure.[436] The capacity of actors in cyberspace is measured by the damage they can cause. The more advanced capacity and versatile strategy an actor has in cyberspace, the more damage it can inflict.[437] Like the importance of military measures in the physical world, cyber security is integrated into national security strategies.[438] At the level of cyber actions, in addition to the previously mentioned cyber attack methods, cyberspace can be used for intelligence gathering, sabotage of systems, or the cyber pillar of international terrorist acts.[439] In terms of actors in cyberspace, there are individual hackers, non-state groups (such as hacking groups, terrorist organizations, or criminal organizations), and finally, nation-states with cyber power.[440] In this sense, the prominent cyber security strategy is "cyber deterrence." Operation Desert Storm is an essential case for cybersecurity, as it is considered the first modern war in which cyber warfare tactics were used. During the operation, the US and its allies also conducted a cyber operation targeting Iraq's military and civilian infrastructure. In this operation, along with the attacks on the military wing, the command and control systems and communication networks of the Iraqi state were targeted, and the air defense systems were tried to be disabled.[441] In this sense, with this operation, cyber deterrence has become a topic of discussion in the context of information warfare.[442] The cyber war against Estonia mentioned in the previous section, the Georgian attacks that coincided with the same period, and the Stuxnet attack against Iran have led nation-states, academic circles, and military units to approach cyber security more sensitively.

[435] Singer and Friedman (n 208) 34–35.
[436] Saltzman (n 437) 56.
[437] ibid 43–44.
[438] James Andrew Lewis, 'Linking National Security and Innovation: Part 1' (Center for Strategic and International Studies (CSIS) 2021) 575 <https://www.jstor.org/stable/resrep31134> accessed 19 March 2024.
[439] Martin Rudner, 'Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge' (2013) 26 International Journal of Intelligence and CounterIntelligence 453, 454.
[440] Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence' (2017) 40 Journal of Strategic Studies 92, 96.
[441] Tabansky and Ben Israel (n 35) 12.
[442] Tor (n 443) 98–99.

Cyber attacks cannot directly kill people or destroy structures like other physical means of attack. Still, they can create long-term economic damage, and cyber intelligence activities can jeopardize data security.[443] As a natural outcome of all these processes, states and other organizations feel threatened by cyberspace. They try to ensure their security in cyberspace by pursuing policies to prevent this threat.[444] As computer technologies develop and systems become more dependent, threats are also shaped. Obtaining information by accessing the cell phone of a bureaucrat is important for national security and can create a national security problem for the country in question. Malware such as the Pegasus software, which first emerged in 2016, has been used to steal and track many people's personal data. This incident, discussed in more detail in the following sections, is an example of the diversification of cyber threats.

As a result, vulnerabilities have emerged as individuals, companies, and nation-states have started participating in cyberspace. These vulnerabilities and threats have been tried to be eliminated with cyber security strategies at both individual and state levels, and these strategies have started to find a place in national security doctrines.

4.10. Israel Cyber Security Strategy 2015

In 2015, the IDF Chief of Staff, Gadi Aizenkot, published the Official Strategy of the IDF, which includes sections on cyber security. In this document, cyberspace is recognized as a battlefield. It is stated that defense, intelligence gathering, and offensive activities are carried out in cyberspace.[445] To increase the IDF's power in cyberspace and expand its capabilities, it is envisaged that a cyber security unit will be established under the IDF.[446] It is stated that cyber security is essential for the order of the state, the functioning of institutions, and the IDF's ability to continue its operations in times of war and emergency.[447] A high-speed network infrastructure that enables inter-agency information communication is established to achieve this goal.[448]

[443] 'Cyber Conflict and Deterrence' (2016) 22 Strategic Comments iii, 2.
[444] KÖKSOY (n 221) 332–333.
[445] 'Israel Defense Forces Strategy Document | Belfer Center for Science and International Affairs' 44 <https://www.belfercenter.org/israel-defense-forces-strategy-document> accessed 20 June 2024.
[446] ibid.
[447] ibid.
[448] ibid 21.

4.11. Israel's Cyber Security Strategy: Cumulative Deterrence

Cyber deterrence requires a strategy derived from, but distinct from, traditional deterrence. In its simplest definition, deterrence is preventing negative actions by frightening enemies with the threat of violence. In a classical definition, deterrence is to make enemies believe that they are not militarily superior, convince them that an attack will harm them, and prevent it.[449] According to Wilner, if the use of violence occurs, the deterrence strategy has failed.[450] Deterrence in Israel's national security strategy differs from the classical approach. The strategies referred to in the literature as "Cumulative" and "Asymmetric"[451] deterrence differ from the classical definition. There is no absolute deterrence in the Israeli security doctrine shaped by Jabotinsky's Iron Wall strategy. This is because it is not assumed that the threat of violence can deter Israel's enemies. The conflict is believed to be continuous in the short and long term.

Israel's deterrence policy is perpetuated because it seeks to prevent potential threats by constantly demonstrating force against hostile actors. Military operations are continuous to prevent its rivals from using force. In this sense, resorting to violence does not make the strategy a failure. In fact, it shows that the strategy is successful. Israel's deterrence doctrine is based on preventing, postponing, and mitigating the next hot conflict rather than eliminating the attack.[452]

Israel's first Prime Minister, David Ben-Gurion, shaped this Israeli-specific deterrence strategy. The assumption among Israeli policymakers that the conflict would not end through diplomatic compromise demonstrated the ineffectiveness of absolute deterrence.[453] Therefore, Israel pursues a strategy of cumulative deterrence. Cumulative deterrence is an alternative to absolute deterrence. The 20th-century model of absolute deterrence with nuclear deterrence strategies is considered useless in the cyber domain. Tor states that Israel's deterrence strategy differs from the US deterrence policy. According to

[449] Shmuel Bar, 'Israeli Strategic Deterrence Doctrine and Practice' (2020) 39 Comparative Strategy 321, 329.
[450] Alex S Wilner, 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism' (2011) 34 Journal of Strategic Studies 3, 8–10.
[451] Amos Malka, 'Israel and Asymmetrical Deterrence' (2008) 27 Comparative Strategy 1.
[452] Dmitry (Dima) Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force' (2017) 26 Security Studies 157, 163.
[453] Jabotinsky (n 90).

the American doctrine, using force means the deterrence strategy has failed.[454] In contrast, Israel's deterrence strategy includes the use of force. Retaliating for attacks and using military force when necessary is necessary to maintain the effect of cumulative deterrence. This strategy aims to deter aggressive actions by increasing their cost. [455] Israel also seeks to apply the principle of cumulative deterrence in the cyber domain. Israel's cumulative deterrence policy in the cyber domain is a strategy used to eliminate cyber threats against it. This strategy assumes that deterrence should be cumulative rather than terminal, that is, absolute.[456] Due to the nature of cyberspace, it is believed that attacks should be punished continuously since cyber attacks cannot be ended in an absolute manner. In this regard, Adamsky notes that this strategy is inspired by Criminal law.[457] In conclusion, Israel's cumulative cyber deterrence strategy in cyberspace is related to its national security policy and the nature of cyberspace. It is an outcome of the assumption that conflict and attacks are inevitable and continuous.

4.12. Israel's Cyber Security Actors - State and Non-State Actors

Israel is one of the most important actors in the world in cyber security. Its success in this field can be attributed to the security needs of its founding and its investment in high technology. Although information technologies came to the fore in the 1980s, Israel's journey in this field began in the 1990s. In particular, specially trained units such as Unit 8200, established within the Israel Defense Forces, have specialized in cyber security and cyber intelligence.

Established in 1997, Tehila (Israel's e-government project) is considered an influential starting point in building Israel's cybersecurity infrastructure. The Tehila project pioneered the secure construction of the state's internet infrastructure and the transfer of state institutions to the digital world. [458]

[454] Tor (n 443) 93–94.
[455] ibid.
[456] ibid 92.
[457] Thomas Rid, 'Deterrence beyond the State: The Israeli Experience' (2012) 33 Contemporary Security Policy 125–127.
[458] KÖKSOY (n 221) 336.

Academia and the private sector have also played a significant role in developing Israel's cyber security capacity. In particular, universities such as Technion, which existed even before the establishment of the State of Israel, and various research organizations have played a role in increasing cyber security capacity. In the private sector, a start-up nation story has emerged thanks to the state's pioneering R&D investments and policies. Relatively small cities like Tel Aviv and Be'er Sheva are home to many globally advanced cybersecurity companies.[459] These companies have become cybersecurity exporters, producing world-class products. [460]

The State of Israel has regulated its dominance in the field of cyberspace through various laws and institutions. The Israel National Cyber Directorate (INCD), the Israeli National Cyber Bureau (INCB), and the National Cyber Security Authority (NCSA) are the leading institutions of the State of Israel in this field. In 2015, the IDF Strategy Document, prepared under the leadership of IDF commander Gadi Aizenkot, acknowledged the need to develop capacity in the cyber domain and recognized cyber as the fourth most important area in Israel's defense after Air, Land, and Sea.[461] In 2017, the Israel National Cyber Security Strategy prepared by the INCD aimed to improve Israel's resilience and defense in the cyber domain. This section examines Israel's state and non-state actors in the field of cyber security.

4.13. Israel's State Actors in Cybersecurity

4.13.1. Tehila

In 1996, the Israeli Ministry of Finance established a computer unit to develop an e-government project. The Tehila project, which was realized through the work of this unit, aimed to increase efficiency and control costs.[462] With the contributions of the teams in the Ministry's computer unit, Tehila has become the government's most significant assistant in financial transactions in Israel. Established in 1997, Tehila was created to create a secure IT infrastructure for the government. Its main functions included allowing citizens to securely access government services from their networks, securing government websites, and

[459] Tabansky and Ben Israel (n 35) 53.

[460] '6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry' <https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/> accessed 20 June 2024.

[461] 'Israel Defense Forces Strategy Document | Belfer Center for Science and International Affairs' (n 448).

[462] Tabansky and Ben Israel (n 35) 33–34.

creating a secure infrastructure for future digital projects. Tehila also included what we might consider a forward-thinking approach: digital identity cards, electronic forms and contracts, access to taxation, etc., electronic payment services, biometric databases, etc. The focus of the Tehila project was security. IT security was a key element of this security approach, and as access to the internet increased, projects like Tehila became more important.[463] This effort can be considered the government's first critical infrastructure protection effort.

4.13.2. Special Resolution B/84 and National Information Security Authority

By 2002, with the increase in digitalization and computer technologies, cybersecurity problems and system vulnerabilities began to emerge. The first groundbreaking development was the "critical infrastructure protection" (CIP) regulation, which we mentioned in the previous section.[464] In short, critical infrastructure protection means protecting the vital infrastructure of a region or a nation and being prepared for potential risks such as natural disasters, terrorist acts, and cyber threats.[465] In 2002, the Israeli government commissioned the National Security Council to assess current risks and take measures and drafted Special Resolution B/84 to secure all computer-based systems in Israel.[466] With this resolution, cybersecurity policies in Israel began to gain meaningful coherence. This resolution was one of the first in the world for its time. According to the definition of the resolution, computer systems were recognized as physical entities, not virtual environments. This did not meet the concept of cyberspace, which is confusing concept even today. A controlling committee was established, which included members from the following departments: NSC (the presidency), senior government officials, representatives of the Bank of Israel, and representatives from the defense establishment. Resolution B/84[467] , which gives users of computer systems the right to appeal decisions to the Knesset, guides users on the following eight issues: [468]

1. Periodic identification of threats
2. Informing the committee to identify and regulate critical infrastructure systems
3. Determining appropriate defense strategies for these systems

[463] ibid.
[464] ibid 38.
[465] RS Radvanovsky and A McDougall, *Critical Infrastructure: Homeland Security and Emergency Preparedness, Fourth Edition* (Taylor & Francis 2021) 4.
[466] Tabansky and Ben Israel (n 35) 35–36.
[467] ibid 36.
[468] ibid 36–37.

4. Integrating information from defense units and private companies into this protection system
5. Providing professional training
6. Determination of standards and operating procedures for the protection of critical infrastructures
7. Establishment of cooperation with allies in Israel and abroad and the study of expertise in high technology
8. Supporting research studies on the subject
9.

With this special decision, the National Information Security Authority (NISA or Re'em) was established, and the implementation of CIP tasks was transferred to this unit. This unit was established under the Shin Bet (Israel's domestic intelligence service).[469]

4.13.3. Government Resolution 3611 and Israeli National Cyber Bureau (INCB)

Resolution 3611, passed in 2011, is Israel's first comprehensive cybersecurity initiative since Special Resolution B/84. This Israeli government resolution is designed to capture global cybersecurity trends and strengthen Israel's position.[470] The main motivations include the development of high-level cybersecurity technologies and their adoption by relevant organizations, as well as creating innovative solutions for Israel's security challenges in the technology field. In addition, the decision aims to develop strategies to eliminate threats to national security and critical infrastructure systems.[471] The Israeli National Cyber Bureau (INCB) was established with this decision. This bureau is tasked with coordinating cyber security efforts in Israel, advising the government on security issues, and promoting research and development in this field. Another significant emphasis of this resolution is inclusiveness. It is an accepted fact that cybersecurity does not only involve state organizations. It aims to include private companies, academia, and organizations in need of cybersecurity in the understanding of cybersecurity.[472] Thus, with a comprehensive approach, not only the technical aspects of cybersecurity but also its social and legal outputs were included in the studies. As a result of INCB's work, two new legal regulations have

[469] Frei (n 38) 10.
[470] ibid.
[471] Tabansky and Ben Israel (n 35) 50–51.
[472] Frei (n 38) 18.

emerged. Government Decisions No. 2443 and 2444 established the legal basis for cybersecurity strategies.

4.13.4. Government Resolution 2443 - National Cyber Security Authority (NCSA)

Decision 2443, issued in 2015, is an improved version of Decision 3611.[473] As with the other two resolutions, the main element of this resolution is the protection of critical infrastructure systems. Designed to cover the issues of the previous resolution, the first prominent issue in the resolution is the effort to provide legal frameworks in cybersecurity. Arrangements have been made to ensure flexibility and compatibility between freedom, privacy, and civil rights, as well as the provision of cybersecurity. In addition, guidelines have been issued to guide institutions and organizations operating in cybersecurity. It aims to provide cybersecurity support to small and medium-sized enterprises that have problems finding resources and are vulnerable to cyber threats. Since threats also target the private sector, strategies were developed to provide training and resource support. The National Cyber Security Authority (NCSA) was established as a new unit besides the INCB. This body is envisaged to operate simultaneously with the INCB and is responsible for operational matters. NCSA's role is to be the main center of Israel's cyber security strategy. It is intended to provide overarching coordination. NCSA took over the protection of critical infrastructure from the Shin Bet and established CERT-IL (Computer Emergency Response Team - Israel).[474]

CERT-IL was established to respond to cyber security incidents and manage units at the national level in Israel. CERT-IL, under the NSCA, protects against cyber threats in cooperation with various institutions. CERT-IL is the first defense unit against attacks that threaten national security.[475]

4.13.5. Government Resolution 2444

With this decision, the NSCA was given the task of creating a National Cyber Security Doctrine in cyber security. This decision was issued in 2015. This doctrine is expected to prepare guiding statements and directives in the fields of international

[473] ibid 10.
[474] Tabansky and Ben Israel (n 35) 58–59.
[475] Frei (n 38) 11.

cooperation, public disclosure, licensing, auditing, and training. There is also an effort to raise public awareness.[476]

4.13.6. Government Resolution 3270

In 2018, the Israeli National Cyber Directorate (INCD) was established with this decision. The INCD merged and incorporated the previously established INCB and NCSA. INCD is at the center of the cyber security structure in the civilian sphere.[477] It reports directly to the Prime Minister's Office. It is authorized with the following tasks[478] :

1- Raising Israel's robustness in cyberspace and protecting critical infrastructure
2- Implementing and organizing national cyber security strategies
3- Ensuring international cooperation and making legal arrangements in this regard
4- Ensuring peacetime cyber defense management
5- Cooperation with the Israel Police and the Ministry of Justice
6- Cooperation with defense agencies such as Shin Bet, Mossad, and IDF to strengthen cyber security

4.13.7. IDF and Cyber Security

Cyber warfare can be strategically advantageous if less costly and lethal than physical or kinetic warfare. In Israel's overall understanding of national security, cyber warfare fits into Israel's strategy. It is possible to cover the quantitatively deficient defense areas with a qualitatively better cyber weapon.[479] The IDF's Air Force, C4I Corps, and Intelligence units have long adapted information technology to their operations. In 2009, Major General Amos Yadlin, Director of Military Intelligence in the IDF, stated that cyber warfare methods are better suited to their strategy and are important for young Israeli citizens.[480] Israel's military strategy is based on a qualitative advantage over its adversaries. This necessitates keeping pace with technological and scientific developments. According to Tabansky and Ben-Israil, the Israel Defense Forces have matured in cyber attack, defense, and deterrence.[481] However,

[476] Tabansky and Ben Israel (n 35) 59.
[477] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy' (n 36) 120.
[478] Frei (n 38) 14.
[479] Tabansky and Ben Israel (n 35) 63.
[480] ibid 64.
[481] ibid 64–65.

cybersecurity should be addressed at the national level, not only in the military sphere but also in the civilian sphere. The IDF's 8200 Unit works for offensive operations, while the C4I Directorate works defensively.

4.13.8. C4I

The C4I Directorate is responsible for Israel's cyber defense operations and the IDF's critical infrastructure security. The C4I Directorate cooperates with other key organizations such as the Shin Bet, Mossad, Israel Police, and the Ministry of Justice.[482] These collaborations are coordinated by the Israel National Cyber Directorate (INCD). It is responsible for the defense of the country's critical infrastructure in times of war and emergency.[483] The C4I cyber defense approach has recently been renewed as an active defense. This active defense approach includes deterring attacks. This approach is aligned with Israel's national defense doctrine. The C4I Directorate has established a center that integrates both the computer division and military intelligence forces.[484] Cyber defense (C4I) took a more offensive direction and remained separate from Unit 8200. It shows the relation between Israel's state actors in the field of cybersecurity.

[482] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy' (n 36) 120.
[483] ibid.
[484] 'C4I and Cyber Defense Directorate' (*IDF*) <https://www.idf.il/en/mini-sites/directorates/c4i-and-cyber-defense-directorate/c4i-and-cyber-defense-directorate/> accessed 20 June 2024.

Figure 12. Hierarchical Relationship Between Israeli State Organs in Cyberspace[485]

4.13.9. Unit 8200

Unit 8200 has remained a secret unit until today. It came to light in Dan Senor and Saul Singer's 2009 book "Start-Up Nation: The Story of Israel's Economic Miracle," which was the first time the unit was publicized.[486] It originates in a secret intelligence gathering agency called NILI, which operated during the British Mandate of Palestine. After Israel gained independence, the signals intelligence unit SIGINT was established and continued its work.[487] After the 1973 Yom Kippur War, Unit 8200 was restructured and began R&D activities. The unit produces innovative solutions and inventions for operations and is characterized by human resources and information processing.[488] Claimed to cooperate closely with Israel's high-tech community, the unit is also active in cyber security. The operations attributed to and associated with Unit 8200 are listed below in Table 6.

[485] Tabansky and Ben Israel (n 35).
[486] Cordey (n 39) 4.
[487] ibid 5.
[488] ibid 6.

Table 6. Operations associated with Unit 8200 (Adapted from The Israeli Unit 8200)[489]

Operation Name	Content
Stuxnet (2005-2010)	According to Sanger, Stuxnet was a joint operation between Unit 8200 and the NSA in the US.
Operation Orchard (2007)	Unit 8200 disrupted Syria's radar systems, enabling an airstrike on a facility in Deir ez-Zor.
Operation Full Disclosure (2014)	Israeli operation on a ship allegedly carrying weapons to Hamas
Ogero Case (2017)	According to the Lebanese government, Israel carried out a cyber attack on the telecommunications company Ogero.
Prevention of ISIS Terrorism Plan (2018)	Israel detected and intercepted a civilian airliner from Australia to the UAE that was targeted in an ISIS terrorist attack.
Flame (2007-2012)	Malicious software created against Iran
Duqu (2009-2011)	Multi-layered and multi-stage malware targeting industrial systems in several countries. According to Kaspersky, this malware shared the same platform as Stuxnet.
Gauss (2011-2012)	A tool for cyber intelligence on Lebanon and Palestine
miniFlame (2012)	Cyber espionage software
Duqu 2.0 (2014 - 2015)	Cyber espionage software targeting the negotiations on the P5+1 Iran Nuclear Deal.

[489] Cordey (n 39).

4.14. Non-State Actors of Israel Cybersecurity

Until this chapter, the background of Israel's cybersecurity success, strategies, and state actors have been analyzed. The framework of cybersecurity for the state of Israel has been drawn with the authorities and institutions established by the state of Israel with special resolutions and government decisions. In this section, where we will discuss the non-state actors in Israel, the issue of Israel being a start-up nation will be addressed. Although Israel's cyber defense, attack, and security units were mentioned in the previous section, cyberspace is not only composed of state actors. Actors such as individual users, companies, terrorist groups, and white hacker groups are also involved in cyberspace.[490] For example, the Pegasus spyware software created by the Israel-based technology company NSO Group could access personal and confidential information on the devices of the people it targeted by clicking on links sent to their phones.[491] This cyber espionage carried out by this group is a non-state actor issue. Again, many companies emerging from Israel's innovation economy in cybersecurity and information technologies strengthen Israel's cybersecurity ecosystem. After analyzing these non-state actors, cyberspace activities associated with Israel will be analyzed.

4.14.1. Israeli Cyber Security Companies

Israel is called a “start-up nation” because it is a hub for innovative technologies and is home to companies that create cutting-edge technological products.[492] Non-state actors are also important in Israel's national defense approach. The Israeli state has specifically supported this innovation economy through R&D investments, special incentives, and public-private partnerships. Israel's highly skilled workforce is specialized in technology and cyber security. Universities and research institutions have a stake in cybersecurity R&D investments.[493] Graduates of military programs such as the Academic Reserve can establish successful start-ups with their experience and network in this field.[494] Another prominent

[490] KÖKSOY (n 221) 8–10.

[491] JD Rudie and others, ‘Technical Analysis of the NSO Group’s Pegasus Spyware’, *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (2021) 747 <https://ieeexplore.ieee.org/document/9799180> accessed 24 June 2024.

[492] Frei (n 38) 13.

[493] Tabansky and Ben Israel (n 35) 15–18.

[494] Baram and Ben-Israel (n 169) 76.

feature of Israeli companies is their importance in cooperating with global partners. Technology giants such as Google and Microsoft open branches in Israel, while Israeli companies are listed on American stock exchanges.[495] Public authorities responsible for cyber security, such as INCD, examine national cyber security efforts and formulate the necessary policies. Military units such as Unit 8200 partner with Israeli companies and support them during the incubation period.[496] In this way, Technology Transfer takes place, and the cyber security ecosystem develops simultaneously in the private and public spheres. Israeli cyber security companies also contribute to the Israeli economy by exporting the high-tech products and solutions they produce.[497]

4.14.2. Overview of Israel's Cyber Security Sector

According to Startup Nation Central[498] , the total value of Israeli technology companies in 2023 reached 7.5 billion dollars. Of this amount, 51 percent, or $3.8 billion, belongs to cybersecurity companies. Israel already has over 450 startups and companies.[499] In 2018, Israel is known to have received approximately 20% of global cybersecurity investments.[500] The table below shows the most valuable cybersecurity companies, their fields of endeavor, estimated market capitalization, and the US stock exchanges where they are listed.

[495] Tabansky and Ben Israel (n 35) 22.

[496] Cordey (n 39) 12.

[497] Tabansky (n 33) 112–113.

[498] 'Startup Nation Finder - Explore the Israeli Tech Ecosystem' <https://finder.startupnationcentral.org/?_gl=1*1r1hef8*_gcl_au*MTI4MjgxODY2NS4xNzE4ODgxNDU5*_ga*MTgyMzE2NjIxNS4xNzE4ODgxNDYw*_ga_XR55W56KTR*MTcxOTI2OTQ0MS41LjEuMTcxOTI2OTQ1MS41MC4wLjA.> accessed 25 June 2024.

[499] Corinne Berzon, 'Cybersecurity in Israel: Leading the World to a Safer Digital Future' (*Startup Nation Central*, 6 May 2024) <https://startupnationcentral.org/blog/cybersecurity/cybersecurity-in-israel/> accessed 25 June 2024.

[500] 'Israeli Cyber Investments Exceed $1 Billion for First Time in 2018' (*The Jerusalem Post | JPost.com*, 28 January 2019) <https://www.jpost.com/israel-news/investment-in-israeli-cyber-exceeds-1-billion-for-first-time-in-2018-578906> accessed 25 June 2024.

Table 7. Israeli IT and Cybersecurity Companies

Company Name	Description	Headquarters	Market Value (Year)	US Market Listed
Check Point Software Technologies	Network cybersecurity solutions provider	Tel Aviv	$15.98B[501]	(NASDAQ: CHKP)
CyberArk Software	Privileged access security	Petah Tikva	$10.77B	(NASDAQ: CYBR)
Radware	Cybersecurity and application delivery solutions	Tel Aviv	$1.03B [502]	(NASDAQ: RDWR)
Varonis Systems	Data security and analytics	Herzliya	$4.83B [503]	(NASDAQ: VRNS)
Alarum Technologies Ltd. (Safe-T Group)	Zero-trust access solutions	Herzliya	$193M [504]	(NASDAQ: SFET)
Snyk	Vulnerability scanning and security for code and containers	Tel Aviv	$7.4B [505]	
Aqua Security	Cloud-native security for containers and serverless architectures	Ramat Gan	$1B [506]	
Wiz	Cloud security platform	Tel Aviv	$10B [507]	
Cato Networks	Secure access service edge (SASE) solutions	Tel Aviv	$3.0B [508]	

[501] 'Check Point Software (CHKP) Market Cap & Net Worth' (*Stock Analysis*) <https://stockanalysis.com/stocks/chkp/market-cap/> accessed 25 June 2024.

[502] 'Radware Ltd. (RDWR) Statistics & Valuation Metrics' (*Stock Analysis*) <https://stockanalysis.com/stocks/rdwr/statistics/> accessed 25 June 2024.

[503] 'Varonis Systems (VRNS) Market Cap & Net Worth' (*Stock Analysis*) <https://stockanalysis.com/stocks/vrns/market-cap/> accessed 25 June 2024.

[504] 'Alarum Technologies Stock Price Today (NASDAQ: ALAR) Quote, Market Cap, Chart | WallStreetZen' <https://www.wallstreetzen.com/stocks/us/nasdaq/alar> accessed 25 June 2024.

[505] 'Snyk Closes $196.5 Million Series G Funding at $7.4 Billion Valuation' (*Snyk*, 12 December 2022) <https://snyk.io/news/snyk-closes-196-5-million-series-g-funding-at-7-4-billion-valuation/> accessed 25 June 2024.

[506] 'Aqua Security Closes $60M Additional Funding at a Valuation Above $1B' (*Aqua*) <https://www.aquasec.com/news/60m-additional-funding/> accessed 25 June 2024.

[507] 'Unstoppable Wiz: Cyber Startup Nets Another $1 Billion in Funding as Valuation Jumps to $12B' (*ctech*, 7 May 2024) <https://www.calcalistech.com/ctechnews/article/rjs3pupf0> accessed 25 June 2024.

[508] 'Cato Networks Raises $238M in Equity Investment at Over $3B Valuation | Cato Networks' <https://www.catonetworks.com/news/cato-networks-raises-238m-in-equity-investment-at-over-3b-valuation/> accessed 25 June 2024.

5. CYBER OPERATIONS AND STATE RESPONSBILITY

In this section, the actions of state and non-state actors in cyberspace will be evaluated in the context of state responsibility. The diversity of actors in cyberspace has already been mentioned. In cyberspace, states, groups, and individuals can be actors and take action. These actions can be legal or illegal, such as cyber-attacks, deterrence measures, cyber wars, and cyber espionage. The Stuxnet attack, the cyber-attack on Estonia, and military operations such as Operation Orchard are among the most high-profile actions in cyberspace. This section will analyze and evaluate the Israeli-based non-state actor in cyberwarfare. NSO Group and the Pegasus spyware attributed to it in the context of state responsibility law.

5.1.Cyber Operations and International Law

A cyber operation refers to actions taken in cyberspace to interfere with, damage, or access computer networks.[509] Cyber operations include espionage, data breach, disruption of services, and damage or manipulation of critical infrastructure systems. A cyber attack is a malicious act carried out through cyberspace that threatens information security, confidentiality, integrity, and availability. These attacks can range from small-scale phishing attacks to large-scale attacks with various political and economic objectives, such as gaining unauthorized access to sensitive information, disrupting or destroying IT infrastructure, and physically damaging industrial systems.[510] There is no agreed definition of the term cyber-attack in the context of international law.[511]

The assessment of cyber-attacks in international law is complex. In particular, the fact that cyberspace differs from the physical world by nature makes it challenging to understand and interpret the event with the concepts of the physical world. In international law, "use of force" refers to the use of military force by one state against another state. According to Article 2(4) of the UN Charter, states may not use force against each other.[512]

[509] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 417.
[510] Nath (n 231) 1.
[511] Waxman (n 46) 433–434.
[512] United Nations, "Charter of the United Nations," Article 2(4)

The article explicitly prohibits the use of force. There is a historical difference between international law and cyberspace. International law was shaped before the emergence of cyberspace. However, cyberspace has been developing very rapidly in the last 30 years. Therefore, international law has traditionally been applied to concrete and physical conflicts.[513] The nature of cyberspace makes it challenging to consider cyber operations as a use of force under international law.

According to E. Yılmaz, while the rules of international law can provide a framework for analyzing state behavior in cyberspace, applying these rules is fraught with uncertainties.[514] In the case of the Stuxnet attack described in the previous section, technical investigations revealed evidence that the virus was carried out jointly by the US' NSA and Israel's Unit 8200. Still, this evidence was insufficient to attribute the incident to the aforementioned states.[515] According to Deleure, if it could be proven that a state was behind Stuxnet, it could be considered an unlawful intervention.[516] In order to determine whether a cyber operation violates the rule prohibiting the use of force, the operation's urgency, severity, and military characteristics should also be examined.[517] According to Ecemiş, if a cyber operation seriously interferes with the sovereignty and independence of a state, it may be considered a prohibited use of force under Article 2(4) of the UN. The Tallinn Manual states the matter as follows: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[518] In other words, in evaluating a cyber operation as a use of force, he utilizes the definitions of the traditional use of force. Waxman, on the other hand, stated that it is not enough to examine only technologies and tools in terms of the law of cyber attacks; changing and evolving interests, capacities and vulnerabilities, in short, the strategies of actors in this field are also essential.[519] He also believes it is difficult to agree on a definition of cyber attacks in terms of legal interpretation and impose this definition on other states.[520] Deleure, on the other hand, states that cyber operations are within the scope of prohibiting the use of force. However, he adds that not all cyber operations can be defined as the use of force. For

[513] Ecemiş Yılmaz (n 51) 24.
[514] ibid 25.
[515] Lindsay (n 345) 365.
[516] Delerue (n 45) 12.
[517] Ecemiş Yılmaz (n 51) 88.
[518] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 330.
[519] Waxman (n 46) 425.
[520] ibid 426.

Deleure, cyber operations must cause physical destruction or death in order to fulfill this condition.[521]

While Article 2(4) of the UN Charter prohibits the use of force, Article 51 grants states the right of self-defense in the event of an armed attack.[522] However, the term "armed attack" is not entirely clear. According to this article, an armed attack must have occurred for the right to self-defense. In order to exercise the right to self-defense, it is important to identify the actor behind the armed attack and the timing of the attack.[523] It is not correct to say that the aggressor always fires first. An action to prevent an operation to attack itself can also be considered as self-defense.[524] Self-defense must be based on the principles of proportionality and necessity. It should not include motivations such as revenge or retaliation.[525]

Schmit argues that for a cyber attack to be considered an armed attack in the traditional sense, it must have a certain gravity; Robertson argues that a cyber attack can be viewed as an armed attack if it causes extensive damage to military and civilian networks, death or physical harm.[526] . Scientifically, there are three views on when a cyber attack is considered an armed attack and gives rise to the right to armed self-defense: "'means-based approach,' 'target-based approach,' and 'effects-based approach.'" [527]

5.2.Non-State Actors and International Law

States may indirectly or directly conduct cyber operations or implicitly encourage actors. It becomes more difficult to detect law violations for non-state actors' operations in cyberspace.[528] It is difficult to understand whether the interests and motivations of non-state actors are directly behind the attacks or whether they are encouraged and supported by states. According to Schmitt, for an operation by non-state actors to be attributed to a state, the

[521] Delerue (n 45) 9.

[522] United Nations, "Charter of the United Nations," Article 51

[523] Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn, Cambridge University Press 2017) 205 <https://www.cambridge.org/core/product/267F637971002C839A8AB472DD0CDB8B>.

[524] Ecemiş Yılmaz (n 51) 93.

[525] ibid 98.

[526] Horace Robertson, 'Self-Defense against Computer Network Attack under International Law' (2002) 76 International Law Studies 121 <https://digital-commons.usnwc.edu/ils/vol76/iss1/19>.

[527] Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) null Public International Law eJournal null, 845.

[528] Ecemiş Yılmaz (n 51) 132.

following conditions must be met: the operation by non-state actors must be carried out under the instructions, direction, or control of a nation-state, or the state must officially acknowledge that it carried out the operation.[529] International law's regulation of cyber operations by non-state actors is limited. According to the International Group of Experts, a cyber operation conducted by a non-state actor violates the law of the state from which it was launched (such as the prohibition on the use of force). [530]

5.3.Attribution and Burden of Proof

Determining responsibility for cyber attacks is difficult due to the nature of cyberspace. If a state is directly or indirectly involved in cyber operations, this is where legal norms come into play.[531] For a state to counterattack a cyber-attack directed against it within the scope of self-defense, it must first identify the attack's origin. For an unlawful act to give rise to responsibility under international law, the act must be legally attributable to a state.[532] For a cyber operation to be clearly attributable to a state, that state must undertake the operation. However, this is unlikely due to the secrecy of the operations and the closed nature of cyberspace.[533] Although the actors conducting cyber operations can take precautions to prevent who is carrying out the operation, attribution is not made only through technical tracking. In addition to technical dimensions, there are also legal and political dimensions.[534] Apart from these determinations, the extent to which states are involved in an operation is also important. [535]

Cyber operations are fast, anonymous, and deceptive, making it challenging to identify the actor responsible for the operation and its relationship with states. Some states may use non-state actors as proxies, further complicating the attribution problem.[536] In addition, a specialized actor may carry out attacks using the networks of another state, and these attacks may cause legal problems for that state.[537] The attribution of an operation requires a technical team. It requires the work of a team of experts in different fields. In line

[529] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 95.
[530] ibid 174–175.
[531] Ecemiş Yılmaz (n 51) 110.
[532] Finlay and Payne (n 47) 202.
[533] Roscini (n 48) 39.
[534] Tsagourias (n 49) 233–234.
[535] Ecemiş Yılmaz (n 51) 110.
[536] ibid 111.
[537] Rid and Buchanan (n 50) 5.

with the findings of the technical teams, teams examining the non-technical aspects of the incident evaluate the outputs and try to reach a conclusion.[538] Another problem in the attribution of cyber operations is evidence and proof.[539] In cyberspace, evidence is collected through technical examinations.[540] However, due to the nature of cyberspace, the process of gathering evidence is complex and challenging.

In law, the concept of "burden of proof" refers to the responsibility of a party to produce evidence to support its claims and propositions.[541] The occurrence of a cyber-attack, which would be considered an armed attack, does not mean that self-defense is required. The victim state of an armed attack must prove that it has no choice but to defend itself with arms.[542] According to Tsagourias, the issue of attribution is very delicate,[543] and when a cyber operation is attributed to a state, evidence of a link between the guilty act and the accused state must be brought.[544] Lindsay argues that attackers are likely to make mistakes that expose them if they conduct sophisticated attacks[545], but the nature of cyberspace means that evidence can be difficult to gather.[546]

Evidence in cyberspace varies according to the type of operation and the platforms and tools used. This evidence is classified according to its form, nature, and source. IP addresses, data logs, and malware analysis can be used as evidence to identify those responsible for a cyber operation. [547]

As a result, conclusive evidence is needed to establish that a state is behind a cyber-attack. The only way for a state to be held responsible for an attack is to make a legal attribution with conclusive evidence. According to Ecemiş, if a state is not found responsible for a cyber operation, the benefits of the operation may increase disproportionately. Due to the structure of international law and the nature of cyber operations, states do not often face a deterrent against these attacks.[548]

---

[538] ibid 6–13.
[539] Ecemiş Yılmaz (n 51) 117.
[540] ibid 112.
[541] ibid 119.
[542] Mehmet Yayla, 'Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma' [2013] Türkiye Barolar Birliği Dergisi 199, 216.
[543] Tsagourias (n 49) 233.
[544] ibid 235.
[545] Lindsay (n 345) 55.
[546] ibid 53.
[547] Susan Brenner and Leo Clarke, 'Civilians in Cyberwarfare: Conscripts' (2010) 43 Vanderbilt Journal of Transnational Law 1011, 1070.
[548] Ecemiş Yılmaz (n 51) 130.

5.4.Prohibition on Use of Force and Related Cases

5.4.1. Responsibility Of States

International law is state-centered, and the most fundamental right of states is to protect their sovereignty. These rights granted to states are reinforced by the obligation of states to respect these rights. These obligations were published in the UN's 2001 document "Articles on State Responsibility for Violations of International Law." These articles do not constitute a binding treaty. It is a guide in international law.[549] International law imposes a responsibility on states, and this responsibility is that international law should not be violated, and if it is violated, it will create an obligation on the state that commits the violation. Ecemiş explained the concept of compliance as the obligation of states to abide by the rules and norms established by international law.[550] According to Crawford, state responsibility refers to the legal principles of how and when a state is held responsible for a given violation.[551] The first article of the Articles on State Responsibility for Internationally Wrongful Acts reads as follows*: "Every internationally wrongful act of a State entails the international responsibility of that State."*[552] This rule is one of the fundamental principles of international law, and it is a consequence of having rights, which in turn leads to having responsibilities.[553] This is a consequence of natural law. [554]

The second article reads as follows: ***"****There is an internationally wrongful act of a State when conduct consisting of an action or omission:is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."*[555]

Under this article, a violation must be attributable to a state for it to occur under international law. In addition, the failure of a state to stop or attempt to control the act during the commission of a violation also gives rise to responsibility for that violation.[556]

---

[549] G Von Glahn and JL Taulbee, *Law Among Nations: An Introduction to Public International Law* (Routledge 2017) 334–335 <https://books.google.com.tr/books?id=lok2vgAACAAJ>.

[550] Ecemiş Yılmaz (n 51) 143; Yücel Acer and İbrahim Kaya, *Uluslararası Hukuk Temel Ders Kitabı* (13th edn, Seçkin Yayıncılık 2022) 407–408.

[551] James Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013) 7 <https://www.cambridge.org/core/books/state-responsibility/EE846D9378B83A9DCC5E794FC086B07E> accessed 24 June 2024.

[552] Draft Articles on Responsibility of States for Internationally Wrongful Acts," Article 1, 2001

[553] Acer and Kaya (n 553) 408.

[554] Ecemiş Yılmaz (n 51) 136.

[555] Draft Articles on Responsibility of States for Internationally Wrongful Acts," Article 2, 2001

[556] Ecemiş Yılmaz (n 51) 141.

The third article states that:

"The characterization of an act of a State as internationally wrongful is governed by international law. Such characterization is not affected by the characterization of the same act as lawful by domestic law."

This article states that international law prevails over national law, and the existence of provisions in national law that pave the way for actions does not eliminate the state's responsibility.[557] National law cannot be used as an excuse for violations of international law.[558]

5.4.2. Reasons Eliminating Wrongful Acts

There are six reasons that can elımınate the wrongfulness of a state's actıons: consent, self-defense, countermeasures, necessity, force majeure, and distress.[559] The first of these, consent, is addressed in Article 20 of the Articles on State Responsibility for Acts Contrary to International Law[560] under the heading "consent":

"Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act about the former State to the extent that the act remains within the limits of that consent."

If a state consents to an action by another state that would generally constitute a violation of international law, this does not create responsibility for states. However, the action must not exceed the limits of consent.[561]

Another reason is the right to self-defense. As mentioned in the previous section, the right of self-defense is the right of a state to defend itself against an armed attack by another state and is regulated in Article 51 of the UN Charter. A state's self-defense by resorting to self-defense does not allow that state to violate international law.[562] The right to self-defense

[557] Von Glahn and Taulbee (n 552) 334–335.
[558] Ecemiş Yılmaz (n 51) 141.
[559] Acer and Kaya (n 553) 415.
[560] Draft Articles on Responsibility of States for Internationally Wrongful Acts," Article 20, 2001
[561] Acer and Kaya (n 553) 415.
[562] Ecemiş Yılmaz (n 51) 157.

is stated in Article 21 of the Articles on State Responsibility for Acts Contrary to International Law as follows[563] :

"The wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defense taken in conformity with the Charter of the United Nations."

The Article clearly states that the right to self-defense must be realized in accordance with the UN Charter.

The third reason is countermeasures. Countermeasures are measures that states can resort to when they violate the obligations they have undertaken to each other in the context of agreements under international law.[564] For a state to resort to countermeasures, the violation must be a violation of international law; that is, this action must be contrary to international law.[565] The article on the application of countermeasures is as follows[566] :

"The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of part three."

Another reason that eliminates illegality is considered as force majeure. Force majeure can be defined as a situation that is beyond the control of the state, prevents the fulfillment of the obligation imposed by international law, and is physically irresistible or in no way foreseeable.[567] Article 23 on force majeure is as follows[568] :

"The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the act is due to force majeure, that is, the occurrence of an irresistible force or an unforeseen event, beyond the control of the State, making it materially impossible in the circumstances to perform the obligation. Paragraph 1 does not apply if: (a) the situation of force majeure is due, either alone or in combination with other

[563] Draft Articles on Responsibility of States for Internationally Wrongful Acts," Article 21, 2001
[564] Ecemiş Yılmaz (n 51) 160.
[565] ibid.
[566] Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 22, 2001
[567] Acer and Kaya (n 553) 415.
[568] Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 23, 2001

factors, to the conduct of the State invoking it, or (b) the State has assumed the risk of that situation occurring."

Another reason that eliminates illegality is distress. If a state has to violate the law as a last resort to protect the lives of its citizens or people entrusted to its care in case of danger, this situation does not impose an obligation on that state.[569] What distinguishes the concept of distress from necessity is that human life is in danger.[570] Article 24 on this subject states the following[571] : "*1. The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the author of the act in question has no other reasonable way, in a situation of distress, of saving the author's life or the lives of other persons entrusted to the author's care. Paragraph 1 does not apply if (a) the situation of distress is due, either alone or in combination with other factors, to the conduct of the State invoking it, or (b) the act in question is likely to create a comparable or greater peril."*

Finally, the state of necessity also prevents responsibility for violations of international law. Ecemiş defines a state of necessity as a situation where a state acts to protect an important interest, but has no alternative option in the face of a severe and imminent danger.[572] However, he also states that if the state in question has a role or contribution to the emergence of this state of necessity, this will eliminate the state of necessity.[573] The article on the state of necessity states the following[574] :

"Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole. 2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if (a) the international obligation in question excludes the possibility of invoking necessity or (b) the State has contributed to the situation of necessity."

[569] Acer and Kaya (n 553) 415.
[570] Ecemiş Yılmaz (n 51) 162.
[571] Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 24, 2001
[572] Ecemiş Yılmaz (n 51) 163.
[573] ibid.
[574][574] Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 25, 2001

5.4.3. Cyber Operations And State Responsibility

In cyberspace, state and non-state actors coexist, and these actors can act lawfully or unlawfully. The conduct of cyber operations by states can also be defined as legal or illegal, and cyber actions that violate international law can create responsibility for the state that carries out the operation. According to the Tallinn Manual, a cyber operation may violate the sovereignty of another state, the prohibition of intervention, and the prohibition of the use of force.[575] If a cyber tool is used for coercive actions, it may violate the relevant provisions of the UN Charter.[576] In the context of cyber warfare operations, an act contrary to international law may be a possible violation of the UN Charter, for example, in the form of a coercive action carried out by cyber means or a breach of an obligation arising from the law of armed conflict, for example in the form of a cyber warfare attack against a civilian target. It could also breach peacetime arrangements, which may not necessarily involve a conflict.[577] According to Delibasis, the fact that an act is harmful does not make it directly contrary to international law. For a state to claim damages from another state, the act must be in violation of international law.[578] Again, the legal consequences of such an act may have different legal consequences depending on the nature of the act. [579]

For cyber operations to be attributed to a state, this activity must be carried out directly by the state public, institutions, and authorized persons. Ecemiş stated that in the context of state responsibility, the following three conditions must be met for an act to constitute responsibility for a state: the act must be attributed to the state, the act must be contrary to international law, and there must be no reasons that eliminate the illegality.[580]

Attributing cyber operations to a state is complicated by the nature of cyberspace. Cyberspace is borderless and allows for a high degree of anonymity. Unlike real personas in the physical world, a person in cyberspace can have multiple identities, be anonymous, manage numerous vehicles at the same time, or commit crimes in a way that implicates different actors through the use of masking and VPNs. After a cyber operation, technical

[575] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 4,66,68.
[576] Demetrius Delibasis Fokas and Albert Klein, 'Cyberspace Operations & State Responsibility' (14 July 2019) 7–8 <https://papers.ssrn.com/abstract=3505428> accessed 24 June 2024.
[577] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 30–31.
[578] Delibasis Fokas and Klein (n 579) 8.
[579] Ecemiş Yılmaz (n 51) 174.
[580] ibid 182–183.

examination and detailed analysis are critical. For the incident to be legally examined, the technical aspects must first be analyzed, and evidence must be obtained. One of the biggest problems in attributing a cyber operation to a state is that it is difficult to reach a definitive conclusion due to the investigations. It is often difficult to understand when a cyber operation was detected, how widespread it was, and what kind of damage it caused.[581] It is also essential to comprehend cyber operations' methods, means, and objectives. A cyber operation may not cause the intended damage or may cause more harm than the intended effect. The actors designing the malware may also develop techniques that make it difficult to trace. These characteristics pose difficulties in the attribution of cyber operations.[582] There are two main challenges in the attribution of cyber operations. The first one is the risk of misattribution of cyber operations. A cyber operation carries the risk of being misattributed for the reasons and manipulations mentioned above. The other is the difficulty for the state that thinks that it has been attacked to exercise its right to self-defense due to the long attribution process.[583]

5.4.4. Cyber Operations of Non-State Actors and State Responsibility

The process of attributing a cyber operation to a state is complex and intricate. Cyber operations carried out by states or actors authorized by states are attributed to states if proven.[584] Rule 15 of the Tallinn Manual states in this regard[585] : **"***Attribution to a State occurs in several circumstances. The clearest case is when State organs, such as the military or intelligence agencies, commit wrongful acts.138 For instance, all cyber activities of the US Cyber Command, the Netherlands Defense Cyber Command, the French Network and Information Security Agency (ANSSI), the Estonian Defense League's Cyber Unit, the People's Liberation Army cyber unit, and Israel's Unit 8200 are fully attributable to the respective States."* . At this point, the Tallinn Manual stated that cyber operations conducted by different wings of the state would be attributed to the state.

Cyber operations are not always carried out by states. Individuals, groups, or companies can carry out these operations. In this case, the operation can be attributed to a

[581] ibid 183–184.
[582] ibid 184.
[583] ibid.
[584] ibid 185.
[585] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 15.

state under certain conditions. If the non-state actor is authorized by the state, then the operation can be attributed to the state. If non-state actors cross the boundaries of what states have authorized them to do, states are held responsible for violations of international law.[586] For example, Schmitt says that if a company authorized by a state for cyber defense exceeds its authorization and goes into active defense, these actions can also be attributed to the state.[587] For another example, if a company authorized by the state uses different servers in order to fulfill the task assigned to it by going beyond the facilities provided to it, the violation that will arise from this situation can also be attributed to the state.[588]

For a cyber operation to give rise to responsibility for a state, it must be attributed to the state. However, if it is a non-state actor, certain conditions must be met for the operation to be attributed to the state.[589] Unless there is clear evidence that a cyber operation can be attributed to a state, such attribution is not valid under international law. [590]

In Schmitt's Talinn Manual, the first requirement for a cyber operation by a non-state actor to be attributed to a state is the state's direction and control of the actions. If a cyber operation takes place under the direction and control of a state, the violation can be attributed to the state.[591] Secondly, the operation can be attributed to the state if the state adopts the action and accepts it as its own. If a state approves a cyber operation and allows it to continue when it has the capacity to stop it, it can be attributed to the state.[592] However, it is not sufficient for attribution if the state provides incentives and support for a cyber operation. For example, if a state provides software, financing, training to an IT company, this does not make that state directly responsible for the actions of the company. However, if it has control over this company, the actions can be attributed to the state.[593] State control over an operation means that the state has authority over the execution of the operation. Actions that take place outside the aforementioned conditions are considered ultra vires actions, i.e. excess of authority, and cannot be attributed to the state. In the event that a non-state actor tasked with infiltrating another state's network and planting malware on the instructions of a state exceeds its borders and commits an act that harms a third state, the authorized state is not

[586] Ecemiş Yılmaz (n 51) 187.
[587] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 90–91.
[588] ibid.
[589] Ecemiş Yılmaz (n 51) 188.
[590] ibid.
[591] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 94.
[592] ibid 95.
[593] ibid.

held responsible.[594] In conclusion, whether the actions of non-state actors can be attributed to the state should be determined by taking into account the circumstances of each individual case. After this section, the Pegasus spyware of the Israel-based NGO Group will be evaluated in the context of state responsibility.

5.5.Pegasus Spyware and State Responsibility

In the previous section, the actions of state and non-state actors in cyberspace were evaluated in the context of state responsibility. Actors in cyberspace include states, groups and individuals, and they can carry out various actions such as cyber-attacks and cyber espionage. Important cyber-attacks such as Stuxnet, the Estonia attack and Operation Orchard are analyzed.

Cyber operations include actions such as interfering with, damaging or denying access to computer networks. There is no agreed definition of cyber attacks in international law and the nature of cyberspace makes it difficult to understand and interpret events. While Article 2(4) of the UN Charter[595] prohibits states from using force against each other, there is controversy over whether cyber operations should be considered a use of force. Schmitt[596] stated that a cyber operation can be considered as a use of force if it produces effects similar to the traditional use of force. International law is state-centered and it is essential for states to protect their sovereignty. Situations in which states can be held responsible for acts contrary to international law have been determined. Among the reasons that eliminate illegality are consent, self-defense, countermeasures, force majeure, danger, and necessity.

Attribution of cyber operations by non-state actors to the state is complex and the processes of gathering evidence are difficult. According to Tsagourias, for a cyber operation to be attributed to a state, evidence must be brought.

In this chapter, the Pegasus spyware of the Israel-based NSO Group will be analyzed and evaluated in the context of state responsibility. The use of Pegasus software, the possible

[594] ibid 96.
[595] United Nations, "Charter of the United Nations," Article 2(4)
[596] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44).

consequences of states' use of this software and its evaluation in terms of international law will be discussed.

5.5.1. Pegasus Spyware

Pegasus spyware is a highly sophisticated piece of spyware developed by the Israeli-based NSO Group and allegedly used by governments internationally.[597] The target device is Apple's iPhone 6 and other products, while those affected include high-profile people from a wide range of groups, including politicians, journalists and human rights activists.[598] The main purpose of the software is to jailbreak infected devices, transfer personal data from the devices and use the device's hardware such as cameras and microphones without the user's knowledge.[599] To understand how Pegasus software works, we will first look at its technical analysis.

[597] Rudie and others (n 494) 747.

[598] 'Forensic Methodology Report: How to Catch NSO Group's Pegasus' (2021) <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> accessed 24 June 2024.

[599] Bill Marczak and John Scott-Railton, 'The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender' (University of Toronto 2016) Citizen Lab Research Report No. 78 13–14 <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/> accessed 24 June 2024.

Figure 13. Illustration of Pegasus Spyware Target Data Variety[600]

5.5.2. Pegasus Software Overview

In 2016, Ahmed Mansoor, a human rights defender in the UAE, became suspicious about an SMS he received on his phone and contacted CitizenLab, a cybersecurity research organization, to find out what it was. Mansoor was sensitive to the issue as he had been the victim of a cyber attack before. CitizenLab found that the links sent to Mansoor were being accessed and different processes were taking place on the device.[601] As a result of the joint work by Citizen Lab and Lookout Security, two reports were published in 2016 and 2018.[602] According to these reports, it was revealed that Pegasus infects iPhone devices using zero-day vulnerabilities and is a spyware used to remotely monitor these devices. As a result of the technical analysis, it was revealed that the software was owned by the Israel-based NSO Group.[603] After an employee of Amnesty International was exposed to this spyware, a forensic report was published. According to the report, the Pegasus software affected more than 80 journalists from 17 different media organizations. According to reports, the total number of victims is around 50,000 and the Pegasus software operated in 45 countries.[604] They allegedly include 600 politicians, 85 human rights activists and 65 businessmen.[605] In this section, the NSO Group will first be examined, followed by a technical analysis of the Pegasus software in the light of these reports.

5.5.3. NSO Group - Israeli-based CyberWarfare Company

NSO Group, a cyber intelligence company that provides remote access to mobile devices, was founded in Herzliya, Israel in 2010 by three Israeli entrepreneurs, Niv Carmi,

[600] Marczak and Scott-Railton (n 602).
[601] ibid 5–6.
[602] Marczak and Scott-Railton (n 602); Bill Marczak and others, 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (University of Toronto 2018) Citizen Lab Research Report No. 113 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 24 June 2024.
[603] Marczak and Scott-Railton (n 602) 10–11.
[604] Marczak and others (n 605).
[605] ToI Staff, 'NSO Said to Block Some Government Clients from Using Its Spyware' <https://www.timesofisrael.com/nso-said-to-block-some-government-clients-from-using-its-spyware/> accessed 24 June 2024.

Shalev Hulio and Omri Lavie.[606] Shalev Hulio is the CEO of the company. According to a screenshot from the CitizenLab report, which is currently inaccessible, the main goal of the company is as follows[607] :

"NSO Group is a leader in the field of Cyber warfare. The company works with military and homeland security organizations in order to enhance their technological abilities in both the offensive and defensive cyber warfare arenas. NSO Group is backed by large organization and Israeli technology. The company's focus is on the mobile and cellular Cyber Warfare needs, where it now offers state of the art, advanced solutions. Our offering includes coverage of the most popular coverage of the most popular handset Operating Systems, surgical activity monitoring solution exclusively for the use of Government, Law Enforcement and Intelligence Agencies. The system introduces a powerful and unique monitoring tool, called Pegasus, which allows remote and stealth monitoring and full data extraction from remote targets devices via untreceivable commands."

As the company's official publicity makes clear, the company cooperates with governments and promises remote tracking, surveillance and the acquisition of personal data of victims.

It is also alleged that the company has ties with UNIT 8200 and the Mossad. As we have detailed in previous sections, UNIT 8200 is the current version of Israel's SIGINT unit, which was established to collect signals intelligence. UNIT 8200 is the unit responsible for military technologies and cyber security in the IDF. After completing their mandatory military service in Israel, many people have founded and succeeded in security start-ups. [608] Some of the company's employees are known to be former employees of UNIT 8200 and Mossad.[609] In 2014, NSO Group was sold by US-based Francisco Partners for 130 million dollars. It is known that the estimated annual revenues of the company in 2015 were around 150 million dollars. In 2019, founders Shalev Hulio and Omri Lavie bought back the majority stake in the company from Francisco Partners. It is stated that this sale was a sale

[606] 'NSO'nun Perde Arkası: WhatsApp'i Hackleyen Şirket Hakkında Bilmemiz Gerekenler' <https://siberbulten.com/uluslararasi-iliskiler/isrl/nsonun-perde-arkasi-whatsappi-hackleyen-sirket-hakkinda-bilmemiz-gerekenler/> accessed 24 June 2024.

[607] Marczak and Scott-Railton (n 602) 10.

[608] 'NSO'nun Perde Arkası: WhatsApp'i Hackleyen Şirket Hakkında Bilmemiz Gerekenler' (n 609).

[609] Ronen Bergman and Mark Mazzetti, 'The Battle for the World's Most Powerful Cyberweapon' *The New York Times* (28 January 2022) <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html> accessed 24 June 2024.

of 1 billion dollars.[610] Finally, in 2021, the US Department of Commerce blacklisted NSO Group and imposed an export ban on the company. [611]

5.5.4. Government of Israel and NSO Group

The NSO Group is a cybersecurity company that develops technologies for cyber warfare and sells them to governments and security organizations. The most famous product of this company that has caused outrage around the world is the Pegasus cyber espionage product. Since the company is based in Israel and provides digital surveillance of thousands of people from 45 countries, the role of the Israeli government in these sales and operations has been discussed. According to a report by the Council on Foreign Relations, the Israeli government oversees all arms exports and licenses the sales it approves.[612] According to the same report, the Pegasus spyware is also considered a "weapon" and the Israeli Ministry of Defense has admitted to licensing it for export.[613] The Wassenaar Arrangement, a voluntary export control regime on the export and control of dual-use weapons, was established in 1996 with the participation of 42 countries.[614] Although the State of Israel is not a member of this regime, it has been emphasized that it is an implementer of this arrangement. In this context, the Pegasus software can only be used to combat terrorism and prevent serious crimes. However, the fact that the software has been used in many countries for purposes other than the aforementioned purposes and has violated human rights in violation of the law has brought criticism to both the company and Israel.[615]

5.5.5. Infection Methods of Pegasus

Pegasus spyware infiltrates the targeted device in three different ways.

---

[610] 'Novalpina Capital and Founders Buy NSO at $1b Co Value - Globes' <https://en.globes.co.il/en/article-novalpina-capital-and-founders-buy-nso-for-1b-1001273312> accessed 24 June 2024.

[611] David E Sanger and others, 'U.S. Blacklists Israeli Firm NSO Group Over Spyware' *The New York Times* (3 November 2021) <https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html> accessed 24 June 2024.

[612] 'How Israel's Pegasus Spyware Stoked the Surveillance Debate | Council on Foreign Relations' <https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate> accessed 24 June 2024.

[613] ibid.

[614] 'Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary' (*Federal Register*, 5 October 2020) <https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2019> accessed 24 June 2024.

[615] Atul Alexander and Tushar Krishna, 'Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism' (2022) 11 Laws 85, 1–5.

Spear-Pishing Method: The spyware sends fake e-mails or SMS messages to targeted users, aiming to get them to click on the links sent. The message content is designed to attract the attention of the targeted people. The SMS sent to activist Ahmed Mansoor says that he has provided a link with information about the cases he is following. The links usually used the link addresses of sites that people encounter in daily life, such as news websites. This way, the target person would not be aware of a cyber-attack. Once the target person clicks on these links, the process of installing the malware on the device begins. [616]

If the target person clicks on these links, JavaScript code is downloaded to the device via the link. By executing this code, the device is accessed. The code causes a corruption in the Webkit Browser engine, the engine of the Safari browser that Apple uses on its devices. [617]

Physical Access to the Device: This is the method in which an agent or official physically accesses the target audience's phone and installs spyware on the device.[618]

Zero-Click Method: Zero-Click method is an attack that is carried out without the targeted user clicking on any link or taking any action, unlike the spear-pishing method. Zero-click attacks exploit zero-day vulnerabilities in cyber systems. In addition to spear-pishing, the Pegasus spyware was also found to use the zero-click method. [619]

Once the Pegasus spyware is transferred to the device in one of these ways, the code exploits a vulnerability in the WebKit browser engine (CVE-2016-4657) to arbitrarily execute code on the device.[620] A zero-day vulnerability in the browser engine is used for the next stage. This allows access to the device's Kernel system, the kernel memory.

[616] Rudie and others (n 494) 748.
[617] Marczak and Scott-Railton (n 602) 16.
[618] Rudie and others (n 494) 748.
[619] Marczak and Scott-Railton (n 602) 12.
[620] ibid 16.

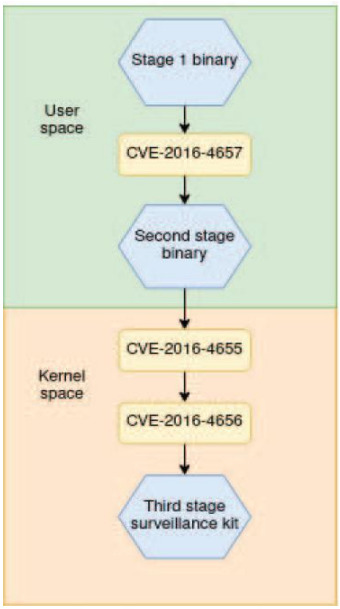

Figure 14. Pegasus Spyware Breach Stages[621]

The kernel is the core of a computer operating system and is the bridge between hardware and software. It is the core component of the operating system. The kernel performs the following tasks on a device: Managing the hardware of the device; managing system resources such as CPU, GPU, and RAM; implementing the security protocols of the device and managing access; and establishing the connection between software and hardware.[622] Kernel addresses represent memory areas in this center. Once the Pegasus software gains access to the Kernel system, it exposes the Kernel addresses and accesses the kernel memory. By targeting the device's kernel memory, Pegasus learns the kernel addresses and bypasses the KASLR (Kernel Address Space Layout Randomization) mechanism. This vulnerability in the Kernel is numbered CVE-2016-4655.[623] Finally, the software exploits CVE-2016-4656,[624] which will cause corruption in the Kernel memory and jailbreak the device.[625] In this way, it injects Pegasus code into the Kernel memory, the main control

[621] Marczak and Scott-Railton (n 602).

[622] 'What Is a Kernel? Types of Kernels - TechTarget.Com' (*Data Center*) <https://www.techtarget.com/searchdatacenter/definition/kernel> accessed 24 June 2024.

[623] Marczak and Scott-Railton (n 602) 17.

[624] CVE, Common Vulnerabilities, and Exposures is a system that lists common vulnerabilities and threats. Each vulnerability is assigned a unique CVE number. These numbers are used to identify and track vulnerabilities.

[625] Marczak and Scott-Railton (n 602) 17.

mechanism of the device, and takes complete control of the device. This process is called the Trident Exploit Chain[626] and consists of exploiting three vulnerabilities as described:

1. CVE-2016-4657: Executing arbitrary code by visiting a malicious website.
2. CVE-2016-4655: Bypassing KASLR by exposing kernel addresses.
3. CVE-2016-4656: Using kernel memory corruption to jailbreak and gain complete device control.

After gaining access to the kernel memory, the Pegasus software provides complete control over the software and hardware tools on the device. Once this control is established, the software allows the device to execute system-level code in Kernel memory. This allows the security protocols defined on the device to be breached, making the software harder to detect. From this point on, Pegasus can collect data and provide complete surveillance. Many surveillance actions are carried out, including acquiring data from all applications on the device (Whatsapp, Viber, Telegram, etc.), especially message applications, emails, and phone calls, and instant tracking of the user's screen.[627] There is also control of the device at the hardware level. The camera and microphone are also tools that Pegasus spyware can access without user authorization. Even if the user is not using the camera or microphone, the software can operate them secretly. The software can track keyboard usage, personal passwords, browser history, and cookies on the device. [628]

The exfiltration of this data is the transfer of the collected data from the device to the actor using the software. All collected data is transmitted to servers controlled by Pegasus, and this process is encrypted and confidential. The collected data is transferred to the Pegasus Data Server via the Pegasus Anonymizing Transmission Network (PATN). Thanks to this network, data is transferred anonymously and securely to the servers. PATN hides the source, content, and destination of the data and thus makes possible disclosure difficult. [629]

5.5.6. Pegasus Spyware and its Global Impact

[626] ibid 6.
[627] Rudie and others (n 494) 750; Marczak and Scott-Railton (n 602) 10.
[628] Marczak and others (n 605) 7.
[629] Marczak and Scott-Railton (n 602) 14.

Since the Pegasus spyware was discovered, studies have shown that it has infected many people in many different countries worldwide, including journalists, academics, human rights activists, members of royal families, high-level politicians, and military officers. We will examine some of the most prominent ones. The first concerns the murder of Jamal Khashoggi. Following the murder of Jamal Khashoggi at the Saudi Arabian Consulate in Turkey in 2018, his close circle is known to have been among the targets of the Pegasus software.[630] Amnesty International reported that Khashoggi's fiancée, Hatice Cengiz, and her close friend, Wadah Khanfar, were monitored.[631] Another example is that this software targeted one of the phone numbers of French President Emmanuel Macron. In addition to Macron, other French government officials are among the victims.[632] The following table lists those affected or thought to be affected by the Pegasus spyware.

[630] Amnesty International Security Lab, 'The Pegasus Project' (2024) <https://securitylab.amnesty.org/case-study-the-pegasus-project/> accessed 7 August 204AD.

[631] 'Forensic Methodology Report: How to Catch NSO Group's Pegasus' (n 601).

[632] 'Pegasus: French President Macron Identified as Spyware Target' <https://www.bbc.com/news/world-europe-57907258> accessed 24 June 2024.

Table 8. Pegasus Spyware Targets[633]

Country	Individual(s) Targeted	Occupation	Country	Individual(s) Targeted	Occupation
Azerbaijan	Khadija Ismayilova, Sevinc Vaqifqizi	Investigative Journalist, Freelance Journalist	**Lebanon**	Lama Fakih	Human Rights Worker
Bahrain	Moosa Abd-Ali, Yusuf al-Jamri, seven rights activists	Activist, Blogger, Human Rights Activists	**Mexico**	Rafael Cabrera, Dr. Simon Barquera, Alejandro Calvillo, Luis Encarnación, Karla Micheel Salas, David Peña, Carmen Aristegui, Emilio Aristegui, Sebastián Barragán, Carlos Loret de Mola, Salvador Camarena, Daniel Lizárraga, Mario E. Patrón, Stephanie Brewer, Santiago Aguirre, Juan Pardinas, Alexandra Zapata, Azam Ahmed, Ricardo Anaya Cortés, Sen. Roberto Gil Zuarth, Fernando	Journalists, Activists, Politicians, Lawyers
El Salvador	Carlos Martínez, Daniel Lizárraga, nine El Faro journalists, other journalists, Noah Bullock, Ricardo Avelar, Jose Marinero, Xenia Hernandez, Oscar Luna, Mariana Belloso, Carmen Tatiana Marroquín	Journalist, Editor, Human Rights Worker	**Morocco**	Hicham Mansouri, Mahjoub Mleiha, Joseph Breham, Oubi Buchraya Bachir, Maati Monjib, Omar Radi, Aboubakr Jamaï, Fouad Abdelmoumni	Journalists, Activists, Lawyer
Finland	Finnish diplomats	Diplomats	**Palestine**	Ghassan Halaika, Ubai Aboudi, Salah Hammouri, three unnamed activists	Human Rights Workers
France	Bruno Delport, Lénaig Bredoux, Edwy Plenel, unnamed France 24 journalist, Claude Mangin, Arnaud Montebourg	Radio Director, Investigative Journalist, Former Minister	**Poland**	Krzysztof Brejza, Roman Giertych, Ewa Wrzosek, Michał Kołodziejczak, Tomasz Szwejgiert	Senator, Lawyer, Prosecutor, Movement Leader, Author
Hungary	Dániel Németh, Zoltán Páva, Adrien Beauduin, Szabolcs Panyi, András Szabó, Brigitta Csikász	Photojournalist, Politician, Student, Journalists	**Rwanda**	Carine Kanimba, Peter Verlinden, Marie Bamutese, Placide Kayumba	Activist, Journalist
India	Jagdeep Singh Randhawa, Mangalam Kesavan Venu, Paranjoy Guha Thakurta, Prashant Kishor, Rona Wilson, Syed Abdul Rahman Geelani, Sushant Singh, S.N.M. Abdi, Bela Bhatia, Siddharth Varadarajan, unnamed legal officer, Ankit Grewal	Lawyer, Editor, Journalist, Political Pollster, Activist	**Saudi Arabia**	Hatice Cengiz, Omar Abdulaziz, Wadah Khanfar, Ragip Soylu, Ben Hubbard	Journalist, Activist, Al Jazeera Director General
Israel	Shai Babad, Avi Berger, Aviram Elad, Iris Elovitch, Keren Terner-Eyal, Shlomo Filber, Miriam Feirberg, Stella Handler, Yair Katz, Rami Levy, Topaz Luk, Dudu Mizrahi, Avner Netanyahu, Emi Palmor, Yaakov Peretz, Moti Sasson, Ilan Yeshua, Jonatan Urich, Walla journalists, protest leaders, extreme settlers	Government Officials, Journalists, Activists	**United States**	11 unnamed U.S. officials	Government Officials
Jordan	Hala Ahed Deeb, Ahmed al-Neimat, Suhair Jaradat, Malik Abu Orabi, anonymous journalist	Lawyer, Activist, Journalist	**United Arab Emirates**	Alaa al-Siddiq, Abdulaziz Alkhamis, Ayman Nour, Rania Dridi, Tamer Almisshal, Ebtisam al-Saegh, 34 Al Jazeera staffers	Human Rights Activists, Journalists
Kazakhstan	Aizat Abilseit, Dimash Alzhanov, Tamina Ospanova, Darkhan Sharipov	Activists	**United Kingdom**	David Haigh, Anas Altikriti	Lawyer, Activist

[633] Amnesty International Security Lab (n 633); 'Forensic Methodology Report: How to Catch NSO Group's Pegasus' (n 601); Marczak and others (n 605).

This figure shows the map of Suspected Pegasus Infections according to the CitizenLab report.

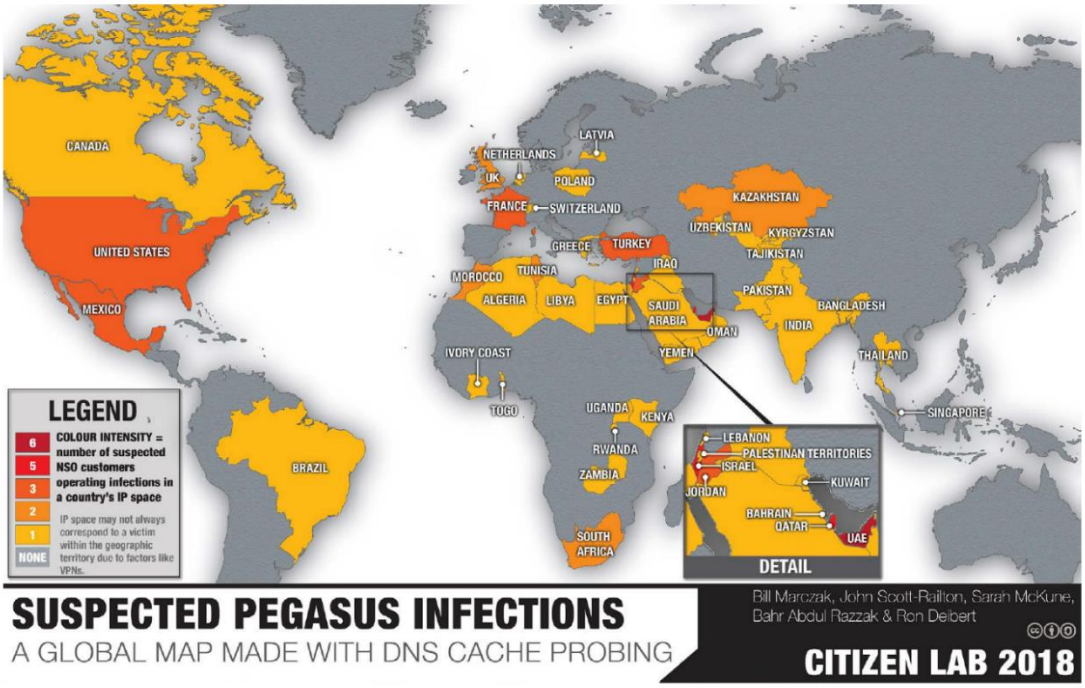

Figure 15. of Suspected Pegasus Infections[634]

In conclusion, Pegasus spyware is a tool developed by the Israel-based NSO Group, used by many governments around the world, and has led to severe human rights violations. The software specifically targets politicians, journalists, and activists, collecting their personal data and making unauthorized use of their devices' cameras and microphones. NSO Group's links to the Israeli government and the licensing and export of the software have put the company and Israel at the center of international criticism.[635] The effects of the Pegasus software have compromised the digital privacy of thousands of people worldwide, affecting many high-profile individuals and organizations.

[634] Marczak and Scott-Railton (n 602).

[635] 'Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware - Kaster - 2023 - Thunderbird International Business Review - Wiley Online Library' 358 <https://onlinelibrary.wiley.com/doi/10.1002/tie.22321> accessed 24 June 2024.

5.5.7. Pegasus Software and State Responsibility

In international law, cyber operations must be conducted in accordance with the principles of state sovereignty, human rights, and global peace and security. States are obliged to take the necessary measures to prevent harmful cyber activities originating from their territory. They should also refrain from cyber operations that violate the sovereign rights of other states and hold actors who engage in such actions accountable. During cyber operations, states must respect human rights, particularly protecting the privacy of personal data and freedom of expression. Cooperation between states and the principles of legal responsibility are crucial for the peaceful use of cyberspace. In the context of the principle of state responsibility, acts contrary to international law hold the state responsible for its action, unless there is a reason that eliminates the illegality.

Actors in cyberspace include states, groups, and individuals anonymously or openly. Cyber operations include actions such as interfering with, damaging, and denying access to a computer system's networks.[636] Cyber surveillance is a significant aspect of cyber operations. Cyber surveillance and cyber espionage may include actions such as obtaining data from a system that an actor has identified as a target, accessing the system's tools, and controlling or directing it.[637] While Article 2(4) of the UN Charter prohibits the use of force by states against each other, there is debate over whether cyber operations constitute the use of force. Schmitt has stated that a cyber operation can be considered a use of force if it produces effects similar to the traditional use of force.[638] Attribution of cyber operations by non-state actors to the state is complex, and evidence-gathering processes are complicated.[639]

Pegasus spyware is software that installs spyware inside a targeted device (usually Apple iPhone devices) to gain full access to the target device, use the device's hardware tools, and intercept personal data. The company is required to request a license from the Israeli Ministry of Defense when exporting the product, and Israeli authorities classified

[636] KÖKSOY (n 221) 10–11.

[637] 'CYBER-SURVEILLANCE Dictionary' <https://dictionnaire.enap.ca/Dictionnaire/63/Index_by_word.enap?by=word&id=21> accessed 24 June 2024.

[638] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44).

[639] Ecemiş Yılmaz (n 51) 188.

Pegasus software as it can be exported by NSO Group.[640] The software, which has infected thousands of people and has been detected in more than 45 countries, has infiltrated the devices of many influential people, from senior politicians and journalists to human rights activists and members of the royal family.[641] According to the official website of NSO Group, the company that owns the software, the company's primary customers are government bodies and security organizations.

Studies have indicated that Pegasus violated different legal rules, especially human rights violations. In this section, the software sold by the NSO Group, a non-state actor, to other state and non-state actors will be analyzed regarding state responsibility. As mentioned earlier, states are the main actors in international law, and states can only be held responsible for acts that violate international law under certain criteria. The Peg spyware case is complex, with state and non-state actors operating together. For an operation to be attributed to a state under the law of state responsibility, the following conditions must be fulfilled: the action must be attributable to the state, it must constitute an unlawful act, and there must be no justifications that negate its unlawfulness.[642]

5.5.8. Pegasus Software and Attribution Problem

For a state to be held responsible for a cyber operation, the operation must be attributable to that state. Without attribution, a state cannot be held responsible for an act.[643] When the act is a cyber operation, two separate investigations must be carried out to attribute this cyber operation. The cyber operation must be attributed both technically and legally to the alleged state. Since the Pegasus spyware is owned by an Israeli company and licensed by the government, Israel has been criticized for violating the law.

Israel-based NSO Group is a cyberwarfare company. A company's cyber operations can only be attributed to a state under certain conditions. The first of these conditions is that the state authorizes the company. For a cyber operation carried out by a non-state actor to be

[640] 'Pegasus Spyware Row Is Really about Who Controls Cyber Weapons' (*Middle East Eye*) <https://www.middleeasteye.net/opinion/pegasus-spyware-row-who-controls-cyber-weapons> accessed 24 June 2024; 'Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware - Kaster - 2023 - Thunderbird International Business Review - Wiley Online Library' (n 638) 358.

[641] Amnesty International Security Lab (n 633).

[642] Ecemiş Yılmaz (n 51) 183.

[643] ibid 182–183.

attributable to a state, the state in question must have authorized the operation or have control over it.[644] If a non-state actor operates under the direction of the state, its actions can be attributed to that state. Another requirement is that the state officially accept and adopt cyber operations. If a state accepts and endorses the cyber operation, the cyber operation can be attributed to the state. The fact that a state provides financial, technical, training, etc. support to the cyber operations of a non-state actor does not make the state responsible for this operation.[645] Finally, if a company commissioned by a state exceeds the powers granted to it without the knowledge of government officials (Ultra Vires), this operation cannot be attributed to the state. [646]

The Israeli government has not taken any official responsibility for the NSO Group's Pegasus software and has not acknowledged the cyber operations that took place with the software. he government's authority and control over these operations have not been clarified. However, Israel's licensing of the software as a weapon through the Ministry of Defense represents an endorsement of the Pegasus software. However, there is no conclusive evidence as to whether the NSO Group's operations were under the direct direction and control of the Israeli state. Therefore, the requirements for attributing a cyber operation by a non-state actor to a state do not seem to be met in the light of technical reports and investigations.

5.5.9. Pegasus Software and Violation of Law

For a state to be held responsible for a cyber operation, it must be an act in violation of international law. Once a cyber operation is attributed to a state, the legal dimension of the action is addressed. According to Alexander and Krishna, Pegasus spyware involves acts that violate the right to privacy. The Pegasus software, which was discovered by analyzing the message received on Ahmad Mansoor's phone, technically transferred data without the consent and knowledge of the person and spied on his private life. Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[647] and Article 8 of the

[644] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) 17.
[645] ibid 17.
[646] ibid.
[647] *International Covenant on Civil and Political Rights*, art. 17

European Convention on Human Rights (ECHR)[648] protect the right to privacy. The Pegasus software violated these rights, and these violations were identified in technical reports. [649]

According to the Tallinn Manual, human rights law applies in cyberspace, and the State is obliged to protect these rights, although courts may differ in their understanding. States are responsible for the human rights violations that result from their actions.[650]

The Pegasus software may be considered a violation of law under Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[651] and Article 8 of the European Convention on Human Rights (ECHR).[652] Where the Pegasus software is attributable to a state (in this case, Israel), it may be considered in conjunction with the abovementioned violations.

5.5.10. Pegasus Spyware and Grounds for Wrongful Acts

According to the Tallinn Manual, the reasons for categorizing a cyber operation as wrongful act include consent, self-defense, countermeasures, necessity, force majeure, and hardship.

a) Consent: Consent is a state's consent to an unlawful operation to be carried out on its territory. Consent removes the illegality of the action.[653] Pegasus software is a cyber espionage tool and can be used by governments. If the government of a state purchases this software from NSO Group, it can activate the cyber espionage software due to a request for security support from an allied government. If the country requesting the support gives its consent, it cannot hold the other state responsible for these actions within its borders. However, according to the Tallinn Manual, if consent is obtained due to threats and coercion, it is invalid

[648] *European Convention on Human Rights*, art. 8

[649] Rudie and others (n 494); Marczak and others (n 605); Marczak and Scott-Railton (n 602); 'Forensic Methodology Report: How to Catch NSO Group's Pegasus' (n 601).

[650] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) rr 34-35–36.

[651] "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation, and everyone has the right to the protection of the law against such interference or attacks"*

[652] Alexander and Krishna (n 618) 8–10.

[653] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 20

consent.[654] In addition, the limits of consent should not be exceeded. Consent should not always be given explicitly but should not be assumed. If consent is obtained, the illegality disappears. [655]

b) Self-Defense[656] : While Article 2 of the UN Charter prohibits the "use of force," Article 51 states that actions taken by a state in the event of an armed attack will eliminate the illegality. According to the Tallinn Manual, assessing a cyber operation as an armed attack depends on the impact and scope of the operation.[657] The element of an armed attack must be cross-border. However, the attribution of cyber operations by non-state actors against another state to a state is complicated by the nature of cyberspace. According to CitizenLab's report, the Pegasus spyware, whose use dates back to 2013, was discovered in 2016.[658] In other words, the software was discovered three years after the first known action, and it also took some time for technical analysis. Pegasus spyware was developed for surveillance and data extraction. According to Daskal, the data collected in cyber operations can lead to the unlawful arrest, torture, or even murder of victims.[659] The use of Pegasus software has also created such vulnerabilities.[660]

c) Countermeasures: States have the right to take measures in response to violations of law committed against them. Countermeasures can only be taken in response to an unlawful act.[661] Countermeasures must be temporary and must cease when the unlawful act has ceased.[662] A State's countermeasure must follow the principle of proportionality. The victim state may use force to deter the attack against it.[663] States exposed to the harmful effects of Pegasus software may use countermeasures to eliminate this threat. However, this measure must be proportionate to the damage caused by the Pegasus software (such as terminating data transfer and control over the device).

---

[654] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 19.
[655] ibid.
[656] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 21
[657] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 19.
[658] Marczak and Scott-Railton (n 602) 1.
[659] Jennifer Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues' (2016) 8 Journal of National Security Law and Policy 482 <https://digitalcommons.wcl.american.edu/facsch_lawrev/1100>.
[660] Alexander and Krishna (n 618) 4.
[661] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 22
[662] Ecemiş Yılmaz (n 51) 201.
[663] ibid 193–205.

d) Force Majeure: In international law, the emergence of force majeure is the inability of a state to fulfill an obligation due to unforeseen and unforeseeable circumstances. If the state invoking force majeure has the opportunity to meet its obligations and refrains from doing so due to the cost, the right to force majeure disappears.[664] If a state is subjected to a cyber-attack on its critical infrastructure systems, it may resort to taking measures to stop the attack and use Pegasus software where possible. However, the state must have exhausted legal remedies to stop this action. [665]

e) Distress: In international law, acts of individuals who violate the law can sometimes be attributed to the state. Another reason for eliminating the illegality of such acts is distress. In the case of distress, actions taken by a person to save his or her own life or the lives of others are exempt from illegality.[666] It is not very common for cyber operations to save a person's life.[667] Nevertheless, the increasing digitalization and integration of human life into digital systems strengthens this possibility. If the possibility of the Pegasus software saving human life is realized, the illegality arising from using the software may disappear.

f) Necessity[668] : It is stated in the Tallinn Manual that a state may be exempted from violations of law arising from its cyber actions if it is unable to fulfill its obligations in case of necessity.[669] Necessity arises when the protection of the vital interest of the state or the prevention of a very serious and imminent danger can only be realized in the event of a breach of obligations. However, if the state is placed in this dangerous situation as a result of its own actions, it cannot be held to have acted out of necessity. A state's use of Pegasus software to counter a threat to itself or to protect its vital interest may be a case of necessity.

---

[664] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 23
[665] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 19.
[666] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 24
[667] Ecemiş Yılmaz (n 51) 203.
[668] Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001), art. 25
[669] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 19.

5.5.11. Testing the Attribution of Cyber Actions of Pegasus Software

Tsagourias mentions three tests for the attribution of cyber operations of non-state organizations to the state: the institutional, impact, and agency tests. [670]

a- Corporate Test

First, the institutional test states that cyber actions of de jure and de facto organs of states can be attributed to the state in case of illegality. While de jure bodies are determined by international law, de facto bodies are those adopted by states.[671] In the context of this test, according to the available data, the NSO Group must be a de facto or de jure organ of the state for the NSO Group's Pegasus software to be attributed to the State of Israel for cyber espionage in violation of international law. As is well known, the State of Israel has registered the Pegasus software and authorized its use and export in the context of the Wassenaar Arrangement.[672] According to the CitizenLab report, it is known that the NSO Group exports Pegasus software to governments to monitor targeted individuals and acquire data.[673] It is even alleged that the Israeli police purchased this software, but the Israeli authorities have denied these allegations.[674] Important technical details should be emphasized here. The data from the target devices using Pegasus software is collected at Pegasus' server center in Israel.[675] The state of Israel is responsible for overseeing cyberspace activities in its territory[676] and is alleged to know the content of these activities since it licenses them. However, as Schmitt points out, the fact that a state provides support such as financing and training to a non-state actor does not make that state responsible for the actions of that non-state actor.

b- Functionality Test

---

[670] Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (2016) 21 Journal of Conflict and Security Law krw020, 462.

[671] ibid.

[672] 'Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware - Kaster - 2023 - Thunderbird International Business Review - Wiley Online Library' (n 638) 358.

[673] Marczak and Scott-Railton (n 602).

[674] Bethan McKernan, 'Police Use of Pegasus Malware Not Illegal, Israeli Inquiry Finds' *The Guardian* (22 February 2022) <https://www.theguardian.com/world/2022/feb/22/police-use-of-pegasus-malware-not-israeli-inquiry-finds> accessed 25 June 2024.

[675] Marczak and Scott-Railton (n 602) 14.

[676] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) rr 6–7.

The functional test refers to the delegation of authority by a state to a non-state body. Under the functional test, a state is responsible for unlawful acts committed by a body it has authorized.[677] In other words, if a state has authorized a company or body to carry out cyber operations, it is responsible for these actions. However, at this point, it is essential to draw attention to ultra vires acts. According to the Tallinn Manual, if a non-state actor carries out cyber operations without the knowledge of the government outside of its authorized tasks, the state cannot be held responsible for these actions.[678] In this case, the question is whether the state has effective control over the actions. Although the Pegasus software was made available by an Israeli company and licensed by the Israeli government, it is stated that the Israeli government licensed the software based on the company's commitment to use it with the consent of governments to fight terrorism and prevent serious crimes.

c- Agency Test

Finally, the agency test establishes that an unlawful cyber operation can be attributed to a state if it is carried out by a non-state actor, provided that the state has either commissioned or authorized these individuals or groups to perform the action.[679] This principle highlights the responsibility of states in overseeing the activities of non-state actors, particularly in the context of cybersecurity. There is credible information suggesting that the state directly instructed the NSO Group to utilize the Pegasus software, which raises significant questions about state accountability in cyber operations.

In conclusion, Pegasus spyware is a cyber espionage tool developed by the Israel-based NSO Group and used by many governments worldwide. It infiltrates the devices of high-profile individuals, such as politicians, journalists, and activists, collecting their personal data and making unauthorized use of their devices' cameras and microphones. Using Pegasus software can lead to serious human rights violations and can be considered a violation of international law. However, according to the Tallinn Manual, there are also grounds for ruling out the illegality of a cyber operation. If a state consents to an operation on its territory, the action is not unlawful. Also, when a state is subjected to an armed attack, actions taken in the exercise of its right to self-defense are not unlawful. States may take

[677] Tsagourias (n 673) 462.
[678] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 44) r 17.
[679] Tsagourias (n 673) 462.

proportionate countermeasures in response to violations of international law committed against them. Force majeure can legitimize a state's temporary breach of its international obligations to protect its vital interests. Force majeure can save a state from illegality if it is unable to fulfill its obligations due to unforeseen events beyond its control. Finally, distress may justify actions taken because of the necessity to protect a person's life or physical integrity. When the use of Pegasus software is considered in this context, it may, in some cases, be in accordance with international law, or its illegality may be eliminated.

6. CONCLUSION

This thesis analyzes Israel's national security policies and their direct and indirect effects on its cyber security in detail. It argues that despite having limited natural resources and a relatively small population, Israel has become one of the leading states in the world in both high technology and cyber security thanks to its strategic investments and policies in science and technology. The factors underlying this success are discussed in different chapters throughout the thesis.

Israel's cyber security strategy is based on the fundamental national security approach that Israel has had since its establishment. This national security approach goes beyond just military and technical defense mechanisms and has been realized in a wide range of areas, from infrastructure investments to elite education programs. Israel's first prime minister, David Ben-Gurion's approach to national security, which includes not only military defense tactics and strategies but also economic and social issues despite the “existential threats,” has been essential for the country's development. The main feature of Israel's cyber security policy is that it is a structure that encourages academic education, joint solutions with civilian and military organizations, and total defense. In particular, programs such as the Academic Reserve (Atuda), which allows the most successful high school students to receive both academic and military education at the same time, enable the country to train experts in science, technology, and cyber security. In addition, international cooperation and diplomacy play an essential role in Israel's cybersecurity strategy and are vital to countering cyber threats and building regional security. Direct and indirect US investment and assistance to Israel have had significant benefits for Israel's security structure.

In addition, the State of Israel has made efforts to secure its presence in cyberspace by establishing its cybersecurity laws and institutions. As a result of these efforts, Israel, with its state and non-state actors, has gained a strong position in cyberspace. The data and analyses examined throughout the thesis provide valuable insights into how Israel has increased its cybersecurity capacity and how this capacity has been aligned with its national security strategy. The Israeli model represents a complex strategy that takes a proactive approach to cybersecurity threats and effectively counters them. It is clear that this model can serve as an example for other countries in integrating cybersecurity and national security policies.

Cybersecurity is a relatively new field and exists in a different space from the traditional understanding of security, which has made its status in terms of international law controversial. In cyberspace, state and non-state actors both pose threats and are exposed to threats. International law should develop norms appropriate to this situation in cyberspace, and the efforts at this point are presented in this thesis. A cyber-attack can be as harmful or even more harmful than an armed attack. A state may attack another state in cyberspace in violation of the prohibition on the use of force. Although the International Law of Responsibility, which determines the responsibilities of a state towards another state, is tailored to conventional attacks, it can also be applied in cyberspace. However, for a state to be held responsible to another state, a cyber operation must first violate the law, and this operation must be attributable to a state with evidence and proof. When these conditions are met, the state can be held responsible for the operation if no principle eliminates the illegality in the conduct of this operation. In operations in cyberspace, attribution of cyber actions is difficult due to the nature of cyberspace. In order to attribute a cyber operation, evidence is needed, and this is usually done through technical analysis.

Nevertheless, a state's cyber networks can be used by malicious actors and non-state actors. This is why this process requires sensitivity. As discussed in the Pegasus spyware, the actions of a non-state organization violating international law under the auspices of a state can trigger the principle of state responsibility. The conditions for holding states responsible for the actions of non-state organizations have been analyzed extensively and discussed in the context of a case study on the Pegasus spyware and the responsibility of the State of Israel in this case.

Although cybersecurity studies have gained increasing importance over the past few decades, their growth has been exponential, making cybersecurity a dominant priority over other pressing security issues. International law has traditionally aimed to resolve global challenges between nations, but cyber threats present a relatively new challenge. Addressing these issues and compensating for the resulting harms requires international courts to take a more active role. The evolving dynamics of cyberspace demand new regulations, and this new order, in turn, requires specific concepts and legal principles to secure this domain. Policymakers, academics, and legal scholars must collaborate to build a sustainable cyber world and actively resolve cyber issues at both the individual and international levels. Most importantly, we must develop mechanisms to protect individuals' rights and freedoms in cyberspace against both state and non-state actors.

This thesis examines Israel's understanding of national security and how it has evolved since its establishment. It analyzes Israeli cyber security policies, state and non-state actors, and their actions. It also explains cybersecurity in detail with case studies. Finally, it analyzes the link between cybersecurity and international law in the context of non-state actors' operations in cyberspace.

BIBLIOGRAPHY

‘6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry’ <https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/> accessed 20 June 2024

A BD and Milstein DU, ‘The Iron Wall’ [2023] The Iron Wall of Jabotinski <https://www.academia.edu/108287725/The_Iron_Wall> accessed 11 June 2024

Acer Y and Kaya İ, Uluslararası Hukuk Temel Ders Kitabı (13th edn, Seçkin Yayıncılık 2022)

Ackerman D, ‘From Ben-Gurion to Netanyahu: The Evolution of Israel’s National Security Strategy’ [2019] FDD <https://www.fdd.org/analysis/2019/05/13/from-ben-gurion-to-netanyahu-the-evolution-of-israels-national-security-strategy/> accessed 19 March 2024

Adamsky D, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel (Stanford University Press 2010)

Adamsky D (Dima), ‘From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force’ (2017) 26 Security Studies 157

Dima Adamsky, ‘The Israeli Odyssey toward Its National Cyber Security Strategy’ (2017) 40 *The Washington Quarterly* 113

Akyeşilmen N, Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik (2018)

‘Alarum Technologies Stock Price Today (NASDAQ: ALAR) Quote, Market Cap, Chart | WallStreetZen’ <https://www.wallstreetzen.com/stocks/us/nasdaq/alar> accessed 25 June 2024

Albright D and others, ‘Preventing Iran From Getting Nuclear Weapons: Constraining Its Future Nuclear Options’ (2012) <https://dissem.in/p/37253385/preventing-iran-from-getting-nuclear-weapons-constraining-its-future-nuclear-options-p-10-5-march-2012> accessed 7 August 2024

Alexander A and Krishna T, ‘Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism’ (2022) 11 Laws 85

Almor T, ‘Born Global: The Case of Small and Medium Sized, Knowledge Intensive, Israeli Firms’ (2000)

Amidror Y, ‘Israel’s National Security Doctrine’ (JISS, 2021) <https://jiss.org.il/en/amidror-israels-national-security-doctrine/> accessed 19 March 2024

Amnesty International Security Lab, ‘The Pegasus Project’ (2024) <https://securitylab.amnesty.org/case-study-the-pegasus-project/> accessed 7 August 2024

‘Aqua Security Closes $60M Additional Funding at a Valuation Above $1B’ (Aqua) <https://www.aquasec.com/news/60m-additional-funding/> accessed 25 June 2024

Armaoğlu F, 20. Yüzyıl Siyasi Tarihi 1914-1995 (Kronik Kitap 2019)

US Government Army, Joint Publication JP 3-0 Joint Operations (CreateSpace Independent Publishing Platform 2012)

Avag R, ‘Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security’ <https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant> accessed 9 June 2024

Avidor J, Building an Innovation Economy: Public Policy Lessons from Israel (SSRN 2014) <https://ssrn.com/abstract=1856603> accessed 7 August 2024

Marie Baezner and Patrice Robin, *Stuxnet* (CSS Cyberdefense Hotspot Analyses, No 4, ETH Zurich, 18 October 2017) https://doi.org/10.3929/ethz-b-000200661 accessed 7 May 2024.

Baldwin DA, ‘The Concept of Security’ (1997) 23 Review of International Studies 5

Bar S, ‘Israeli Strategic Deterrence Doctrine and Practice’ (2020) 39 Comparative Strategy 321

Baram G, ‘Israeli Defense in the Age of Cyber War’ (2017) 24 Middle East Quarterly

Baram G and Ben-Israel I, ‘The Academic Reserve’ (2019) 34 Israel Studies Review 75

Barnett M and Duvall R, ‘Power in International Politics’ (2005) 59 International Organization 39

Bar-Siman-Tov Y, ‘The United States and Israel since 1948: A “Special Relationship”?’ (1998) 22 Diplomatic History 231

Bay M, ‘What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era’ (2016) 6/2016 French Journal for Media Research

Bergman R and Mazzetti M, ‘The Battle for the World’s Most Powerful Cyberweapon’ The New York Times (28 January 2022) <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html> accessed 24 June 2024

Berzon C, ‘Cybersecurity in Israel: Leading the World to a Safer Digital Future’ (Startup Nation Central, 6 May 2024) ‘Cybersecurity in Israel’ (Startup Nation Central, 2024) https://startupnationcentral.org/blog/cybersecurity/cybersecurity-in-israel/ accessed 25 June 2024

Betz DJ and Stevens T, Cyberspace and the State: Towards a Strategy for Cyberpower (1st edition, Routledge 2011)

Biju J, Gopal N and Prakash A, ‘Cyber Attacks and Its Different Types’ (2019) 6 International Research Journal of Engineering and Technology https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf accessed 7 August 2024

Booth K, ‘Security and Emancipation’ (1991) 17 Review of International Studies 313

Booth K, *Theory of World Security* (Cambridge University Press 2007)

Borghard ED and Lonergan SW, ‘Deterrence by Denial in Cyberspace’ (2023) 46 Journal of Strategic Studies 534

Brenner S and Clarke L, ‘Civilians in Cyberwarfare: Conscripts’ (2010) 43 Vanderbilt Journal of Transnational Law 1011

Breznitz D, ‘Industrial R&D as a National Policy: Horizontal Technology Policies and Industry-State Co-Evolution in the Growth of the Israeli Software Industry’ (2007) 36 Research Policy 1465

Broude M, Deger S and Sen S, ‘Defence, innovation and development: the case of Israel’ (2013) 12 Journal of Innovation Economics & Management 37

Brown LR 1934-, Redefining National Security (Worldwatch Institute 1977)

Buchan R and Devanny J, 'South African Cyber Diplomacy and Cyber Governance' (Carnegie Endowment for International Peace 2024) <https://www.jstor.org/stable/resrep57025.7> accessed 4 June 2024

Burton J, 'Cyber Deterrence: A Comprehensive Approach?' <https://ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/> accessed 7 June 2024

Buzan B, People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era (Harvester Wheatsheaf 1991)

'C4I and Cyber Defense Directorate' (IDF) <https://www.idf.il/en/mini-sites/directorates/c4i-and-cyber-defense-directorate/c4i-and-cyber-defense-directorate/> accessed 20 June 2024

'Cato Networks Raises $238M in Equity Investment at Over $3B Valuation | Cato Networks' <https://www.catonetworks.com/news/cato-networks-raises-238m-in-equity-investment-at-over-3b-valuation/> accessed 25 June 2024

Caudle SL, 'National Security Strategies: Security from What, for Whom, and by What Means' (2009) 6 Journal of Homeland Security and Emergency Management <https://www.degruyter.com/document/doi/10.2202/1547-7355.1526/html> accessed 19 March 2024

Cavelty MD, The Politics of Cyber-Security (Taylor & Francis 2024)

Chang F (ed), 'Building a National Program for Cybersecurity Science' (2012) 19 The Next Wave <https://www.govinfo.gov/content/pkg/GPO-TNW-19-4-2012/pdf/GPO-TNW-19-4-2012.pdf> accessed 7 August 2024

'Check Point Software (CHKP) Market Cap & Net Worth' (Stock Analysis) <https://stockanalysis.com/stocks/chkp/market-cap/> accessed 25 June 2024

Chen J, 'Cyber Deterrence by Engagement and Surprise' (2017) 7 PRISM 100

Chen TM and Abu-Nimeh S, 'Lessons from Stuxnet' (2011) 44 Computer 91

Chernenko E and others, ‘Russia’s Cyber Diplomacy’ (European Union Institute for Security Studies (EUISS) 2018) <https://www.jstor.org/stable/resrep21140.8> accessed 4 June 2024

‘Coğrafya ve İklim’ <https://embassies.gov.il/ankara/AboutIsrael/history/Pages/cografyaveiklim.aspx> accessed 20 March 2024

Cohen SA, ‘DAVID RODMAN’S “ISRAEL’S NATIONAL SECURITY DOCTRINE”:’ (2001) 5

Cohen SA and Klieman A, Routledge Handbook on Israeli Security (Taylor & Francis

Collins A, Çağdaş Güvenlik Çalışmaları (Nasuh Uslu tr, Uluslararası İlişkiler 2017)

Collins S and McCombie S, ‘Stuxnet: The Emergence of a New Cyber Weapon and Its Implications’ (2012) 7 Journal of Policing, Intelligence and Counter Terrorism 80

‘Constitution for Israel’ <https://knesset.gov.il/constitution/ConstIntro_eng.htm> accessed 20 March 2024

Cordey S, ‘The Israeli Unit 8200: An OSINT-Based Study’ (Center for Security Studies 2019)

‘Council of Europe – Convention on Cybercrime (ETS No. 185) – Translations - Treaty Office - Www.Coe.Int’ (Treaty Office) <https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations> accessed 8 June 2024

‘Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon’ (Cybersecurity & Digital Trust, 6 February 2021) <https://icdt.osu.edu/countdown-zero-day-stuxnet-and-launch-worlds-first-digital-weapon> accessed 9 June 2024

Craigen D, Diakun-Thibault N and Purse R, ‘Defining Cybersecurity’ 13

Crawford J, State Responsibility: The General Part (Cambridge University Press 2013) <https://www.cambridge.org/core/books/state-responsibility/EE846D9378B83A9DCC5E794FC086B07E> accessed 24 June 2024

‘Cyber Conflict and Deterrence’ (2016) 22 Strategic Comments iii

‘Cyber Security Strategy for Germany’ (Federal Ministry of the Interior and Community) <https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-

security-strategy-artikel.html;jsessionid=CBA5C6A6A1FE88917BAC7ED12F5703E1.live892?nn=16825398> accessed 6 June 2024

'Cybercrime' (United Nations : UNODC ROMENA) <https://www.unodc.org/romena/en/cybercrime.html> accessed 8 June 2024

'Cybersecurity' (ITU) <https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx> accessed 4 June 2024

'Cybersecurity Definition & Meaning - Merriam-Webster' <https://www.merriam-webster.com/dictionary/cybersecurity> accessed 4 June 2024

'CYBER-SURVEILLANCE Dictionary' <https://dictionnaire.enap.ca/Dictionnaire/63/Index_by_word.enap?by=word&id=21> accessed 24 June 2024

Daskal J, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues' (2016) 8 Journal of National Security Law and Policy <https://digitalcommons.wcl.american.edu/facsch_lawrev/1100>

De Falco M, 'Stuxnet Facts Report. A Technical and Strategic Analysis' <https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/> accessed 9 June 2024

Delerue F, Cyber Operations and International Law (Cambridge University Press 2020) <https://www.cambridge.org/core/books/cyber-operations-and-international-law/74D210E76E46531542AD27CECF07ABDE> accessed 24 June 2024

Delibasis Fokas D and Klein A, 'Cyberspace Operations & State Responsibility' (14 July 2019) <https://papers.ssrn.com/abstract=3505428> accessed 24 June 2024

Dinstein Y, War, Aggression and Self-Defence (6th edn, Cambridge University Press 2017)

Dissolution FSR to, 'Demography in the Middle East: Population Growth Slowing, Women's Situation Unresolved | The Washington Institute' <https://www.washingtoninstitute.org/policy-analysis/demography-middle-east-population-growth-slowing-womens-situation-unresolved> accessed 22 March 2024

Downes C, ‘Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns’ (2018) 3 The Cyber Defense Review 79

Doyle R, ‘The U.S. National Security Strategy: Policy, Process, Problems’ (2007) 67 Public Administration Review 624

Dror Y, ‘Does Israel Have a National Security Policy?’ (Institute for National Security Studies 2011) <https://www.jstor.org/stable/resrep08959.7> accessed 19 March 2024

Duo W, Zhou M and Abusorrah A, ‘A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges’ (2022) 9 IEEE/CAA Journal of Automatica Sinica 784

Dyson E, ‘Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)’ (1996) 12 The Information Society 295

Ecemiş Yılmaz HK, Siber Operasyonların Uluslararası Hukukla İlişkilendirilmesi (Yetkin Yayınları 2023)

Barak, E, ‘Israel’s Military Doctrine: by Ehud Eilam (Lanham: Lexington Books, 2018), 159 pages’ (2019) 13 *Israel Journal of Foreign Affairs* 415–419 https://doi.org/10.1080/23739770.2019.1710805.

Eisenkot G, ‘Deterring Terror - How Israel Confronts the Next Generation of Threats’ (Belfer Center for Science and International Affairs 2016) <https://www.belfercenter.org/israel-defense-forces-strategy-document> accessed 19 March 2024

Eisenkot G and Siboni G, ‘Guidelines for Israel’s National Security Strategy | The Washington Institute’ (The Washington Institute for Near East Policy 2019) 160 <https://www.washingtoninstitute.org/policy-analysis/guidelines-israels-national-security-strategy> accessed 19 March 2024

‘Ensuring Equitable Digital Futures for Everyone’ (UNDP) <https://www.undp.org/turkiye/press-releases/ensuring-equitable-digital-futures-everyone> accessed 6 June 2024

‘Enterprise Security Solutions | IBM’ <https://www.ibm.com/security> accessed 4 June 2024

‘Fact Sheets: Iran | Arms Control Association’ <https://www.armscontrol.org/factsheets/IranProliferation> accessed 9 June 2024

Farwell J and Rohozinski R, ‘Stuxnet and the Future of Cyber War’ (2011) 53 Survival 23

Fidler DP, ‘Was Stuxnet an Act of War? Decoding a Cyberattack’ (2011) 9 IEEE Security & Privacy 56

Finlay L and Payne C, ‘The Attribution Problem and Cyber Armed Attacks’ (2019) 113 202

Flowers S, The History and Development of the Weizmann Institute of Science (University of London 1975)

‘Forensic Methodology Report: How to Catch NSO Group’s Pegasus’ (2021) <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> accessed 24 June 2024

Forum IP, ‘The Haredi Exemption’ (Israel Policy Forum, 2 April 2024) <https://israelpolicyforum.org/2024/04/02/the-haredi-exemption/> accessed 25 June 2024

Foundation TH, ‘Index of Economic Freedom: Israel | The Heritage Foundation’ (Index of Economic Freedom | The Heritage Foundation) <https://www.heritage.org/index> accessed 12 June 2024

Frei J, ‘Israel’s National Cybersecurity and Cyberdefense Posture: Policy and Organizations’ (ETH Zurich 2020) Report <https://www.research-collection.ethz.ch/handle/20.500.11850/440107> accessed 20 June 2024

Freilich C, ‘Israel’s National Security Policy’ in Reuven Y Hazan and others (eds), The Oxford Handbook of Israeli Politics and Society (Oxford University Press 2021) <https://doi.org/10.1093/oxfordhb/9780190675585.013.25> accessed 19 March 2024

Freilich CD, ‘National Security Decision-Making in Israel: Processes, Pathologies, and Strengths’ (2006) 60 Middle East Journal 635

Freilich CD, Israeli National Security: A New Strategy for an Era of Change (Oxford University Press 2018)

Freilich CD, Cohen MS and Siboni G, Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power (Oxford University Press 2023)

Fried Y, ‘Military, Civilian, or Both: David Ben-Gurion’s Perception of National Security After the War of Independence’ (2020) 7 Contemporary Review of the Middle East 125

Gal R, A Portrait of the Israeli Soldier: (Praeger 1986)

‘George Bush and the Axis of Evil’ The Economist <https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil> accessed 9 June 2024

Gewirtz J, Israel’s Edge: The Story of The IDF’s Most Elite Unit - Talpiot (Independently published 2016)

Gibson W, Neuromancer (Ace Books 1984)

Gilboa E, ‘American Contributions to Israel’s National Security’ (2020) 23 18

Goodman W, ‘Cyber Deterrence: Tougher in Theory than in Practice?’ (2010) 4 Strategic Studies Quarterly 102

Greenberg Y, ‘The Swiss Armed Forces as a Model for the IDF Reserve System—Indeed?’ (2013) 18 Israel Studies 95

‘Hackers Exploited Record “Zero-Day” Flaws in 2021, Google Researchers Say - Bloomberg’ <https://www.bloomberg.com/news/articles/2022-04-19/google-caught-record-number-of-zero-day-hacks-in-2021> accessed 9 June 2024

Halevi-Davidov N and Tishler A, ‘Innovation in Israel: Facts and Measures’ (2007) https://www.researchgate.net/publication/251554847_Innovation_in_Israel_Facts_and_Measures accessed 30 May 2024.

Hathaway OA and others, ‘The Law of Cyber-Attack’ (2012) 100 *California Law Review* 817, Yale Law & Economics Research Paper No. 453, Yale Law School Public Law Working Paper No. 258 https://ssrn.com/abstract=2134932 accessed 27 May 2024.

Horowitz D, ‘The Israeli Concept of National Security’ in Talal Asad and Roger Owen (eds) (Macmillan Education UK 1983) <http://link.springer.com/10.1007/978-1-349-17282-5_4> accessed 20 March 2024

‘How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | WIRED’ <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/> accessed 9 June 2024

‘How Israel Turned Itself into a High-Tech Hub - BBC News’ <https://www.bbc.com/news/business-15797257> accessed 20 March 2024

‘How Israel’s Pegasus Spyware Stoked the Surveillance Debate | Council on Foreign Relations’ <https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate> accessed 24 June 2024

Hunker J, ‘Cyber War and Cyber Power: Issues for NATO Doctrine’ (NATO Defense College 2010) <https://www.jstor.org/stable/resrep10354> accessed 4 June 2024

Huysmans J, ‘Security! What Do You Mean?From Concept to Thick Signifier’ (1998) 4 European Journal of International Relations - EUR J INT RELAT 226

‘Hybrid CoE Paper 8: Cyber Deterrence: A Case Study on Estonia’s Policies and Practice’ (Hybrid CoE, 2024) https://www.hybridcoe.fi/publications/hybrid-coe-paper-8-cyber-deterrence-a-case-study-on-estonias-policies-and-practice/ accessed 7 June 2024 ‘IAI Company Profile - The Solution to Defense and Security Challenges’ <https://www.iai.co.il/about/company-profile> accessed 25 June 2024

‘Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary’ (Federal Register, 5 October 2020) <https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2019> accessed 24 June 2024

‘Intel’s $15 Billion Purchase of Mobileye Shakes up Driverless Car Sector | Reuters’ <https://www.reuters.com/article/idUSKBN16K0Z4/> accessed 11 June 2024

‘Israel Defense Forces Strategy Document’ (Belfer Center for Science and International Affairs) https://www.belfercenter.org/israel-defense-forces-strategy-document accessed 20 June 2024

‘Israel GDP’ (World Bank Open Data) <https://data.worldbank.org> accessed 25 June 2024

‘Israel Has Seen Arms Embargoes Before’ The Economist <https://www.economist.com/middle-east-and-africa/2024/05/16/israel-has-seen-arms-embargoes-before> accessed 7 August 2024

‘Israel Shipyards – DIMSE’ <https://dimse.info/israel-shipyards/> accessed 25 June 2024

‘Israeli Army to Extend Mandatory Service: Report’ <https://www.aa.com.tr/en/middle-east/israeli-army-to-extend-mandatory-service-report/3131078> accessed 25 June 2024

‘Israeli Cyber Investments Exceed $1 Billion for First Time in 2018’ (The Jerusalem Post | JPost.com, 28 January 2019) <https://www.jpost.com/israel-news/investment-in-israeli-cyber-exceeds-1-billion-for-first-time-in-2018-578906> accessed 25 June 2024

‘Israeli Security Chief Celebrates Stuxnet Cyber Attack’ (The Telegraph, 16 February 2011) <https://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html> accessed 9 June 2024

‘ITU Cybersecurity Activities’ (ITU) <https://www.itu.int:443/en/action/cybersecurity/Pages/default.aspx> accessed 8 June 2024

Jabotinsky Z, ‘The Iron Wall’ (1923) <https://en.jabotinsky.org/media/9747/the-iron-wall.pdf> accessed 7 August 2024

Jansons J, ‘Was Stuxnet an Act of War?’ (2017) 1 Security Forum 109

‘Jews, Arabs, and French Diplomacy: A Special Report’ (Commentary Magazine, 1 May 2005) <https://www.commentary.org/articles/pryce-jones/jews-arabs-and-french-diplomacy-a-special-report/> accessed 24 March 2024

Kamiya S and others, ‘What Is the Impact of Successful Cyberattacks on Target Firms?’ (National Bureau of Economic Research, March 2018) <https://www.nber.org/papers/w24409> accessed 6 June 2024

Karaoğlu O and Elhan N, İsrail Bir Ülkenin Akademik Anatomisi (İnkılap Kitabevi, 1st edn, 2023)

Khalili L, ‘The Iron Wall’ [2006] Feminist Review 2

Kinsella D, ‘Conflict in Context: Arms Transfers and Third World Rivalries during the Cold War’ (1994) 38 American Journal of Political Science 557

Kirsh N, ‘The Foundations of Israel’s Ongoing Love Affair with Science’ (2022) 46 Endeavour 100837

Kissel RL, ‘Glossary of Key Information Security Terms’ [2013] NIST <https://www.nist.gov/publications/glossary-key-information-security-terms-1> accessed 6 June 2024

Knudsen BB, ‘Developing a National Security Policy/Strategy: A Roadmap’ (2012) 30 Sicherheit und Frieden / Security and Peace 135

Kober A, ‘Arms Races and the Arab–Israeli Conflict’ in Thomas Mahnken, Joseph Maiolo and David Stevenson (eds), Arms Races in International Politics: From the Nineteenth to the Twenty-First Century (Oxford University Press 2016) <https://doi.org/10.1093/acprof:oso/9780198735267.003.0010> accessed 8 July 2024

Köksoy F (ed), Yeni Küresel Tehdit Siber Saldirilar: Siber Güvenlik ve Politika Uygulamalari (Nobel Akademik Yayincilik 2020)

Kramer FD, Butler RJ and Lotrionte C, ‘Cyber, Extended Deterrence, and NATO’ (Atlantic Council 2016) <https://www.jstor.org/stable/resrep03464> accessed 7 June 2024

Kulesza J, ‘State Responsibility for Cyberattacks on International Peace and Security’ (2010) *Polish Yearbook of International Law* 139-152 https://ssrn.com/abstract=1668020 accessed 30 September 2024

Landler M and Markoff J, ‘Digital Fears Emerge After Data Siege in Estonia’ The New York Times (29 May 2007) <https://www.nytimes.com/2007/05/29/technology/29estonia.html> accessed 8 June 2024

Langner R, ‘Cyber Power: An Emerging Factor in National and International Security’ [2016] Horizons: Journal of International Relations and Sustainable Development 206

Leffler MP, ‘National Security’ (1990) 77 The Journal of American History 143

Lewis JA, ‘Linking National Security and Innovation: Part 1’ (Center for Strategic and International Studies (CSIS) 2021) <https://www.jstor.org/stable/resrep31134> accessed 19 March 2024

Lindsay JR, ‘Stuxnet and the Limits of Cyber Warfare’ (2013) 22 Security Studies 365

Lindstrom L and Signoretti M, ‘12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020’ (CCDCOE 2020) <https://ccdcoe.org/library/publications/12th-international-conference-on-cyber-conflict-20-20-vision-the-next-decade-proceedings-2020/> accessed 6 June 2024

Lu Y, ‘Cybersecurity Research: A Review of Current Research Topics’ (2018) 03 Journal of Industrial Integration and Management 1850014

Luttwak EN and Horowitz D, The Israeli Army, 1948-1973 (Harper & Row, 1975)

Luttwak EN and Shamir E, The Art of Military Innovation: Lessons from the Israel Defense Forces (Harvard University Press 2023)

Mahmoud KW, 'Cyber Attacks: The Electronic Battlefield' (Arab Center for Research & Policy Studies 2013) <https://www.jstor.org/stable/resrep12651> accessed 4 June 2024

Malka A, 'Israel and Asymmetrical Deterrence' (2008) 27 Comparative Strategy 1

Marczak B and others, 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (University of Toronto 2018) Citizen Lab Research Report No. 113 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 24 June 2024

Marczak B and Scott-Railton J, 'The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender' (University of Toronto 2016) Citizen Lab Research Report No. 78 <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/> accessed 24 June 2024

Margulies P, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melbourne Journal of International Law 496

Matrosov A and others, 'Stuxnet under the Microscope' (2010) 6 ESET LLC (September 2010) <http://ca-apac.com/image/ITR%201.pdf> accessed 9 June 2024

McKernan B, 'Police Use of Pegasus Malware Not Illegal, Israeli Inquiry Finds' The Guardian (22 February 2022) <https://www.theguardian.com/world/2022/feb/22/police-use-of-pegasus-malware-not-israeli-inquiry-finds> accessed 25 June 2024

Meridor D and Eldadi R, 'Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later' (Institute for National Security Studies 2019) Memorandum 187 <https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf> accessed 7 August 2024

Merom G, 'Israel's National Security and the Myth of Exceptionalism' (1999) 114 Political Science Quarterly 409

Mohamad HA, ‘Review of The Iron Wall: Israel and the Arab World’ (2001) 9/10 The Arab Studies Journal 146

Mueller P, ‘The Stuxnet Worm’ (Proceedings of the 2012 International Conference on Cyber Security, 2012) https://api.semanticscholar.org/CorpusID:53698349 accessed 9 June 2024

Nath C, ‘Cyber Security in the UK’ <https://post.parliament.uk/research-briefings/post-pn-389/> accessed 6 June 2024

‘National Cyber Power Index 2022’ (Harvard’s Belfer Center for Science and International Affairs 2022) <https://www.belfercenter.org/publication/national-cyber-power-index-2022> accessed 7 August 2024

Nations U, ‘United Nations Charter (Full Text)’ (United Nations) <https://www.un.org/en/about-us/un-charter/full-text> accessed 6 June 2024

Nevill L and Hawkins Z, ‘Cyber Deterrence’ (Australian Strategic Policy Institute 2016) <https://www.jstor.org/stable/resrep04232.6> accessed 4 June 2024

‘New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction | WIRED’ <https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/> accessed 6 June 2024

Nicolas Falliere, Liam O. Murchu and Eric Chien, ‘Symantec, W 32. Stuxnet Dossier, Version 1.4, February 2011. Not Classified.’ (2011) <https://nsarchive.gwu.edu/document/21440-document-44> accessed 7 August 2024

‘Novalpina Capital and Founders Buy NSO at $1b Co Value - Globes’ <https://en.globes.co.il/en/article-novalpina-capital-and-founders-buy-nso-for-1b-1001273312> accessed 24 June 2024

‘NSO’nun Perde Arkası: WhatsApp’i Hackleyen Şirket Hakkında Bilmemiz Gerekenler’ <https://siberbulten.com/uluslararasi-iliskiler/isrl/nsonun-perde-arkasi-whatsappi-hackleyen-sirket-hakkinda-bilmemiz-gerekenler/> accessed 24 June 2024

Nye JS Jr, ‘Deterrence and Dissuasion in Cyberspace’ (2017) 41 International Security 44

OECD, Education at a Glance 2022: OECD Indicators (Organisation for Economic Co-operation and Development 2022) <https://www.oecd-ilibrary.org/education/education-at-a-glance-2022_3197152b-en> accessed 25 June 2024

Orchin M, Fenichel H and Jensen WB, Scientist in the Service of Israel: The Life and Times of Ernst David Bergmann (Magnes Press,Israel 2011)

'Our Story' (Rafael) <https://www.rafael.co.il/our-story/> accessed 25 June 2024

Paikowsky D and Ben Israel I, 'Science and Technology for National Development: The Case of Israel's Space Program' (2009) 65 Acta Astronautica 1462

'Pegasus: French President Macron Identified as Spyware Target' <https://www.bbc.com/news/world-europe-57907258> accessed 24 June 2024

'Pegasus Spyware Row Is Really about Who Controls Cyber Weapons' (Middle East Eye) <https://www.middleeasteye.net/opinion/pegasus-spyware-row-who-controls-cyber-weapons> accessed 24 June 2024

Peled D, Defense R&D and Economic Growth in Israel: A Research Agenda (Samuel Neaman Institute for Advanced Research in Science and Technology, University of Haifa, March 2001)

Penslar DJ, Zionism and Technocracy: The Engineering of Jewish Settlement in Palestine, 1870-1918 (Indiana University Press 1991)

'PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher | PCMag' <https://www.pcmag.com/archive/playstation-hack-to-cost-sony-171m-quake-costs-far-higher-264796> accessed 6 June 2024

Pratama A and Rafrastara FA, 'Computer Worm Classification' (2012) 10 *International Journal of Computer Science and Information Security* 21-24

'Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware - Kaster - 2023 - Thunderbird International Business Review - Wiley Online Library' <https://onlinelibrary.wiley.com/doi/10.1002/tie.22321> accessed 24 June 2024

Radvanovsky RS and McDougall A, Critical Infrastructure: Homeland Security and Emergency Preparedness, Fourth Edition (Taylor & Francis 2021)

‘Radware Ltd. (RDWR) Statistics & Valuation Metrics’ (Stock Analysis) <https://stockanalysis.com/stocks/rdwr/statistics/> accessed 25 June 2024

Raska M, ‘Building a Cyber Iron Dome: Israel’s Cyber Defensive Envelope’ (2014) 192 RSIS Commentaries <https://hdl.handle.net/10356/94095> accessed 7 August 2024

Samet R and Aslan Ö, ‘Kötü Amaçlı Yazılımlar ve Analizi’ in Şeref Sağiroğlu and Mustafa Alkan (eds), Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık (1st edn, Aralık 2018, Ankara) 227, ISBN: 978-605-2233-22-1

‘Remarks by the President at AIPAC Policy Conference’ (whitehouse.gov, 4 March 2012) <https://obamawhitehouse.archives.gov/the-press-office/2012/03/04/remarks-president-aipac-policy-conference-0> accessed 23 March 2024

‘Research and Development (R&D) - Gross Domestic Spending on R&D - OECD Data’ (theOECD) <http://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm> accessed 27 June 2024

Rid T, ‘Deterrence beyond the State: The Israeli Experience’ (2012) 33 Contemporary Security Policy

Rid T and Buchanan B, ‘Attributing Cyber Attacks’ (2015) 38 Journal of Strategic Studies 4

Robertson H, ‘Self-Defense against Computer Network Attack under International Law’ (2002) 76 International Law Studies <https://digital-commons.usnwc.edu/ils/vol76/iss1/19>

Rodman D, ‘Israel’s National Security Doctrine: An Introductory Overview’ (2001) 5(3) *Middle East Review of International Affairs*

Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014) https://ssrn.com/abstract=2418940 accessed 30 September 2024

Ross D, Doomed to Succeed: The U.S.-Israel Relationship from Truman to Obama (First edition, Farrar, Straus and Giroux 2015)

Rudie J and others, ‘Technical Analysis of the NSO Group’s Pegasus Spyware’, 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (2021) <https://ieeexplore.ieee.org/document/9799180> accessed 24 June 2024

Rudner M, ‘Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge’ (2013) 26 International Journal of Intelligence and CounterIntelligence 453

Saltzman I, ‘Cyber Posturing and the Offense-Defense Balance’ (2013) 34 Contemporary Security Policy 40

Sanger DE and others, ‘U.S. Blacklists Israeli Firm NSO Group Over Spyware’ The New York Times (3 November 2021) <https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html> accessed 24 June 2024

Schatz D, Bashroush R and Wall JA, ‘Towards a More Representative Definition of Cyber Security’ (2017) 12 *Journal of Digital Forensics, Security and Law* 53

Scott P, ‘Israel’s Qualitative Military Edge: U.S. Arms Transfer Policy’ International Relations

Shackelford SJ and Andres R, ‘State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem’ (2010) 42 *Georgetown Journal of International Law* 971

Sharp JM, *U.S. Foreign Aid to Israel* (Congressional Research Service, RL33222, updated 16 November 2020) https://crsreports.congress.gov accessed 30 September 2024

Shlaim A, ‘The Iron Wall Revisited’ (2012) 41 Journal of Palestine Studies 80

Shlaim A, The Iron Wall: Israel and the Arab World (Penguin, 30 July 2015)

Singer PW and Friedman A, Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford Univ Press 2014)

Sinha KN, ‘Political System of Israel’ (1960) 21 The Indian Journal of Political Science 289

‘Snyk Closes $196.5 Million Series G Funding at $7.4 Billion Valuation’ (Snyk, 12 December 2022) <https://snyk.io/news/snyk-closes-196-5-million-series-g-funding-at-7-4-billion-valuation/> accessed 25 June 2024

Sorensen TC, ‘Rethinking National Security’ (1989) 69 Foreign Aff. 1

Spiegel SL, The Other Arab-Israeli Conflict: Making America’s Middle East Policy, from Truman to Reagan (University of Chicago Press 1986)

<https://press.uchicago.edu/ucp/books/book/chicago/O/bo5953649.html> accessed 24 March 2024

Splunk, 'Top 50 Cybersecurity Threats' (2024) <https://www.splunk.com/en_us/form/top-50-security-threats.html> accessed 5 June 2024

Staff T, 'NSO Said to Block Some Government Clients from Using Its Spyware' <https://www.timesofisrael.com/nso-said-to-block-some-government-clients-from-using-its-spyware/> accessed 24 June 2024

'Startup Nation Finder - Explore the Israeli Tech Ecosystem' <https://finder.startupnationcentral.org> accessed 25 June 2024

Stockholm International Peace Research Institute (SIPRI), SIPRI Yearbook 2022: Armaments, Disarmament and International Security (Oxford University Press 2022) <https://www.sipri.org/yearbook/2022>

'Stuxnet Timeline Shows Correlation Among Events | WIRED' <https://www.wired.com/2011/07/stuxnet-timeline/> accessed 9 June 2024

Tabansky L, 'Israel Defense Forces and National Cyber Defense' (2020) 19 Connections: The Quarterly Journal 45

Tabansky L, 'Cyber Power in the Changing Middle East' (2016) *Turkish Policy Quarterly* 15(1) http://turkishpolicy.com/article/804/cyber-power-in-the-changing-middle-east accessed 25 June 2024

Tabansky L and Ben Israel I, Cybersecurity in Israel (Springer International Publishing 2015) <https://link.springer.com/10.1007/978-3-319-18986-4> accessed 19 March 2024

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017) <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 24 June 2024

'Target Cyber Attack | Columbia SIPA' <https://www.sipa.columbia.edu/sipa-education/picker-center-executive-education/case-collection/target-cyber-attack> accessed 25 June 2024

Thakur K and others, ‘Impact of Cyber-Attacks on Critical Infrastructure’, 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (IEEE 2016) <http://ieeexplore.ieee.org/document/7502286/> accessed 7 June 2024

Hazan RY and others (eds), *The Oxford Handbook of Israeli Politics and Society* (Oxford University Press, online edn, 7 June 2018) https://doi.org/10.1093/oxfordhb/9780190675585.001.0001 accessed 27 September 2024

‘The Real Story of Stuxnet - IEEE Spectrum’ <https://spectrum.ieee.org/the-real-story-of-stuxnet> accessed 9 June 2024

‘The White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009. Unclassified. | National Security Archive’ <https://nsarchive.gwu.edu/document/21424-document-28> accessed 5 June 2024

Kuehl D, ‘From Cyberspace to Cyberpower: Defining the Problem’ in Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security* (University of Nebraska Press 2011) http://www.jstor.org/stable/10.2307/j.ctt1djmhj1 accessed 6 June 2024

Tondo L and Kierszenbaum Q, ‘Plan to End Ultra-Orthodox Students’ Military Exemption Sparks Row in Israel’ The Guardian (26 March 2024) <https://www.theguardian.com/world/2024/mar/26/plan-end-ultra-orthodox-students-military-exemption-row-israel> accessed 25 June 2024

Tor U, ‘“Cumulative Deterrence” as a New Paradigm for Cyber Deterrence’ (2017) 40 Journal of Strategic Studies 92

Tsagourias N, ‘Cyber Attacks, Self-Defence and the Problem of Attribution’ (2012) 17 Journal of Conflict and Security Law 229

——, ‘Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts’ (2016) 21 Journal of Conflict and Security Law

‘Ülke Künyesi / T.C. Dışişleri Bakanlığı’ <https://www.mfa.gov.tr/israil-kunyesi.tr.mfa> accessed 25 June 2024

Unger RM, The Knowledge Economy (Verso, March 19, 2019)

‘Unstoppable Wiz: Cyber Startup Nets Another $1 Billion in Funding as Valuation Jumps to $12B’ (ctech, 7 May 2024) <https://www.calcalistech.com/ctechnews/article/rjs3pupf0> accessed 25 June 2024

‘U.S. Aid to Israel in Four Charts’ (Council on Foreign Relations) <https://www.cfr.org/article/us-aid-israel-four-charts> accessed 23 March 2024

‘U.S. Foreign Assistance to the Middle East: Historical, Recent Trends, and the FY2024 Background Request’ (Congressional Research Service 2023) R46344 <https://sgp.fas.org/crs/mideast/R46344.pdf> accessed 7 August 2024

‘U.S. Overseas Loans and Grants (Greenbook) -- Data | Development Data Library’ <https://data.usaid.gov/Administration-and-Oversight/U-S-Overseas-Loans-and-Grants-Greenbook-Data/7cnw-pw8v/about_data> accessed 24 March 2024

‘U.S.-Israeli Missile Defense Budget Appropriations’ (Statista) <https://www.statista.com/statistics/209369/defense-budget-appropriations-for-us-israeli-missile-defense-by-system-type/> accessed 24 March 2024

van Marissing R, ‘The Role of Cyber Diplomacy in Dutch Security Policy: Long Term and Short Term Responses to Coercive Cyber Operations’ (2017) 41 Atlantisch Perspectief 29

‘Varonis Systems (VRNS) Market Cap & Net Worth’ (Stock Analysis) <https://stockanalysis.com/stocks/vrns/market-cap/> accessed 25 June 2024

Von Glahn G and Taulbee JL, Law Among Nations: An Introduction to Public International Law (Routledge 2017)

Wæver O, Securitization and Desecuritization, vol 5 (Centre for Peace and Conflict Research Copenhagen 1993)

Warner M, ‘Cybersecurity: A Pre-History’ (2012) 27 Intelligence and National Security 781

‘Was Stuxnet Built to Attack Iran’s Nuclear Program? | InfoWorld’ <https://www.infoworld.com/article/2626198/was-stuxnet-built-to-attack-iran-s-nuclear-program-.html> accessed 9 June 2024

Waxman MC, ‘Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)’ (2011) 36 Yale Journal of International Law 421 https://scholarship.law.columbia.edu/faculty_scholarship/1653

Weinstein D, ‘Snowden and U.S. Cyber Power’ (2014) *Georgetown Journal of International Affairs* 4

Weitz R, ‘Israel’ (Strategic Studies Institute, US Army War College 2007) <https://www.jstor.org/stable/resrep12108.14> accessed 25 June 2024

‘What Is a Cyberattack? | IBM’ (15 August 2021) <https://www.ibm.com/topics/cyber-attack> accessed 25 June 2024

‘What Is a Kernel? Types of Kernels - TechTarget.Com’ (Data Center) <https://www.techtarget.com/searchdatacenter/definition/kernel> accessed 24 June 2024

‘What Is Cybersecurity? | Microsoft Security’ <https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity> accessed 4 June 2024

‘What Is Cybersecurity? - Cisco’ <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html> accessed 4 June 2024

Williams MC, ‘Words, Images, Enemies: Securitization and International Politics’ (2003) 47 International Studies Quarterly 511

Wilner AS, ‘Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism’ (2011) 34 Journal of Strategic Studies 3

‘World Economic Outlook (October 2023) - GDP, Current Prices’ <https://www.imf.org/external/datamapper/NGDPD@WEO> accessed 22 March 2024

Wunderle W and Briere A, ‘U.S. Foreign Policy and Israel’s Qualitative Military Edge: The Need for a Common Vision’ (2008) *Policy Focus* 80 (24 January 2008)

Yarger HR, Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century (Praeger Security International 2008)

Yayla M, ‘Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma’ [2013] Türkiye Barolar Birliği Dergisi 199

Young K, ‘Cyber Case Study: Target Data Breach’ (CoverLink Insurance - Ohio Insurance Agency, 13 September 2021) <https://coverlink.com/cyber-liability-insurance/target-data-breach/> accessed 6 June 2024

Zagare FC, ‘Reconciling Rationality with Deterrence: A Re-Examination of the Logical Foundations of Deterrence Theory’ (2004) 16 Journal of Theoretical Politics 107

Public Law 110–429, Naval Vessel Transfer Authority (122 Stat. 4842, enacted October 15, 2008)