Cyber, Intelligence, and Security

Volume 3 | No. 2 | October 2019

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber, Intelligence, and Security

Volume 3 | No. 2 | October 2019

Contents

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber, Intelligence, and Security

The purpose of *Cyber, Intelligence, and Security* is to stimulate and enrich the public debate on related issues.

Cyber, Intelligence, and Security is a refereed journal published three times a year within the framework of the Cyber Security Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Graphic Design: Michal Semo-Kovetz, Tel Aviv University Graphic Design Studio
Printing: Digiprint Zahav Ltd., Tel Aviv

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Cyber, Intelligence, and Security is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

ISSN 2519-6677 (print) • E-ISSN 2519-6685 (online)

The Space Arms Race: Global Trends and State Interests

Zeev Shapira and Gil Baram

Today space is an arena with a significant impact on the security, military, economy, and daily routines of many countries around the world and has attracted many stakeholders. As a result, global interest in the development of weapons for use in space—a process known as the "space arms race"—has increased. The purpose of this article is to present the current approaches to the weaponization of space and the activities of the primary and secondary states in this arena, and to propose a new categorization based on their technological standing. The article discusses the similarities and differences between states active in space and their position regarding its weaponization, in order to help understand the map of national and international interests in space at the current time.

Keywords: Weaponization of space, space powers, national security

Introduction

More than a decade after the international community criticized China and the United States for openly conducting anti-satellite missile tests,[1] which helped curb the escalation at the time, countries are now noticeably renewing

Zeev Shapira is an independent researcher on space, cyber, and national security. Gil Baram is the head of research at the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University.

1 Jim Wolf, "U.S. Shot Raises Tensions and Worries over Satellites," *Reuters*, February 22, 2008, https://www.reuters.com/article/us-satellite-intercept-vulnerability/u-s-shot-raises-tensions-and-worries-over-satellites-idUSN2144210520080222; "US, Other Countries Condemn China ASAT Test," *Spacetoday*, January 19, 2007, http://www.spacetoday.net/Summary/3637.

offensive operations in space: Russia conducted suspicious maneuvers in proximity to other countries' satellites; China launched secretive dual-use space systems; the United States is working to establish a separate and independent space force, and in March 2019 India conducted its first test of an anti-satellite weapon. The test by India—a country without a history of offensive space activities—illustrates the dilemma of many countries operating in space: Should they act independently and aggressively in this arena to protect their interests, or should they place their trust in international forums to try to rein in the current space arms race?

The weaponization of space poses two major threats. Firstly, it poses a security threat as unilateral actions by countries to weaponize space increase uncertainty within the international system. For example, space researchers recently warned that the propose establishment of the US Space Force increases the risk of conflict and escalates tensions with its rivals.[2] Secondly, it poses an environmental threat as experiments with anti-satellite weapons have led to the creation of large amounts of space debris and have increased the difficulty of conducting operations close to Earth. If the process of the weaponization of space is accelerated, space could become dangerous and inaccessible to the various players.[3]

Furthermore, the accelerated development of the commercial space market has widened the circle of stakeholders in maintaining space as a neutral arena, but it has also increased the potential risks should it become an arena of war. The value of the space market is currently estimated at $340 billion and is expected to triple its value in about twenty years.[4] Part of that growth is the continued increase in investment by space companies.[5] At the same time, growing political tensions over the past decade between the United States, Russia, and China, combined with new commercial space

2 Laura Grego, "There Are Much Better Options than a Space Force," *Union of Concerned Scientists*, February 19, 2019, https://www.ucsusa.org/press/2019/there-are-much-better-options-space-force-0.

3 "Trump's Proposed Space Force Could Worsen Earth's Orbital Debris Problem," *Washington Post*, August 10, 2018, https://www.washingtonpost.com/world/2018/08/10/trumps-proposed-space-force-could-worsen-earths-orbital-debris-problem/.

4 Jeff Foust, "A Trillion-Dollar Space Industry Will Require New Markets," *Spacenews*, July 5, 2018, https://spacenews.com/a-trillion-dollar-space-industry-will-require-new-markets/.

5 Caleb Henry, "Space Startup Investments Continued to Rise in 2018," *Spacenews*, February 4, 2019, https://spacenews.com/space-startup-investments-continued-to-rise-in-2018.

technologies as part of the "New Space" industry—including cyber and artificial intelligence—have heightened concern over the development of a space arms race.

Today there are two different processes taking place in space: The *militarization of space* refers to the use of space-based technology (communication, remote sensing and navigation) to support military operations, and the *weaponization of space* refers to the introduction of weapons into space, such as anti-satellite weapons, satellites capable of damaging other satellites, and weapons operating from space aimed at Earth. Nowadays, the militarization of space is seen as a fait accompli, but that space has yet to become weaponized and therefore the process is reversible.[6] Indeed, in recent years, the superpowers have intensified the process of weaponizing space. Senior US administration and military officials have voiced concern about China and Russia's offensive use of space,[7] leading to widespread reforms in US space security, the establishment of the US space command at the directive of President Donald Trump,[8] and a surge in tensions with China and Russia.[9]

At the same time, initiatives in the international arena to find diplomatic solutions to the question of the space arms race have intensified in recent years, among them a Russian-Chinese proposal in 2008 to restrict the introduction of weapons into space and the European Union's proposal in 2014 for an international space code of conduct.[10] In addition, non-governmental initiatives have been undertaken to strengthen the transparency of space warfare laws

6 For more on the differences and a review of uncertainty and consensus on the term "space weaponization," see Columba Peoples, "The Securitization of Outer Space: Challenges for Arms Control," *Contemporary Security Policy* 32, no. 1 (2011): 2–5.

7 Sandra Erwin, "DNI Coats: Enemies are Developing Advanced Technology, Space Weapons," *Spacenews*, April 4, 2018, http://spacenews.com/dni-coats-enemies-are-developing-advanced-technology-space-weapons-we-have-to-up-our-game; Colin Clark, "CSAF Predicts War in Space 'In a Matter of Years,'" *Breaking Defense*, February 26, 2018, https://breakingdefense.com/2018/02/csaf-predicts-war-in-space-in-a-matter-of-years.

8 Mike Wall, "Trump Signs Directive to Create Military Space Force," *Space*, February 21, 2019, https://www.space.com/president-trump-space-force-directive.html.

9 Joel Gehrke, "China Warns Trump about Dangers of New Space Force," *Washington Examiner*, June 19, 2018, https://www.washingtonexaminer.com/policy/defense-national-security/china-warns-trump-about-dangers-of-new-space-force; "Russia Warns against Trump's 'Alarming' Plans for US Space Force," *Military*, June 20, 2018, https://www.military.com/daily-news/2018/06/20/russia-warns-against-trumps-alarming-plans-us-space-domination.html.

10 David C. DeFrieze, "Defining and Regulating the Weaponization of Space," *Joint Force Quarterly* 74, no. 1 (2014).

and to examine the adaption of international law to military use of space. For example, the MILAMOS Project,[11] launched at McGill University in Canada in 2016, has experts from various countries working to formulate a guide that defines international law that is applicable for military use in space during peace times. Another example is the Woomera Manual initiative, launched in 2018 at the University of Adelaide in Australia, in collaboration with other universities, which seeks to examine the applicability of existing international law to military space operations.[12]

In recent years, professionals and academics have issued many publications about various countries' military activities in space, including the weaponization of space. Despite the growing discourse on the subject, most of the research deals with the space powers (the United States, China, and Russia), which may limit the scope of the debate on the weaponization of space and present only a partial perspective of the processes occurring in this sphere.

In this article, we illustrate the complexity that exists today in the different approaches to weaponization of space and propose to categorize countries according to their technological capabilities in space. We suggest dividing states that are active in space according to their technological status: (1) space superpowers: the United States, Russia, and China; (2) the medium space powers: the European Union, India, and Japan; (3) the emerging space powers.[13] This division reflects a broader range of interests and different approaches to the weaponization of space among the various countries, unlike the current and widely accepted conceptualization of the weaponization of space.

In the first part of the article, we present the existing approaches to the weaponization of space and discuss the challenges in understanding the current weaponization processes in various countries. In the second part, we propose a different categorization—based on the technological strength of the countries—and discuss the security, national, and diplomatic processes implemented by each country regarding this issue. Finally, we briefly

11 MILAMOS refers to "Manual on International Law Applicable to Military Uses of Outer Space."

12 For further reading on these initiatives see the official websites of MILAMOS at https://www.mcgill.ca/milamos and the Woomera Manual initiative at https://law.adelaide.edu.au/woomera.

13 To create the division, we borrowed the definition "medium space powers" from John J. Klein, "Space Strategy Considerations for Medium Space Powers," *Astropolitics* 10, no. 2 (2012): 3.

discuss Israel and the conclusions that emerge from the categorization we have proposed here and its implications for understanding countries' current space operations.

Approaches to Weaponization of Space

The literature on the weaponization of space is divided into two main camps of "for" and "against" the weaponization of space. In recent years, however, a more complex discourse has emerged, offering a broad range of outlooks and modes of action. Karl Mueller distinguishes six different approaches to the space weaponization process, which include three opposing weaponization (Idealists, Internationalists, Nationalists) and three supporting weaponization (Space Racers, Space Controllers, Space Hegemonists). These approaches represent different stages in the space weaponization spectrum, with the "idealists" at one end and the "space hegemonists" at the other.[14] Mueller's analysis, however, is limited to the American context only and does not provide practical examples of these perspectives. Similarly, Peter Hays also focuses only on the American context and suggests a division into four approaches: two supporting space weaponization (Space Hawks and Inevitable Weaponizers) and two opposing space weaponization (Space Doves and Militarization Realists).[15] Other divisions in the literature reflect a similar tendency,[16] and even though there are variations, all share the same common denominator of two camps—opponents and supporters—with a strong focus on the activities and policies of the United States in this field.

Evidently, researchers who represent different camps in their approach to space weaponization also tend to focus on the United States.[17] Researchers who advocate space weaponization, whether to protect critical space assets,[18]

14 Karl P. Mueller, "Totem and Taboo: Depolarizing the Space Weaponization Debate," *Astropolitics* 1, no. 1 (2003): 5–12.

15 Peter L. Hays, *United States Military Space: Into the Twenty-First Century* (DIANE Publishing, 2002), pp. 96–100.

16 Sterling Michael Pavelec, "The Inevitability of the Weaponization of Space: Technological Constructivism versus Determinism," *Astropolitics* 10, no. 1 (2012): 2–3; Mike Moore, *Twilight War: The Folly of US Space Dominance* (Oakland: The Independent Institute, 2008), p. 16.

17 Bruce M. DeBlois, "Space Sanctuary. A Viable National Strategy," *Airpower Journal*, (Winter 1998); James Clay Moltz, "Preventing Conflict in Space: Cooperative Engagement as a Possible US Strategy," *Astropolitics* 4, no. 2 (2006).

18 Alan Steinberg, "Weapons in Space: The Need to Protect Space Assets," *Astropolitics* 10, no. 3 (2012): 6–7.

or to win the race for operational space weapons,[19] tend to describe China and Russia more extensively, albeit mostly from an American perspective.

The focus on the United States is understandable, given that it is the greatest space power today, publishes detailed space policy documents, and operates with a relatively high level of transparency.[20] This focus, however, presents two limitations. First, approaches to space weaponization are tested according to American activities and are thus often framed as "for or against" weaponization, without examining a broader range of options. Second, relegating other countries in the space weaponization sphere to the margins of the discourse provides only a partial picture of reality and limits the ability to analyze alternative approaches to space weaponization.

In the next section, we propose a new categorization of approaches to space weaponization, based upon a country's degree of technological maturity. This division will help identify similar patterns of operation in the processes of space weaponization among countries that are in the same technological class, thus providing a different perspective from the traditional approach to space weaponization.

The Importance of Technological Status

As mentioned above, the division proposed here consists of three groups: space superpowers, medium space powers, and emerging space powers.[21] The United States, Russia, and China constitute the three space superpowers and have independent satellite development, launch, and control capabilities for all space orbits, and manned space programs. The medium space powers considered here are the European Union, India, and Japan, which possess the capabilities to develop, launch, and control advanced satellites independently but do not have a manned space program (India plans to carry out a manned launch in 2022).[22] Emerging space powers are those countries that do not have the above capabilities, or are in their initial stages of development.

19 Pavelec, "The Inevitability of the Weaponization of Space," 5–6.

20 Rebecca Johnson, "Security without Weapons in Space: Challenges and Options," *Disarmament Forum* 1 (2003): 2–3; Todd Harrison, Kaitlyn Johnson and Thomas G. Roberts, "Introduction," in *Space Threat Assessment 2018* (Center for Strategic and International Studies, April, 2019).

21 To create the division, we borrowed the definition "medium space powers" from John J. Klein, "Space Strategy Considerations for Medium Space Powers," *Astropolitics* 10, no. 2 (2012): 3.

22 Some researchers identify additional countries in this group, such as Israel, North Korea, and Iran.

Despite the large number of countries in this group, we only examine three of them—Pakistan, Brazil, and Australia—upon which we will formulate an assessment of the different interests within this group.

Space Superpowers

United States

The United States is the leading country in space activity today. As a result of its global dominance, the United States has incorporated space-based systems into its national security infrastructure, gaining significant advantage over its rivals. These advantages were highlighted in the Gulf War, the Balkan conflict, and the invasion of Iraq.

During the Cold War, the United States focused on countering the Soviet threat in space and even developed advanced initiatives in the 1980s, such as the Strategic Defense Initiative (also dubbed "Star Wars") to provide protection against intercontinental ballistic missiles. As the Soviet Union declined and collapsed, these initiatives faded.[23] At the beginning of the twenty-first century, the question of space security returned to the fore,[24] but economic and political constraints have prevented the development of a comprehensive strategy on this issue.[25] The United States, however, has continued to maintain an offensive position in space that was reflected in the publication of policy documents calling for the strengthening of its control of space[26] and for withdrawal from the Anti-Ballistic Missile (ABM) Treaty in 2002.[27] Over the past decade, tensions have increased between the United Sates, China, and Russia, reflected, in part, in changes to policy and rhetoric regarding space warfare and in President Trump's directive in 2018 to establish an independent space force.[28]

Diplomatically, the United States consistently opposes treaty proposals such as the Prevention of the Placement of Weapons in Outer Space and of

23 Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Secure World Foundation, April, 2019), pp. 3.1, 3.16.
24 Then US Secretary of Defense Donald Rumsfeld even warned of a "Space Pearl Harbor."
25 Weeden and Samson, *Global Counterspace Capabilities*, p. 3.1.
26 Johnson, "Security without Weapons in Space," 2–3.
27 The ABM Treaty restricted the United States and Russia in developing ballistic missile systems that could also be used against satellites.
28 Weeden and Samson, *Global Counterspace Capabilities*, p. 3.18.

the Threat or Use of Force against Outer Space Objects (PPWT)[29] citing concern for its ambiguity in defining space weapons and its lack of confidence in Russia and China's intentions.[30] The European initiative for a code of conduct for outer space activities, which is non-binding, received reserved support from the United States during President Barack Obama's term,[31] which only weakened since President Trump took office.[32]

The United States has extensive capabilities to damage, neutralize, and prevent its rivals from exercising their capabilities in space. As far back as 1985, the United States conducted a successful satellite destruction experiment with an air-launched missile (ASM-135), designed to counterbalance the anti-satellite weapons developed by the Soviet Union. The United States does not currently have a program to develop a dedicated direct ascent anti-satellite weapon, but its accumulated knowledge, combined with its proven ability to target satellites, reflects a real operational capability to destroy enemy satellites. Given the current technical capabilities of its anti-intercontinental ballistic missile (ICBM), the assumption is that these capabilities are currently limited to Low Earth Orbit (LEO),[33] but it is possible that their range will be increased in the future and will be able to hit higher orbits in space.

In the field of anti-satellite weapons, the United States is developing measures designed for various non-offensive needs, such as on orbit servicing, and has even conducted experiments over the years in rendezvous and proximity operations (RPO). Although the United States has not announced any plans to use these capabilities for offensive purposes, it could utilize the

---

29 "Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects" is a proposal that China and Russia have advanced at the United Nations since 2008. The proposal has been the subject of continued criticism over its ambiguity when it comes to the definition of space weapons.

30 Stephanie Nebehay, "U.S. Warns on Russia's New Space Weapons," *Reuters*, August 14, 2018, https://www.reuters.com/article/us-russia-usa-space/u-s-warns-on-russias-new-space-weapons-idUSKBN1KZ0T1; Jeff Foust, "U.S. Dismisses Space Weapons Treaty Proposal as 'Fundamentally Flawed,'" *Spacenews*, September 11, 2014, https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposal-as-fundamentally-flawed/.

31 Marcus Weisgerber, "U.S. Wants Changes to EU Space Code of Conduct," *Spacenews*, January 12, 2012, https://spacenews.com/18667us-wants-changes-to-eu-space-code-of-conduct/.

32 John Yoo, "Military Use of Space is Coming, Trump can Help America Prepare," *The Hill*, December 28, 2017, https://thehill.com/opinion/national-security/366663-military-use-of-space-is-coming-trump-can-help-america-prepare.

33 This refers to an orbit with an altitude of up to 2,000 km above the Earth.

knowledge it has accumulated to develop such capabilities within a short time.[34] The United States has a system called the Counter Communications System (CCS), which, while secretive, is believed to be capable of disrupting satellite signals should the need arise. In addition, over the years the United States has developed a number of programs in the field of directed-energy weapons, some of which have the potential to damage space assets.[35]

Russia

During the Cold War, the Soviet Union developed a range of capabilities against the space assets of its rival, the United States. With the end of the Cold War and the breakup of the Soviet Union, the Russian space industry lost most of its budget, and many of its military programs were shut down.[36] Over the past decade, Russia seems to have begun to modernize its military and civil space systems in an attempt to restore its status and avoid lagging behind China and the United States. Under President Putin, Russia is working more aggressively to consolidate its regional and international status and, in doing so, has marked space as a significant arena in any future conflict.

Since 2004, Russia has been working in the diplomatic arena together with China to advance limitations on the weaponization of space and has tabled proposals in the United Nations, such as the resolution entitled "No First Placement of Weapons in Outer Space."[37] However, the US administration notes that Russia's diplomatic efforts are incompatible with its offensive actions in space, which, it claims are evidence of Russia's true intentions.[38]

Russia possesses several means of damaging satellite systems, based partly on modernized Cold War-era programs and new developments. In the field of direct ascent weapons, Russia has several ground-to-air anti-satellite programs based on the A-235 and Kontakt systems, which were developed in the 1970s and 1980s. At the same time, it is currently developing the S-500 Anti Ballistic Missile System, which is also believed to have anti-satellite capabilities. Although Russia has not carried out a full-blown satellite interception, as the United States and China have, it can be concluded that the technical experience accumulated during the Cold War will give Russia

34 Weeden and Samson, *Global Counterspace Capabilities*, pp. 3.1–3.6.
35 Ibid, pp. 3.9–3.15.
36 Harrison et al., *Space Threat Assessment 2018*, pp. 17–18.
37 UN General Assembly, Draft resolution, No First Placement of Weapons in Outer Space, 2016.
38 Harrison et al., *Space Threat Assessment 2018*, p. 19.

the ability to deploy weapons against satellites within a few years, despite any technical limitations.

In the 1960s, Russia developed an interception system for satellites in LEO, which was declared operational in 1973. It also aspired to develop a more advanced system called Naryad, designed to damage satellites in Geostationary Orbit (GEO),[39] although the testing on this system ceased in 1991. Over the past decade, Russia has been developing rendezvous and proximity capabilities with secretive satellites that it uses to maneuver suspiciously near foreign satellites—an operation that could in the future be used to physically harm or disrupt those satellites.[40] Russia is also investing in additional anti-satellite weapons, such as means to disrupt signals from navigation, communications and even observation satellites. Furthermore, Russia has extensive technical knowledge based on its development of laser weapons during the Cold War and has even reinstituted a plan to develop aircraft-borne laser to directly target observation satellites, but it is unclear if these plans have reached operational maturity.[41]

China

During the Cold War period, China's space program was given a low priority, and China remained a secondary player in this arena. However, in recent decades China has invested considerable efforts in developing its capabilities in space and has assumed a significant role, as it possesses advanced civil and military programs, such as a space exploration program and independent navigation systems. These programs have enabled China to compete with the United States for regional and global influence.

As part of its growing rivalry with the United States over the past decade, China has developed a strategy based, in part, on denying American capabilities in space. In addition, China has begun to operate more aggressively in the space arena, as seen in published policy documents, which have called for its dominance of space and the development of advanced space weapons. However, it is unknown whether China is currently employing its space

39 GEO refers to an orbit of some 35,000 km above Earth and is used mostly for communications satellites.

40 Weeden and Samson, *Global Counterspace Capabilities*, pp. 2.1–2.14.

41 Ibid, pp. 2.15–2.22.

capabilities for military operations, and it is possible that these capabilities were constructed primarily for deterrence purposes.[42]

In the diplomatic arena, China supports Russia's efforts to promote international legislation to limit the weaponization of space. However, China's refusal to support initiatives such as the code of conduct for space, while encouraging legislation that does not have any enforcement mechanisms and does not preclude anti-satellite tests suggests, at least according to the United States, that China merely seeks to restrict US space activities without adversely affecting its own development programs, while presenting itself as purportedly supporting peace initiatives.[43]

In recent decades, China has developed a number of capabilities in the field of direct ascent weapons for targeting satellites, some having dedicated use and others having the capability to intercept missiles. While China began developing these weapons as early as the 1960s, only the experiments of the last two decades—and especially the satellite interception carried out in 2007—indicate that it has made progress in this field. One can conclude that China is now able to achieve operational capabilities to hit satellites in LEO by using a mobile ground system.

Over the past decade, China has carried out a large number of rendezvous and proximity maneuvers, raising concerns about the development of Chinese offensive capabilities against orbiting satellites. Prominent among China's activities is the launch of the Aolong-1 orbital debris cleanup satellite in 2016, which raised fears about its possible use to target satellites. As with Russia, there is concern that China could, should the need arise, also use its satellite capabilities to physically harm foreign satellites.[44] In addition, China is developing other means of targeting satellites and is believed to have capabilities to disrupt both communication and navigation satellites' signals. Furthermore, China has shown interest in developing counterspace laser devices and may have attempted to blind satellites using this method in 2005 and 2006.[45]

Overall, the three space superpowers have extensive space capabilities, both civilian and military, which enable them to prevent and impair their

42 Ibid, p. 1.1.

43 For extensive discussion of the matter, see "China's Position on a Code of Conduct in Space," *U.S.-China Economic and Security Review Commission*, September 8, 2017, https://bit.ly/2ow9N6V.

44 Weeden and Samson, *Global Counterspace Capabilities*, pp. 1.1–1.4.

45 Ibid, pp. 1.15–1.18.

rivals' space capabilities during a conflict. Although the United States seems to take the most offensive approach in space with the aim of gaining dominance and maintaining freedom of action, Russia and China also see space as a significant arena where the outcome of any future war will be determined. Thus, they also emphasize developing counterspace capabilities and preventing their rivals' achievements.

In the diplomatic arena, Russia and China operate differently from the United States, although seemingly for the same offensive ends. While the United States continues to thwart international legislation that would limit the weaponization of space and favors softer proposals, such as the code of conduct in outer space, Russia and China are pushing for initiatives that would advance limitations on the weaponization of space. In fact, the three superpowers use diplomacy primarily to limit their rivals, while they themselves work to empower their own capabilities with the aim of gaining supremacy in the space arms race.

The three superpowers operate according to an offensive approach, whether to protect their space assets and their international standing or to avoid being at a strategic disadvantage. While some differences exist between them—the United States seeks space hegemony, China aims to achieve equality, and Russia wants to reduce its relative weakness—the shared common denominator is that they all support the weaponization of space.

Medium Powers

Europe

Germany, the United Kingdom, France, and Italy possess extensive military space infrastructure, including observation satellites and other systems. However, none of these countries, other EU countries, nor the European Union itself is known to have a space weaponization plan. In fact, a strategy paper of the European Commission released in 2016 emphasized the space defense component, which includes improving situational awareness of space and analysis of threats, such as space weather and cyberattacks.[46] The European Space Agency is developing a number of initiatives to clean up space debris

46 European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Space Strategy for Europe," October 26, 2016, pp. 8–10, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-705-F1-EN-MAIN.PDF.

and for space exploration. Although these initiatives are seemingly designed for civilian goals, they are believed to have the technical potential to damage space assets if required.[47]

In the international arena, the European Union has opposed China and Russia's proposals to restrict the weaponization of space, on the claim that these proposals are neither clear nor sufficiently comprehensive.[48] Since 2008, however, the European Union has led an initiative to write a code of conduct for activities in space with the goal of breaking the deadlock in the debate over the weaponization of space.[49] Although the European Union's actions are intended to limit the weaponization of space, they also constitute its attempt to emerge as a central player that sets the normative agenda in this arena,[50] as part of a broader approach to the importance of protecting space assets.[51]

India

Although India began developing a space program in the 1960s, it did not make any significant achievements until the 1990s. Although the goal of India's space program was to improve the country's economic status through technological innovation, it was greatly influenced by the growth of China's military power. Thus, India tested primary military uses in space as early as the 1980s with the Integrated Guided Missile Development Program (IGDMP), which was the foundation for the development of its ballistic missile defense systems in the 1990s.[52]

India's rivalry with China and Pakistan continued to influence its military space program and led to the development of its missile defense capabilities and strengthening of its ties with the United States, which has included technology transfers. Although India has repeatedly hinted at the development

47 Harrison et al., *Space Threat Assessment 2018*, pp. 36–37.

48 Statements on behalf of the EU, "EU Explanation of Vote—United Nations 1st Committee: No First Placement of Weapons in Outer Space," Delegation of the European Union to the United Nations – New York, November 2, 2018, https://eeas.europa.eu/delegations/un-new-york/53334/eu-explanation-vote-%E2%80%93-united-nations-1st-committee-no-first-placement-weapons-outer-space_en.

49 Peoples, "The Securitization of Outer Space," 11–14.

50 Max M. Mutschler and Christophe Venet, "The European Union as an Emerging Actor in Space Security?," *Space Policy* 28, no. 2 (2012): 4–6.

51 Phillip A. Slann, "Anticipating Uncertainty: The Security of European Critical Outer Space Infrastructures," *Space Policy* 35 (2016): 8.

52 Zulfiqar Khan and Ahmad Khan, "Chinese Capabilities as a Global Space Power," *Astropolitics* 13, no. 2–3 (2015): 12–13.

of satellite interception capabilities, its plans to develop these weapons were not made public, until March 2019, when it conducted a successful anti-satellite missile experiment and destroyed one of its own satellites. This raised concerns that India intends to continue developing space weapons so as not to be left out of any future agreement restricting space weaponization.[53]

In the diplomatic arena, India continues to support global and regional efforts to use space for peaceful purposes and to advance norms for safety and sustainability in space. As part of its efforts, India has proposed launching a satellite for the South Asian Association for Regional Cooperation (SAARC),[54] and in 2017, it launched a communications satellite to assist countries in the region.[55] India also supports Chinese and Russian initiatives to limit the weaponization of space and recently reiterated this support following its test of an anti-satellite weapon.[56] Furthermore, India also supports the drafting of a code of conduct for activities in space but has retained reservations regarding some of its language, given that it was not a full partner in its formulation.[57]

Japan

At its inception, Japan's space program focused mainly on its civilian component. However, mounting pressure from the United States in the past decade and growing concern over its neighbors have led Japan to adopt a more active approach to space defense and to reorganize its military space infrastructure to increase its independence in this arena.[58] As part of these efforts, Japan has launched communication and observation satellites, has

53 Doris Elin Urrutia, "India's Anti-Satellite Missile Test is a Big Deal. Here's Why," *Space*, March 30, 2019, https://www.space.com/india-anti-satellite-test-significance.html.

54 The organization includes Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka.

55 "India Launches 'Invaluable' South Asia Satellite," *BBC*, May 5, 2017, https://www.bbc.com/news/world-asia-india-39814455.

56 Sachin Parashar, "Not Entering into Outer Space Arms Race, India Tells P-5 Countries," *Times of India*, March 28, 2019, https://timesofindia.indiatimes.com/india/not-entering-into-outer-space-arms-race-india-tells-p-5/articleshow/68604921.cms.

57 Rajeswari Pillai Rajagopalan, "The Space Code of Conduct Debate: A View from Delhi," *Strategic Studies Quarterly* 6, no. 1 (2012): 7–12.

58 Paul Kallender and Christopher W. Hughes, "Hiding in Plain Sight? Japan's Militarization of Space and Challenges to the Yoshida Doctrine," *Asian Security* (2018): 8–9.

set up a new headquarters to monitor space threats,[59] and approved its largest defense budget (some $46 billion) at the end of 2017.[60]

Japan currently does not have a development program for the weaponization of space, but it has the potential to damage satellites through the US Aegis missile system deployed in its territory and through future rendezvous and proximity systems capabilities that it is currently developing.[61] Moreover, Japan's military advances in space in recent years indicate that it is abandoning its traditional defensive norms and shifting to a strategy with more offensive characteristics.[62]

In the diplomatic arena, Japan supports both Chinese and Russian initiatives to limit the weaponization of space and the European initiative to develop a code of conduct for activities in space.[63] However, Japan's strategic alliance with the United States seems to continue to be of paramount importance, as prior to the United States giving its support to the code of conduct initiative, Japan refrained from supporting it fully as well.[64]

In conclusion, the medium powers possess extensive civil space infrastructures, including many dual-use satellites, designed to support military operations should they be needed. So far, however, these countries appear to have been operating with a certain restraint, by not developing any offensive programs in space and continuing to support international initiatives to prevent weaponization of space. Nonetheless, and given the significant technological progress of these countries in recent years and their considerable budgetary investments in this area, it can be assumed that they will be able to develop operational space weapons within a short time.

---

59 Shinichi Fujiwara, "Japan to Set Up Space Command Center to Track Debris, Threats," *Asahi Shimbun*, November 20, 2018, http://www.asahi.com/ajw/articles/AJ201811200034.html.

60 Mari Yamaguchi, "Japan Cabinet Approves Record 46B$ Defense Budget," *Defense News*, December 27, 2017, https://www.defensenews.com/global/asia-pacific/2017/12/27/japan-cabinet-approves-record-46b-defense-budget/.

61 Laura Grego, "A History of Anti-Satellite Programs," *Union of Concerned Scientists* (January 2012): 10–12.

62 Kallender and Hughes, "Hiding in Plain Sight," 17–18.

63 Ministry of Foreign Affairs of Japan, "Japan's Disarmament and Non-Proliferation Policy (Fifth Edition)," March 2011, pp. 26–27, https://www.mofa.go.jp/policy/un/disarmament/policy/pdfs/pamph1103.pdf.

64 Kazuto Suzuki, "Japan, Space Security and the Code of Conduct," in *Decoding the International Code of Conduct for Outer Space Activities*, ed. Ajey Lele (New Delhi: Institute for Defence Studies & Analyses: Pentagon Security International, 2012), pp. 94–96.

Contrary to the space superpowers, which seek to gain supremacy through an offensive military strategy and limited support for international initiatives, the medium powers seek to limit the proliferation of space weapons through international initiatives and the establishment of defensive space infrastructures, such as observation and interception systems. Their motives differ, however. The European Union, which initiated the space code of conduct, seeks to position itself as a central actor in preventing the proliferation of space weapons and thereby strengthen its international standing. India, which seeks to consolidate its regional strategic standing, has signaled its offensive capabilities in space on the one hand, while it continues to support international initiatives against the weaponization of space, as well as regional collaborations on the other hand. Japan may have the most narrow motives, as it seeks to safeguard its national security through strengthening its capabilities in space, its alliance with the United States, and its continued cooperation with the international community regarding restrictions on the weaponization of space.

While the space superpowers have the most offensive approach to space weaponization, the second-tier states presented above operate on a number of levels that represent different, and sometimes contradictory, approaches to the weaponization of space. The presence of these countries in the "middle" of the space technological hierarchy[65] seems to lead to a "middle road" to the weaponization of space: on the one hand, they operate at the diplomatic level to limit the weaponization of space and do not advance offensive space programs (with the exception of India's test of an anti-satellite weapon), but on the other hand, they do not fully commit to all international initiatives and continue to develop space capabilities that may be used for combat should the need arise.

Emerging Space Powers

The third group comprises the emerging space powers, which do not have independent satellite development, launch, and control capabilities. This group includes in practice all countries not included in the previous two groups, and it is divided into two subgroups: one that possesses basic infrastructure and space agencies, such as Pakistan, Brazil, and Australia, and the other that does not possess basic space infrastructure, such as most

65 Klein, "Space Strategy Considerations for Medium Space Powers," 3.

African countries. Due to the large scope of this group, it is impossible to review all the members, but rather their common and unique characteristics will be discussed.

From a military perspective, some of the emerging space powers possess space systems for security or dual use, such as communications and observation satellites, but due to their lack of technological maturity, are forced to seek the assistance from the more advanced space players to launch these systems and sometimes also to develop and operate them. Therefore, it can be assumed that these countries do not have more advanced military capabilities in space.

The emerging space powers operate more strongly in the diplomatic arena, either by expressing almost complete support for China and Russia's initiatives to restrict weaponization of space, or by actively participating in international initiatives, such as the code of conduct in space.[66] Despite the clear support of the emerging space powers for restrictions on the proliferation of space weapons, these countries have different interests for expressing this support.

Pakistan, which is in a decades-long conflict with India, has the more advanced space capabilities among the emerging space powers. Pakistan has expressed support for various international initiatives in the space arena but has expressed its unwillingness to bear the consequences of anti-weapons proliferation treaties or sanctions that may limit its efforts in space.[67] In contrast, Brazil, which is located in a region with less geopolitical tensions, supported and even participated in China and Russia's No First Placement of Weapons in Outer Space resolution,[68] but expressed dissatisfaction with the process of drafting the code of conduct for activities in space as well as

66 For example, in 2017, no developing country voted against "Further practical measures for the prevention of arms race in outer space," and only two (Ukraine and Georgia) voted against the proposal of "No first placement of weapons in outer space." See "First Committee Submits Six Drafts to General Assembly, One Calling for Immediate Start of Negotiations on Treaty Preventing Outer Space Arms Race," United Nations, October 30, 2017, https://www.un.org/press/en/2017/gadis3591.doc.htm.

67 Urooj Tarar, "Pakistan Opposes the Weaponization of the Final Frontier, Outer Space," *Daily Pakistan*, October 19, 2017, https://en.dailypakistan.com.pk/pakistan/pakistan-opposes-the-weaponization-of-the-final-frontier-the-outer-space/.

68 "UN Adopts Russian 'No First Placement of Weapons in Outer Space' Resolution," *Russia Beyond*, December 8, 2015, https://www.rbth.com/news/2015/12/08/un-adopts-russian-no-first-placement-of-weapons-in-outer-space-resolution_548679.

the content of some of its language.[69] In doing so, Brazil has positioned itself as an activist and advocate for the promotion of more powerful measures to restrict space weapons. Australia, which has a strategic alliance with the United States and relies on its capabilities in space,[70] supports the creation of a code of conduct for activities in space, inter alia with the aim of reducing the danger to the space environment and the accumulation of space debris.[71]

As we have seen, despite their support for diplomatic measures to restrict space weapons, emerging space countries operate according to various motives, due to their geopolitical situation, technological aspirations, or different security concepts. Although it is impossible to state that these countries want to discourage a space arms race out of idealistic motives, there is a need to map their different interests, which do not align with the relatively limited approach of "for or against" the weaponization of space.

Like the other groups, the standing of emerging space powers in the technological hierarchy is congruent with their activities in space. As the emerging space powers possess the most basic space capabilities, they support initiatives that restrict space weapons, either because they refuse to bear the burden of future harsher sanctions (in the case of Pakistan) or to maintain the security and safety of space which they aspire to join in the coming decades (as indicated by Brazil and Australia).

Israel

Israel has advanced space capabilities and is now capable of independently developing, launching, and operating advanced satellites (as illustrated by the "Ofeq" satellite series) and could be considered one of the medium superpowers. However, Israel does not have a formal national space strategy and relies on other countries to launch satellites into geostationary orbit. In the field of space weapons, Israel does not have a declared plan to develop anti-satellite means, but it has the technical ability to destroy satellites using the Arrow 3 missile intercept system.[72] In the diplomatic arena, Israel votes

69 Zahid Imroz, "Space Code of Conduct: Need to Re-analyse," in *Decoding the International Code of Conduct for Outer Space Activities*, p. 134.

70 Connie Agius, "Australia's Reliance on US Space Capabilities could Put Security at Risk, Defense Expert Says," *ABCnews*, February 23, 2018, https://www.abc.net.au/news/2018-02-23/australias-reliance-on-us-in-space-a-national-security-risk/9474122.

71 Dylan Welch, "Australia Joins Race to Defend Space," *Sydney Morning Herald*, January 19, 2012, https://www.smh.com.au/technology/australia-joins-race-to-defend-space-20120118-1q6k2.html.

72 Harrison et al., *Space Threat Assessment 2018*, p. 38.

with the United States against Chinese and Russian initiatives to limit the weaponization of space.

Israel operates in a manner that is consistent with its hierarchical position among the countries active in space. Although it does not operate aggressively in space, it continues to oppose initiatives to restrict the weaponization of space, as part of its strategic alliance with the United States, and tends to support the preservation of the existing balance of power in space.

Conclusion

Despite the growing discourse on the weaponization of space in recent years, the academic debate has remained limited and focuses on a relatively simplistic division between its proponents and opponents. For the purpose of reassessing this approach, this article presented a new division of the countries involved according to their technological standing in space. This division enabled the identification of different interests and approaches, which are inconsistent with the existing divisions in academic scholarship.

The space superpowers, which are positioned at the top of the technological hierarchy, express the most aggressive approaches to space weaponization in pursuit of supremacy (United States and China) or strategic parity (Russia). The medium powers have different interests, ranging from a desire to lead a new normative and security discourse (European Union), establishing regional power (India), to maintaining national security through strengthening the alliance with the United States (Japan). The emerging space powers also have differing approaches. Although the members of this group support restrictions on the weaponization of space, their motives are not directly compatible with the idealist perception of opposition to weaponization, as expressed in the current research literature.

Based on an analysis of the activities of countries that are peripheral to the dominant discourse, they appear to have a wide range of interests and approaches regarding the weaponization of space, which challenge the existing debate on this issue. Despite their differences, it is possible to identify a correlation between technological achievement and their determination on the issue of the weaponization of space. These differences should be taken into account in future research regarding the space arms race.

Sectoral Ability to Manage Cyber Risks in the Supply Chain

Gabi Siboni, Hadas Klein, and Ziv Solomon

This article presents the cyber risks that originate in the supply chain and the challenges that they pose. It examines a number of global methodologies and standards for managing cyber risks in the supply chain and proposes a model for concentrated sectoral management of the challenge so that the process of checking and authorizing suppliers will be streamlined. The proposed model has been found to be feasible in terms of the investment and pooling of resources as well as in increasing the general security level of the various sectors, thus raising the level of cyber protection in the Israeli economy as a whole.

Keywords: Cyber threat, cyber risk management, supply chain, cyberspace

Introduction

In July 2018, a research team from Microsoft identified an attack on a software company that was intended to implant malicious code in a legitimate software product and use it to reach thousands of other customers.[1] In this case, anonymous attackers managed to take control of the shared infrastructure of a software company that provided a PDF editor and another company

Prof. Gabi Siboni is the head of the Cyber Security program at INSS. Hadas Klein is a cyber researcher at INSS. Ziv Solomon is a cyber security consultant. The article is based on a research paper written by Gabi Siboni, Ziv Solomon, and Hadas Klein, "National Cyber Risk Management for the Financial Sector: Reducing Supply Chain Risks," INSS, December 2018.

1 "Attack Inception: Compromised Supply Chain within a Supply Chain Poses New Risks," Microsoft Defender Research Team, July 2018, https://bit.ly/2UcVsGB.

that provided an installer, so that the installer would install the malicious code along with the PDF editor. An investigation showed that the software company that provided the PDF editor had not been attacked at all. Rather, its product had been replaced through interfering in the process at the second software company, which provided the installer. This example is an indication of the large amount of resources that attackers invest in order to reach their targets through the supply chain.

A "supply chain" is defined here as "a system of factors involved in the supply of a product or service, including service providers, software and information system suppliers, hardware suppliers, and so forth." In the current global era, which is characterized by technologically complex goods and services and support from a wide variety of suppliers for each product or service, it is necessary to ensure cyber protection for the suppliers of each organization. The example provided above is one of many where an attacker exploited security breaches at an organization's supplier in order to penetrate the computer network of the organization it sought to attack.

The optimal handling of cyber challenges in the supply chain requires a concrete response to the needs of the organization and the sector to which it belongs, as well as a response for organizations that are identified as Israeli because of their exposure to cyberattacks of an anti-Israel nature. Many organizations in Israel are subject to guidelines from regulators such as the Banking Supervision Department; the Capital Market, Insurance, and Savings Authority; the Ministry of Health as the regulator of the various healthcare organizations in Israel; and more. Protecting such organizations requires an array of defensive components, among them a level of technological protection and work procedures, including those that relate to cyber threats in the supply chain. The more organizations successfully identify the threats and take the necessary measures to mitigate them at an earlier stage, the more their overall defensive level will increase.

This article discusses the challenge of dealing with cyber risks in the supply chain and provides general recommendations for dealing with them, while also addressing relevant global standards, Israeli regulations, the relevant threat map in the supply chain context, existing methodologies, models for managing suppliers in the supply chain, and possible approaches. The article provides examples from the Israeli economy that could have a possible connection to the subject.

Theoretical Background

A number of models for managing supply chain risks can be found in both industry and in the professional literature. In the book *Purchasing and Supply Chain Management*, three categories of suppliers are outlined: strategic suppliers that are extremely important to the purchasing company and for which it is difficult to find a replacement; preferred suppliers that are important to the purchasing company but can be replaced with some effort; and transactional suppliers, which can be replaced within a short time.[2] In addition to the proposed types of suppliers, this article provides a survey of several supply chain management models in entities relevant to our discussion.

Deutsche Telekom has a four-stage methodology for managing the supply chain for more than 30,000 suppliers in more than 80 countries.[3] Its aim is to mitigate the risks and encourage the company's suppliers to improve their work methods. In the first stage, all potential suppliers with an annual order volume of more than 100,000 euros are surveyed about topics such as human rights, corruption, environmental protection, and employment health. All suppliers are required to be surveyed again after three years. As business relations continue, the company asks the suppliers that are strategically relevant and/or those at high risk to provide wide-ranging information on their work methods through the information system. In the second stage, these declarations are assessed on the basis of additional background information and a focused study. For suppliers at higher risk, additional information is required, and site visits are made. The efficiency of the review increases, and duplicate visits are avoided by cooperating with 13 additional companies that implement the process through Joint Audit Cooperation (JAC).

In the third stage, the suppliers are classified and assessed based on the information supplied and the results of the audits. According to Deutsche Telekom, the company cooperates closely with its suppliers in order to deal with serious problems that are identified. In the fourth stage, a development program is implemented and workshops are held for suppliers. In cases where a supplier significantly ignores the company's requirements, higher authorities within the supplier are involved and the process intensifies. More

2 W.C. Benton, *Purchasing and Supply Management* (Irwin Professional Publishing, 2nd edition, 2009), Ch. 8.

3 "Corporate Responsibility Report," Deutsche Telekom, 2017.

serious sanctions are occasionally implemented in order to spur the handling and closure of gaps in accordance with Deutsche Telekom procedures.

A document by the Information Technology Infrastructure Library (ITIL) presents a two-dimensional model for classifying suppliers—risk and impact vs. value and importance.[4] The higher the value of the dimensions for a particular supplier, the more significant that supplier is. This model groups suppliers into four classifications:

- Commodity: These are suppliers of goods and services that have a low value and/or are readily available (such as paper or printers).
- Operational: These are suppliers of operational goods or services, generally managed by a junior operations manager, and require infrequent but regular performance reviews of contact people (for example, internet hosting service providers, which provide hosting space for a website that has little influence).
- Tactical: These are suppliers that have significant commercial activity and business interaction, generally led by middle management, and require regular performance reviews as well as ongoing improvement plans (for example, a hardware maintenance supplier who provides solutions for server hardware failures).
- Strategic: These are suppliers with whom confidential or strategic information is shared, who are generally under the responsibility of senior management levels, and require regular and frequent reviews (such as a network services supplier that provides global network services and support).

A more simple pyramid model for classifying suppliers is used by the United Utilities company, which provides water in northwest England, totaling about 1.7 billion liters per day. This model divides suppliers into four groups: partner, strategic, preferred, and approved.[5] The more complex the company's dependency on the supplier is and the higher the value of the goods or services are, the more significant the supplier is. The model makes it possible to define the company's requirements from the supplier against the following performance indices: customers, regulation/law, sustainability, efficiency, safety, and so forth.

4 "ITIL Service Management," Version 3, § 4.7.5.2, https://www.hci-itil.com/ITIL_v3/books/2_service_design/service_design_ch4_7.html.

5 "Suppliers," United Utilities, https://www.unitedutilities.com/corporate/about-us/governance/suppliers.

Another methodology for classifying suppliers appears in the Amway—Europe Supplier Information Portal model.[6] According to this methodology, the type of relationship developed between supplier and customer depends on the strategic importance of the product or service being provided, and the talents, abilities, and performance of the supplier. Every supplier is measured and classified according to the model's criteria. This ensures that each supplier will undertake focused activity that is planned especially to develop, improve, or streamline operational performance. The criteria that are used to measure each supplier include performance (order, inventory, supply, service, and quality control); product/service (innovation, development, marketing advantage, economic value); and financial (dependency, alternatives, financial risks, and pricing). The evaluation of these criteria and its results lead to the formulation of specific programs with the supplier to achieve the operational and performance levels required for business purposes.

In Israel, a number of activities have been implemented to improve the management of cyber risks in the supply chain. One of them is the work of the National Cyber Directorate on developing a supply chain protection method. This method includes a suppliers' questionnaire, as well as a control and auditing method accessible through a portal. The intention is that market forces will develop the use of the method and the portal and not to impose it upon suppliers. In addition, the Ministry of Finance relies upon the Unit for Cyber Regulation and Continuity of the Financial Supply Chain[7] to ensure the resilience of the financial system against cyber risks and the continuity in the financial supply chain, maintain the stability of the system, and meet the service targets for the public and the government. Currently, the unit's activity vis-à-vis the financial system's suppliers is voluntary and free of cost. The activity vis-à-vis the suppliers includes a review of their activity, mapping and assessment of risk and existing controls, and formulating a risk mitigation program. It should be noted that this activity vis-à-vis the financial system suppliers is relatively new and still in its early stages.

A number of approaches from other spheres in the Israeli economy may be relevant to the discussion here, such as a national classification of suppliers in

6 "Supplier Segmentation," Europe Supplier Information Portal, http://supplier.amway.com/europeanportal/suppliersegmentation/SitePages/Home.aspx.

7 "The Unit for Cyber Regulation and Continuity in the Financial Supply Chain," Ministry of Finance, http://mof.gov.il/Units/CyberEmergenciesSafetyDraft/Pages/CyberSeriesUnit.aspx.

other industries (such as building contractors), and an infrastructure process performed or guided by one entity for employees in other entities (such as the government unit for determining security compatibility in the General Security Service). In addition, toward the end of 2018, the National Cyber Directorate in the Prime Minister's Office established a national database,[8] in which any company can check its cyber protection level, information safety, and cyber protection fitness; using the data it obtains, it can receive recommendations on how to prepare, change, and improve. The first module in the system, called YUVAL (Hebrew acronym for organizational targets and controls), is intended to handle the economy's supply chain. The system is based on a defensive doctrine for organizations in the Israeli economy, which was published by the National Cyber Directorate. The challenge facing the officials of the National Cyber Directorate in specifying the system was the need to formulate a methodology to protect the supply chain. The purpose of the initiative was to raise the security level in the Israeli economy, in addition to economic streamlining. As a result, a uniform and orderly system of questions and controls was built, with the aim of creating trust between organizations and suppliers in the economy.

The ISO 27001 standard is a common international information security standard (the standard adopted in Israel is "IS ISO27001"), which institutionalizes the management of organizational information security and deals with the ongoing process involved in establishing and methodically improving the system.[9] Chapter 15 of the standard deals with supplier relations. The controls in this context are detailed in the ISO 27002 standard.[10] Pursuant to this standard, the organization is required to set a documented policy for suppliers to which they will agree. In addition, the policy must focus on the relevant processes that take place at both the organization and the supplier's internet sites. These include identifying the types of suppliers that are allowed access to the organization's information; defining the life cycle for managing supplier relations; defining the types of information accessible to the different types of suppliers; monitoring and controlling access; defining the minimal security requirements according to type of information and type of access so

8 "The National Cyber Directorate Established a System for Protecting the Supply Chain in the Economy," *People and Computers* (January 2019), https://www.pc.co.il/news/282242 [in Hebrew].

9 "Information Technology – Security Techniques – Information Security, Management Systems – Requirements," *ISO/IEC 27001*, 2013.

10 "Code of practice for information security controls," *ISO/IEC 27002*, 2013.

that they serve as a basis for agreements made with every relevant supplier; defining how to handle security incidents and malfunctions connected to the supplier; defining each side's responsibility; and increasing the awareness and training of employees. In addition, a written agreement should be procured of security requirements for each supplier that has the ability to access, process, store, and/or create communication, or provide information or information technology components for the organization. Furthermore, the agreements with the suppliers must include security requirements based on the risks within the goods and services supply chain. The standard also emphasizes the need to manage, monitor, and make changes concerning supplier relations and the supply chain.

Another relevant standard is NIST 800-161, which aims to provide a guide for US federal agencies to help them identify, evaluate, select, and implement risk management processes and controls for the information technology supply chain.[11] The processes and controls published in this comprehensive and detailed standard are subject to change or expand due to regulatory changes, organizational policy, guidelines, and so forth. The standard notes that organizations must develop strategies to mitigate information technology supply chain risks, which are specifically adapted to them and influenced by business needs and tasks, threats, and the operating environment. The standard emphasizes the complexity of the information technology supply chain, and the fact that suppliers have their own suppliers, which makes it difficult for the organization to see, understand, and control the situation. This difficulty increases if the supplier is not a direct supplier. The standard also notes that the handling of risks within the information technology supply chain must be assimilated within the broader organization-wide risk management processes. The controls detailed in this standard relate to the following topics: access control, preparedness and training, expression and responsibility, authorizations, configuration management, continuity, identification and verification, response to events, maintenance, media protection, physical security, planning, application management, employee reliability, control of changes, risk assessment, purchasing of systems and services, protection of systems and communications, and completeness of systems and information.

11 Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," NIST Special Publication 800-161 (April 2015).

Similarly, the General Data Protection Regulation (GDPR) standard, which was set by the European Parliament, the EU Council, and the European Commission, applies to all EU countries concerning the collection, maintenance, and transfer of individuals' personal data and sets out uniform rules for maintaining privacy.[12] The standard was approved on April 27, 2016 and has been enforced since May 28, 2018. It replaces the European directive on data protection (Guideline EC/95/46), which was established in 1995. The standard applies to all data processing organizations of information carriers in EU territory, even if they do not operate in EU territory. This standard imposes prohibitions and restrictions on the transfer of information outside of EU territory due to concern of violations that may occur in regions where privacy is not properly protected. One of the standard's principles is accountability. In cases of organizations that use suppliers as outsourcing for processing personal information (such as producing salary slips), they must ensure that proper security arrangements are in place and that they are consistent with requirements over the entire supply chain, including their suppliers.

The Bank of Israel issued a directive, requiring the banking corporation to determine which operations are essential in order to ensure that external parties take the required measures to reduce its exposure to cyber risks.[13] The directive also deals with "the banking corporation's responsibility for maintaining a secure working environment vis-à-vis material service providers and its obligation to manage the cyber risks appropriate in regard to these service providers' activity on their own premises, on the banking corporation's premises, and in material providers' interfaces with the corporation." The directive relates to the need to map and identify "material service providers,"[14] giving the banking corporation the ability to demand that a provider fulfills the security guidelines and maintains the banking corporation's enforcement and control capability vis-à-vis the provider.

12 "GDPR – General Data Protection Regulation," The European Parliament, 2016.

13 "Supply Chain Cyber Risk Management," Bank of Israel, 2018.

14 The directive defines "material service providers" as "external entities that belong to a banking corporation's supply chain (such as companies that support capital-market trading services), which are material to its activity and/or expose it to potentially high cyber and information-security risks that, when they eventuate, make it possible to attack the banking corporation or impair its activity." The reference is to outside entities that provide services to the banking corporation only in areas connected with information security.

Similarly, the Capital Market, Insurance, and Savings Authority in the Ministry of Finance published a circular that applies to entities that manage the public's money, such as pension and trust funds, including insurance companies and investment houses.[15] Section E of the circular relates to the issue of outsourcing, specifies the cyber protection requirements in outsourcing agreements, and requires that the entity define a procedure that details the cyber protection requirements vis-à-vis outsourcing risks and in relation to supply chain security. In addition, a service provider must be prohibited from transferring to a third party any information it receives within the framework of its interactions, or from using information to which it is exposed due to interactions for any other purpose that is not connected to its contractual obligations. The circular also sets out that when it is necessary to transfer data, access to itemized data shall be controlled, without copying the entire database.

The Privacy Protection Authority's Privacy Protection Regulations (Information Security), which came into effect in Israel in 2018,[16] are based on the assumption that granting access to an external entity creates unique risks. These regulations require that before implementing any interaction with an external entity, any inherent information security risks must be examined, and if the risks are too high when considering the sensitivity of the information, then outsourcing should be completely avoided. The regulations also determine that the following must be defined between the company and the external entity: the information the external entity is permitted to process and for what purposes; which systems it is allowed to access; the type of processes it is permitted to carry out; the duration of the interactions; how the information will be returned to its owners at the end of the interactions; how the information security regulations will be implemented; and the requirement of the authorized employees of the external entity to maintain information confidentiality.

As shown above, standards and regulations for managing general supply chain risks vary throughout the world, indicating global awareness of this issue. Awareness of cyber threats that originate in the supply chain is also

15 "Cyber Risk Management at Institutional Investors," Ministry of Finance, August 2016.

16 "Privacy Protection Regulations (Information Security), Regulation 15—Outsourcing," Knesset, May 2017.

prevalent, and these threats pose a number of challenges that require special attention.

Cyber Threats and Supply Chain Risks

According to the British Computer Emergency Response Team (CERT), four types of threats to the supply chain can be discerned, based on real incidents.[17] The first is an attack on the system through a third-party supplier. In this specific real incident, the attacker attacked an industrial control system (ICT), which a third-party supplier had installed in the organization. The second threat is an attack on commercial websites implemented via website builders and designers. In the specific real incident, the attacker struck financial websites through scripts that were transferred from digitization and design companies. The third threat is an attack on third-party companies that store data, often sensitive information, for other companies. The fourth threat is a "watering hole" attack, which refers to implanting malicious code in sites that are broadly used by the targets of the attack, so that accessing those sites will lead to an attack on the systems of targeted users.

The ISO 27036-1 standard also provides examples of threats in this context:[18] A supplier's physical access to the customer's sites; access to the customer's information or information systems at their sites by the supplier's employees; remote access of the supplier to the customer's information or information systems; processing the customer's information by the supplier outside of the customer's sites; using the customer's applications on the supplier's infrastructure; hosting the customer's equipment at the supplier's sites, and storing the customer's data (including backups) at the supplier.

A report by a cyber intelligence company reviewing significant cyberattacks that took place between 2016 and 2018 in Israel and abroad noted that the financial sector (banks) is a main target for skilled criminal and government hackers, while core banking systems, such as Swift and the ATM network, have in recent years become a preferred target for hackers.[19] The report also notes that in the past decade, companies and organizations have developed front-end protection systems vis-à-vis the internet but have invested less in

17 "Cyber-Security Risks in the Supply Chain," CERT UK, 2015.
18 "Information Technology – Security Techniques – Information Security for Supplier Relationships," *ISO 27036*.
19 "Report on Cyber Events, 2016–2018: Exploiting the Swift Supply Chain," Clearsky, March 2018.

protecting their contacts with suppliers. In this way, a cyberattack originating in one of the links in the supply chain has become an efficient way to gain a foothold into penetrating strategic organizations. The hackers exploit the relative ease of accessing small companies and organizations with a weaker cyber defense system and use them to penetrate target organizations of critical importance. Hackers also exploit the fact that some secondary suppliers of the critical organizations have direct or easier access to the organization and through them penetrate the critical organization. An attack via the supply chain has become more sophisticated and includes the use of legitimate software updates to distribute malware. Since organizations are unable to inspect software updates, the level of risk of damage to the core systems of organizations and countries has increased significantly.

According to the report by the cyber intelligence company, three main insights can be made from the current situation in terms of how organizations deal with the threats:

1. Building a new defensive model: The traditional model, which mainly involves increasing security of the organization's external "boundaries" while leaving the core of the organization unprotected, is no longer appropriate. In recent years, this concept has led to a lack of security for the internal systems. Currently, many organizations are investing tremendous resources in strengthening their defensive parameters but do not sufficiently budget or invest in their internal security. The lack of balance in investment leads to a situation where if a hacker succeeds in penetrating the organization, he can easily spread out and operate within it.

2. Strengthening protective mechanisms between organizations and secondary suppliers: It is extremely difficult to protect the connection between organizations and companies and the secondary suppliers who provide them with services and information. This is even more true when protecting information against companies that provide cloud-based computing services. Some information providers in the banking sector are international entities (such as Bloomberg and Reuters); clearly, the ability to affect their information protection systems is relatively inferior. Banks and regulators have a greater ability to affect and control the security systems of suppliers in Israel, but this requires the setting of clear standards and defensive systems for the information security systems that are required of the secondary suppliers who connect directly to the core banking systems. At the same

time, the protective systems must be strengthened, and the internal systems of the banks and financial institutions need to have limited exposure to secondary suppliers.

3. Deploying a back-end protection system similar in nature to the front-end protection system: It is recommended to build a monitoring and protection system vis-à-vis secondary suppliers, similar in nature to the company's front-end protection system, including the establishment of a DMZ, a strong identification system that includes multi-factor identification, an information filter system, a "sandbox" system to test the results of software update installations, and a monitoring system that includes keeping data for a long period and constantly monitors the connection with the secondary suppliers. This defensive system should also be deployed against the company's subsidiaries, as working with subsidiaries that have separate protection systems and separate software systems puts the company at risk just like with a secondary supplier.

The National Cyber Directorate's document on "Outsourcing Risks in the Supply Chain" lists the following risks as unique to the supply chain: the insertion of software or hardware that is infected with malware; malicious action by a maintenance worker; and malicious action through a remote maintenance channel.[20] The document proposes means to mitigate the risk by integrating it into the organization's risk management; supervising maintenance people by monitoring their network activity, accompanying them while they are on-site, requiring incoming personnel to wear identification tags, monitoring the remote maintenance channel, and disconnecting it when no longer needed; and concealing the specific end-target as part of purchasing for large organization—for instance, when purchasing for a very large organization, of which only parts of the organization are sensitive, it is possible to eliminate the destination of the purchase on the order.

A document by the SANS Institute addresses the required organizational preparedness given the cyber risks from the supply chain.[21] The document proposes that organizations build a supplier management program based on four components: identifying and defining the important suppliers; precisely defining the agreements for each supplier; setting and implementing guidelines and controls; and organizational integration. The document also proposes

20 "Outsourcing and Supply Chain Risks," National Cyber Directorate**,** May 18, 2017.
21 "Combatting Cyber Risks in the Supply Chain," SANS Institute, 2015.

that organizations act according to best practices (in terms of personnel, processes, and technology) in order to minimize their exposure to supply chain risks. Finally, the document summarizes the main components of the supply chain security program according to basic and comprehensive components, cross-referencing each of the three components as in the following table:

Table 1: Main Components of the Supply Chain Security Program

Component	Basic	Comprehensive
Personnel	Background checks	Security requirements appearing in contracts
Processes	Basic surveys and control and risk surveys of the suppliers	Implementation of the full supplier management program
Technology	Network segmentation and monitoring	Code review and inspection of vulnerabilities of third parties, in-depth monitoring, security threat analysis, and reliance on intelligence

A threat to the organization through an attack on its supply chain can occur through a wide variety of mechanisms. These include penetration of the systems of a supplier with relatively low-level protection (but with access to the organization's systems), through which the organization's systems are breached; use of legitimate software updates to distribute malware; and so forth. These are not theoretical threats for organizations but are based on a large number of actual incidents that occurred in Israel and abroad and damaged the organizations by exploiting their supply chains. The complexity of the threat, the wide variety of possible scenarios, and the increasing power of the hackers necessitate organizations to take significant defensive measures to deal with the challenge and mitigate the risks.

The above survey shows that there is much discussion of cyber threats in the supply chain. However, this discussion is inefficient, since each entity must fulfill the guidelines and recommendations on its own, and each supplier must fulfill his customer's requirements separately and invest a tremendous amount of resources in implementing the various requirements, which by nature are not uniform.

The Proposed Model

A critical component in supply chain risk management is the ability to survey cyber risks among suppliers and build a work plan that will make it possible to close gaps through the appropriate controls. In general, this article focuses on formulating a broad, sectoral process that will enable suppliers to receive certification from a central testing entity. The article is based on the assumption that organizations belonging to the same business sector have many common suppliers. For instance, most banks in Israel use the same printing supplier, but currently each bank separately surveys the same printing supplier.

The proposed model is all organizations that use the supplier will finance the certification processes, thereby making it possible to pool resources and invest greater resources in the entire certification process. Different levels of certification will take place according to the characteristics of the supplier and the requirements of the organizations in that sector. This way the organizations will rely on the work of the testing entity, and the suppliers will be saved repeated inspections each time by a different entity. The proposed model can serve as a basis only; if necessary, the various organizations can expand their requirements of their material service providers in the supply chain, for example by imposing more stringent requirements or even requirements to install additional monitoring systems at the supplier's premises.

The risk survey of the suppliers of addressing cyber risk in the supply chain can be carried out through two main operational alternatives:

1. Self-management by each organization in the sector: This is essentially the current situation, wherein each organization acts independently vis-à-vis the suppliers on its supply chain. Each organization also determines its requirements from each supplier or group of suppliers.

2. Central sectoral management (for all or most of the organizations in the sector): To realize this, it will be necessary to establish a main entity that will be jointly owned by the companies operating in a single sector. The purpose of this entity will be to implement cyber risk surveys and monitor performance among the sector's suppliers. This entity will be responsible for managing the surveyors (whether they carry out the survey directly or through surveyors working for the entity, or external surveyors); dictating the survey requirements; monitoring and tracking the implementation of programs to correct the gaps raised in the surveys; and revising the

inspection methodologies and tools used according to the concurrent needs and developments in the field. In addition, the entity will need to discuss the question of controlling foreign suppliers and how to implement the inspections and controls for them as well. One example is the MASAV/Shva company that was established by the large banks in Israel and provides services to the entire banking sector.

The requirements can be based on accepted standards or on the classification of suppliers as proposed by the National Cyber Directorate. These two options address a number of additional aspects:

Improved sectoral cybersecurity: The first aspect addresses the question of which alternative will increase the level of cybersecurity and stability in the specific sector. Given the analysis conducted, the answer is clear. Centralized management of the suppliers cyber risk survey has a variety of advantages: establishing a specialized professional entity will enable it to methodically develop knowledge and to improve and enhance its abilities for the entire sector; a uniform survey of suppliers will allow for setting cybersecurity benchmark requirements for the entire sector, while normalizing the requirements from suppliers in the supply chain; intensifying the requirements from suppliers will better enable the sector to enforce improved controls, since the requirements will be developed by a centralized entity; the burden on suppliers, who are currently dealing with separate risk surveys and requirements from each organization in the sector, will be significantly lightened; and the pooling of resources will increase the quality and depth of the survey and as a result, will improve the risk management level of the suppliers.

Economic aspects: The economic aspects are worth examining and will be particular to each sector. Establishing the capability of conducting a centralized risk survey could lower the costs for each organization while also improving the survey's effectiveness, given the increased professionalism of the surveying entity in the sector.

Anti-trust considerations: In this context, we must examine the extent to which joint activity by the organizations in the sector vis-à-vis suppliers in the supply chain will deviate from anti-trust regulations. According to our analysis, establishing a centralized surveying entity does not affect this component and rather would improve the level of security and stability of the specific sector. In addition, the survey process can ascertain that sensitive organizational information is not shared with other organizations. This is

already happening today, for instance in the Financial Cyber Center in Beer Sheva, as well as in organizations within the global financial system, such as Federal Financial Institutions Examination Council (FFIEC) and others. Clearly, when establishing the centralized body, it will be necessary to regulate a variety of restrictions that will apply to the survey process. As we understand, it will be possible to create regulations that will respond to the requirements of the various regulators.

The opening of new suppliers: Various organizations are already dealing with long processes that involve the opening of new suppliers in the system. These processes last for quite a number of months. A centralized entity could shorten the process and even enable suppliers to request a risk survey and qualification in advance.

The above shows that establishing a centralized entity will significantly improve the level of cybersecurity in a given sector and enable the constant development of knowledge of cyber risks. Moreover, centralized management will increase the strength and impact that the surveying entity has on the suppliers (since it will represent all or most of the organizations in the sector, and not just one), improve the professionalization of the staff (a specialized entity at the sector level), lower overhead (management, physical, and so forth) for each organization, and lead to significant savings in the resources required to survey all components of the supply chain. It should be emphasized that the responsibility for a cyberattack due to a failure in the supply chain will remain with the entity using the supplier, since the aim of the proposed model is only to streamline and improve the process and its associated costs.

Conclusion and Recommendations

From an economic perspective, it is recommended that the surveying of cyber risks in the supply chain be managed by a centralized body by sector. An entity that surveys cyber risks will represent all organizations in the sector and their requirements, and not just one organization, although a single organization will be able to add specific requirements for a certain supplier, if necessary. In order to establish and operate the central entity, a differential pricing mechanism among the organizations in the sector is proposed, reflecting each organization's volume of activity in the initiative.

The proposed model also has risks, which will need to be comprehensively examined and managed accordingly. These risks include, inter alia, potential

harm to the market of the companies that currently provide cyber surveys (it is possible that they may stop providing these services, since fewer companies will be required once the "testing entity" is selected in each sector), which will reduce competition in the industry. When one entity conducts the entire survey process, there is a risk that not all vulnerabilities will be discovered. This is in contrast to having various surveyors that provide an additional "eye" and sometimes discover vulnerabilities that are not discovered by a single centralized surveyor. Another risk concerns the level of protection of this entity and its possible penetration by a malicious actor, which could endanger the entire sector. Finally, there is the potential of a conflict of interests, should the inspecting entity also be responsible for correcting the vulnerabilities. Obviously, this risk is relevant only in a case where the central entity chooses to use outside suppliers to conduct the survey on its behalf.

Within the context of Israel, it is recommended that the National Cyber Directorate conduct an in-depth process examining the proposed model. It is preferable that the process begin with mapping the sectors for which the model is relevant (sectors where it is assumed that a significant portion of the suppliers are shared suppliers). It is then worthwhile to conduct a feasibility study, similar to the financial sector, as presented in this article. After that, we recommend defining the relevant requirements from the various suppliers and the risk survey processes for each sector.

Technology and Intelligence: Changing Trends in the IDF's Intelligence Process in the Post-Information Revolution Period

Jasmin Podmazo

This article addresses the changes that have occurred in the intelligence work of the Israel Defense Forces (IDF) in the period following the information revolution of the 1990s, and it examines how technological developments during this period have improved the intelligence process and how they have affected intelligence surprises. The article describes the effect of technological developments on each stage of the classic "intelligence cycle"—collection, processing, analysis, and dissemination. It also provides a comparative analysis of the processes before and after the information revolution, based on open sources. The technological changes have resulted in three main trends: 1) way in which classic intelligence work is done is changing; 2) the access of operational units to intelligence has improved; and 3) the room for intelligence surprises has become increasingly narrow.

Keywords: Intelligence cycle, technology, information revolution, collection accessibility, jointness

Introduction

The information revolution, which began in the 1990s, is the most significant transformation since the industrial revolution of the nineteenth century. Like

Jasmin Podmazo is a master's degree student in the Security Studies Program at Tel Aviv University.

the latter, it had a profound effect on the economy, politics, and technology. The main feature of the information revolution is broad access to knowledge and rapid connectivity that enables the global transfer of information in the shortest amount of time. This is accomplished through an evolutionary process of change and innovation, mainly in the technological sphere. During the information revolution, the information technologies (IT) came of age and formed the basis of the technological developments of this century. It is hard to distinguish between the end of the information revolution and the period that followed, which constitutes a further evolution of technology and information. This article will focus on the first two decades of the twenty-first century, which will be referred to as "the period following the information revolution of the 1990s."[1]

Today, in an era of information overload and of dynamic and changing arenas, intelligence work done in Israel and abroad faces new, extremely complex challenges. Technological innovation and wise and informed management of the voluminous information available are critical for building the best intelligence picture, which ultimately affects our ability to deal with various adversaries and our deterrent capability concerning unusual events.

The classic function of intelligence is, first and foremost, to clarify the existing situation behind enemy lines. Therefore, high-quality and precise intelligence is tremendously important for dealing with any type of surprise both in times of routine and emergencies. The prevailing view is that high-quality intelligence is a critical source of power in the battlefield (before and during war). Modern technology, which creates advanced information collection and processing capabilities, has enabled us to learn about the enemy and reduce our uncertainty about it. Military supremacy is, to a large extent, gained due to high-quality and precise intelligence about the other side. Intelligence makes it easier to gain control of the field and to prevent the enemy's actions in advance. The more precise the intelligence is, the more focused the operations against the enemy it will enable while reducing peripheral damage. In addition, political and military decision makers rely

1 It is common to attribute the information revolution to the period spanning the end of the 1990s and the beginning of the 2000s, with the technologies developed then influencing the processes taking place around the world today. However, there are those who argue that we are now in a different period, possibly even the next revolution, which features the increased use of cyber and unmanned tools in the field of combat. From an historical perspective, the current decade may be only a stage in the revolution that will remain with us in the coming years as well.

on intelligence as it allows for better control over events both before they happen and as they are taking place. We must remember, however, that the intelligence process is always exposed to potential failures, particularly cognitive ones, which are an inseparable part of the thought and decision-making processes in conditions of uncertainty.

The information revolution of the 1990s and the technological developments in the world of intelligence in the period thereafter significantly improved the ability of intelligence agencies to provide responses to research questions and to build a reliable and optimal picture of the enemy. One of the challenges facing intelligence research today is how to maximize the information and develop technological tools for dealing with it. The information revolution has also significantly affected the other side: The adversary is not resting on its laurels and is constantly working to gather information on the other side and develop tomorrow's tools of combat. Moreover, the enemy is learning about the capabilities of the other side and changing its own behavior accordingly, making it more difficult for the other side to gather intelligence about it.

This article seeks to understand how technological developments in the field of intelligence in the period following the information revolution of the 1990s have improved the intelligence process, including the handling of surprises. The article will examine the changes that have taken place in the wake of the information revolution and the cornerstones that have formed the basis of intelligence work: collection, processing, analysis, and dissemination. Specifically, the article will focus on changes that have taken place in the IDF's intelligence branch in the past two decades. Although the focus here is on the changes that have occurred in each stage of the Israeli intelligence cycle, similar processes taking place elsewhere should not be ignored. The IDF is a single test case within a much broader context of technological change in military intelligence processes in the United States, Britain, China, and elsewhere since the 2000s.[2]

The discussion of each cornerstone will include examples of the effects of technological developments on the ability of the intelligence agencies to build a full and reliable picture that enables warnings and identification of potential surprises. The article will analyze a number of test cases and will

2 About the effect of technological developments on the various intelligence stages within the US intelligence community, see Margaret E. Kosal, ed., *Technology and the Intelligence Community: Challenges and Advances for the 21st Century* (Springer, 2018).

argue that the technological developments have a positive impact on how intelligence work is conducted. At the same time, the age of information overload presents challenges in separating the grain from the chaff and sometimes requires organizational adjustments and changes in order to provide the full intelligence response. Moreover, dealing with an adversary that learns and continues to constantly improve also requires proper adaptations.

On Intelligence Work in the Post-Information Revolution Era

Technological capabilities in the field of information have grown and strengthened since the early 2000s until now following the information revolution. The flood of information, accessibility, and rapid global connectivity have created new challenges. Within this framework, we can identify two main trends that are mutually dependent. The first trend relates to the change in how technology for creating information is used, and as a result, the exponential increase in the quantity of available information. The second one relates to technological developments in the field of information analysis, resulting from the need to analyze and process large quantities of information in short periods of time.[3]

One of the more significant and influential developments in the field of information processing is the Big Data revolution. The world of big data developed as a result of a number of parallel technological developments: 1) improved ability to gather large quantities of information with a wide variety of sensors, which led to increased data storage capacity; 2) immense growth in the quantity of information throughout the world, due to the increasing use of technologies that leave a digital signature; and 3) improved computational ability, enabling rapid and parallel processing and analysis of large quantities of information.[4]

According to the classic approach, there are a number of stages in the intelligence process known as the "intelligence cycle": information collection, processing of the material collected, analysis of the materials, and dissemination of the intelligence product to its consumers. The stages

3 Lt. Col. T., "Intelligence Derivatives of the World of Big Data," in *Intelligence in Theory and in Practice*, no. 3 (May 2018): 24–32 [in Hebrew].

4 M., deputy principal of the Israel Security Agency's school of intelligence, "Angels in the Skies of Berlin": New Intelligence Questions in a World Steeped in Data," in *Intelligence in Theory and in Practice,* no. 3 (May 2018): 55–60 [in Hebrew].

repeat themselves in a circular fashion (see figure 1 below) and are directed by the essential elements of information (EEI) sought, in other words, by the research questions that must be answered. The process begins with analysts sending questions regarding EEI to information collection personnel, and then those personnel continue the process by working to bring in the required information. In the next stage, the raw material is processed, and it is then disseminated to its consumers.

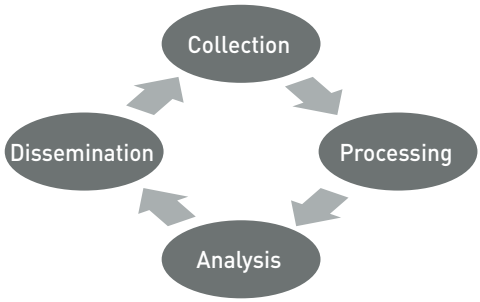

Figure 1. The intelligence cycle

When we examine the information revolution's effect on the classic intelligence cycle, we can see changes in each stage of intelligence. The clear trend in **intelligence collection** is the growth and improvement of cyber capabilities, which is the newest dimension of warfare. In the digital age, many types of information can be converted into bytes, which are connected to various information networks. In this kind of world, where everything is connected on the network, the basic assumptions of intelligence work in the fields of information and knowledge change. The quantity of information that is currently available to intelligence personnel creates a new challenge in terms of utilizing it: filtering out the information that is relevant to the research questions. Moreover, in the digital age, intelligence personnel potentially have accessibility to collect information and must have new skills to mine it.

Intelligence agencies today are flooded with information from the various sensors deployed in areas of interest and from access to databases in cyberspace that are constantly being filled and renewed. In places where access to information is complex due to security and encryption parameters, the job of the intelligence personnel is to develop cyber tools to exploit security breaches and weakness on the other side. The main challenge,

however, is the storing of large volumes of information, which involves considerable costs. Therefore, Israel's Military Intelligence Directorate has decided, for example, to not allow certain intelligence materials into their databases—despite the resources invested and risks taken to obtain those materials—and also to limit the duration for which materials are to be kept. This method poses challenges for researchers, since it limits their ability to ask intelligence questions based on learning processes over time.[5]

Intelligence collection also has developed in the field of satellites. Satellite capabilities make it possible to obtain pictures from all over the world through advanced optical systems, aiding intelligence research of distant sites of interest. Technological developments in the field of photography and optics have resulted in high-quality products with high resolutions and are used in deciphering during site analysis.

In the field of satellite-based visual intelligence collection, the information revolution enabled the transition from the analog era to the digital age. The analog era was characterized by a lack of raw material (imaging)[6] and long manual processing, while the digital age has enabled a quicker processing time and a better quality of the raw material. Today, a wealth of satellite imagery is available at resolutions that are constantly improving, at various wavelengths (multispectral and radar), and covering vast areas.[7] Multispectral satellites, for instance, help provide a response to complex EEIs, helping to study the adversary who tries to maintain a low signature profile and in complicated areas, either densely urban or covered with vegetation. For example, imagery of various wavelengths makes it possible to identify a depot of metals camouflaged by vegetation and to find hidden launch sites in a forested area. Another type of satellite used in intelligence is the Synthetic Aperture Radar (SAR) satellite, based on controlled transmission of electromagnetic radiation. The main advantage of these radars is the ability

5 Lt. Col. T., "Intelligence Derivatives of the World of Big Data," 27–28.

6 Imaging is a visual presentation of a picture, obtained through various methods, tools, and types of measurement that are not necessarily optical; that is, they are not necessarily based on visible light.

7 Lt. Col. A., "Geographic Intelligence – From Paper Napkin to 'Geo-Network'" in *The Challenges of the Israeli Intelligence Community*, ed. Shmuel Even and David Siman Tov (Tel Aviv: INSS, 2018), p. 99 [in Hebrew].

to generate images of a given area at any time and under any weather and visibility conditions.[8]

In recent years, space has become increasingly filled with satellites, with the number today almost two-and-a-half times greater than it was two decades ago.[9] The information collected by the satellites reaches intelligence agencies in accordance with EEIs. Geographical applications make the information directly accessible to intelligence researchers, who can use the material themselves without the involvement of professional deciphering agencies. This is an additional element that underlines the need for jointness between intelligence agencies (see below).

The use of unmanned aerial vehicles (UAVs) is another element in visual intelligence collection. The past decade has witnessed an upward trend in the use of various types of UAVs to help field echelon units in their tasks. For example, UAVs outfitted with high-quality sensors that are able to remain in the air for prolonged periods help connect the real-time situational picture in the field to both intelligence personnel working to identify the targets and force operators seeking to close in on the targets as quickly as possible. In addition, using small UAVs and drones for tactical intelligence collection and for helping field forces during combat has increased. The access to advanced technologies and low production costs have facilitated the widespread production of various types of UAV, including commercial drones. As a result, they have become accessible for many countries and even non-state military actors.[10]

From the **intelligence analysis** point of view, cyber, to some extent, has created a joint intelligence space in which collection and research personnel share skills. Technological developments in the Military Intelligence Directorate in recent years have created "the intelligence officer's new work table," including applications for networked intelligence spaces. One example is the "Tracebook" system, to which collection personnel, engaging in preliminary processing, upload raw excerpts of intelligence before Unit

8 Ami Rojkes Dombe, "Seeing Everything, From Everywhere, Any Time," *IsraelDefense*, November 29, 2014, https://www.israeldefense.co.il/he/content-מקום-כל-מכל-הכל-לראות/זמן-כל-בכל [in Hebrew].

9 Herzi Halevi, "Military Intelligence 2048 – Intelligence Supremacy in the Digital Age," *Ma'arachot*, no. 477 (2018): 28–29 [in Hebrew].

10 Liran Antebi, "The Watchful Eye in the Sky – Advantages and Challenges in the Use of UAVs for Intelligence Collection," in *Challenges of the Israeli Intelligence Community*, pp. 113–120 [in Hebrew].

8200 (the main collection unit of the IDF's Intelligence Corp) fully processes them in accordance to its standard.[11]

Other technological developments for dealing with vast amounts of data, such as automatic photo identification technologies or speech-to-text (STT) technologies, are also be employed by intelligence agencies. Currently, technologies in the civilian sector can convert sound files to text files based on natural language understanding models. Companies such as Google, IBM, and even the Israeli Verbit company have developed transcription engines that make it possible to save many hours of work transcribing recorded discussions.[12] The use of STT technologies by intelligence agencies may lead to a revolution in the volume of sound that is translated in a given time period and could create warning mechanisms based on queries defined in advance according to the relevant EEI.

The world of visual intelligence has developed additional methods of information processing methods. The transition from the analog era to the digital age shortened the amount of time it takes to produce intelligence, enabled the fusion of information from various intelligence disciplines, and has led to applications that visually present geographic layers of information. These capabilities made it possible, for example, to combine information from optical and radar imagery together with other layers of information of infrastructure in the field. The result has been a marked improvement in being able to complete the circle from the collection stage to the real-time attack stage and the process of producing targets in general.[13]

In terms of imagery information processing, computerized imagery and machine learning have made it possible to identify objects, discern changes in territory, and discover patterns of phenomena. The use of algorithms to compare pictures and automatically identify changes in infrastructure and land cover, applied to large quantities of images, could save intelligence agencies many hours of deciphering and could help analyze a tremendous amount of material in the shortest possible time. In the future, algorithms may be able to provide warnings of visual intelligence incidents.

---

11 Or Glick, "The Walls Were Not Broken – The Story of Tracebook," *Bein Haqtavim* 18 (2018): 164–165 [in Hebrew].

12 Ehud Maximov, "Vocabulary: Has the Ultimate Solution to Transcription been Found?," *Makor Rishon*, August 19, 2018, https://www.makorrishon.co.il/magazine/70017 [in Hebrew].

13 Lt. Col. A., "Geographic Intelligence – From Paper Napkin to 'Geo-Network,'" pp. 98–99.

The technological capability of **disseminating intelligence** has also developed since the 1990s, making intelligence increasingly more accessible to field operatives, based on cooperation between the Military Intelligence Directorate and land forces. One of the lessons of the Second Lebanon War (2006), however, was that intelligence products intended for the use of field units did not reach their intended recipients, partly due to the information being highly compartmentalized.[14] In recent years, the development of the intelligence-based combat (IBC) doctrine in the IDF has also affected the dissemination of information. This concept focuses on the need to provide relevant intelligence to field forces so that they will be more effective and efficient in terms of their maneuverability and with the understanding that the enemy has changed and that the IDF must deal with sub-state terrorist organizations, which operate differently than the military forces of a state. This concept has led to developing real-time intelligence-gathering sensors and adapting the classification levels of the information to facilitate its dissemination. Digital command-and-control systems have also been developed and employed by the IDF. In addition, network combat units were established to realize the vision of network combat and adjust it to the new capabilities and challenges.[15]

The Digital Ground Forces (DGF) project within the land forces began in the early 2000s. As part of the project, the Elbit company developed command-and-control systems for the entire land forces.[16] The systems connect intelligence collection personnel with command echelons and fire-and-attack elements based on a fiber optic network and encrypted wireless communications. Among other things, the project includes video systems, systems to manage field combat on computerized maps, and a comprehensive and relevant intelligence picture, which now reach the field forces in record time. The system has both stationary and mobile configurations, and one of its advantages is its resilience against jamming so that when it is jammed, all the information stored on the system at that time is saved.

One technological development that has facilitated intelligence access to combat forces is the augmented reality glasses device developed by the

14 Compartmentalization prevents certain parties from being exposed to information for information security reasons.

15 Gabi Siboni and Sagi Ben-Yaakov, "Intelligence-Directed Land Combat," in *Challenges of the Israeli Intelligence Community*, p. 78.

16 The system was fully deployed in most IDF land forces by 2014.

IDF's Unit 9900.[17] This device provides the combat soldier with geographic information about the adversary's territory and activity.[18] The unit adapted the device to the needs of the IDF with an off-the-shelf product by Oculus, which produces masks for gamers. The main idea behind the device is to incorporate most of the existing information from the collection personnel and make it accessible to fighters. Through the augmented reality glasses, targets can be labeled, information on rocket launches can be sent in real time, and the soldier can look "inside" buildings. The main challenge that the device tries to address is the surplus of information. The final product reflected in the system has been processed and is relevant for undertaking both training and operational tasks.

It should be noted that many of the technological developments used by the IDF originate in the civilian sector, which has inspired the military to adapt the technology to its own sphere. Some examples are tools based on the Google search engine used in order to extract information from the databases of Unit 8200; development of applications based on civilian websites for use by intelligence analysts, such as "Tracebook," which was discussed above; and technological developments created by civilian companies, such as the augmented reality glasses by Oculus. The advanced technologies embedded in the military have provided significant support for intelligence and field personnel.[19]

The Beginning of a New Paradigm in Intelligence Work

The information revolution created the foundation for a new paradigm in intelligence work, partly due to the increased use of cyber tools.[20] In recent years, the new technologies have transformed the classic functions of collection and analysis and have blurred the difference between the two. These changes weakened the classic "intelligence cycle" and underlined the

17 Unit 9900 is a unit in the Intelligence branch that deals with visual intelligence.

18 Inbal Orpaz, "From the People Who Brought You 8200: Meet 9900 – The Ambitious Younger Sister," *TheMarker*, March 31, 2015, https://www.themarker.com/technation/1.2603595 [in Hebrew].

19 Florin-Eduard Grosaru, "The Revolution in Military Affairs in Information Age and its Impact on Defense Resources Management Performance," *Conference Proceedings of eLearning and Software for Education (eLSE)* 1 (April 2015), pp. 445–452.

20 David Siman Tov and Noam Alon, "The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs," *Cyber, Intelligence, and Security* 2, no. 1 (April 2018): 73–92.

need for a new paradigm for dealing with reality. This is consistent with the theory presented in the 1990s by Andrew Marshall and Richard Hundley, who addressed revolutions in military affairs and argued that technology itself could not lead to a revolution but must be accompanied by organizational adaptations and changes for a revolution to occur.[21]

The term "jointness" refers to operations and actions in which more than two military branches take part. In the context of intelligence, jointness refers to the processes of organizational change that have taken place within the intelligence agencies, as a result of cooperation between separate frameworks. The advantages of each are fused into a new organizational unit, with the capabilities exceeding those of each one separately.[22] Although each organization must obtain and develop its own knowledge, most of that knowledge is, in fact, found in the space between organizations. Mediation is necessary as a result, and it should be accomplished through contacts and cooperation, even though that cooperation does not always exist, partly because each organization seeks to maintain its own independence and prestige.

The terrorist attacks in the United State on September 11, 2001 exemplifies a lack of jointness. The committee investigating the attacks concluded that the United States had ample information and could have thwarted the attacks. The problem was that none of the US intelligence agencies understood the complete picture, as the collection of information and its analysis was spread among various intelligence agencies. Those agencies did not share information with one another due to a lack of cooperation that had been entrenched over the years in addition to unnecessary compartmentalization.

Today, the United States is the leader in jointness, which it had begun to develop already in the late 1970s. The September 11 attacks led to the establishment of the office of Director of National Intelligence (DNI), which serves as a framework for managing the American intelligence community. The DNI was given authority to formulate the US intelligence doctrine, recommend the appointment of senior officials in the intelligence community, and set up joint teams among the country's intelligence agencies. The concept

21 Richard O. Hundley, *Past Revolution Future Transformation* (Washington DC: RAND, 1999), pp. 1–17; Andrew W. Marshall, "Some Thoughts on Military Revolutions," Memorandum for the Record, Office of Secretary of Defense, Office of Net Assessment, July 27, 1993.

22 Kobi Michael, Dudi Siman Tov, and Oren Yoeli, "Development of the Jointness Concept in Intelligence Organizations," in *Intelligence in Theory and in Practice*, no. 1 (May 2017): 6.

behind the DNI was to increase jointness, advance cooperative efforts, and synchronize the various intelligence agencies to prevent a recurrence of events like those of September 11.[23]

A Future Look at Advanced Technologies

One of the newest developments is the Internet of Things (IoT), which enables advanced communication between devices that contain electronics, software, sensors, and camera components. IoT describes a world in which day-to-day objects are equipped with microcomputers that can monitor their surroundings, display information, and execute actions with a certain degree of independence. Communication between these objects creates the opportunity to collect information by accessing the networks to which these objects are connected.[24]

In the next few years, jointness is expected to expand as will the ability to monitor and access information around the world so that it will be possible to know what is happening at any point of interest at any given time. Consequently, the field of IoT also will grow significantly and will require methods of data analysis, processing, and storage to change accordingly. The expansion of the IoT and the accessibility of the information collected by their components will create new opportunities for intelligence agencies to gather information and to develop a new intelligence field that will enable intelligence analysts to obtain information that complements the other fields of intelligence.

The world of IoT can provide intimate information on specific human targets by connecting to networks that are linked to the targets through their watches or smartphones, for example. Thus, it is possible to learn about the targets' routine activities and to use this information as necessary as a means of incriminating them and to help thwart actions. It is also possible to connect to devices, such as smart TVs, which can transmit what is heard in their vicinity, to which there was no access beforehand. In addition, visual intelligence on distant targets around the world can be obtained not only

23 Kobi Michael, Dudi Siman Tov, and Oren Yoeli, "Jointness in Intelligence Organizations: Theory Put into Practice," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 5–30.

24 Tal Steinhartz, "Internet of Things – Cyber Protection in the IOT World," *IsraelDefense*, May 23, 2015, https://bit.ly/2JIgISC.

through high-quality satellite images but also by connecting via cyberspace to security cameras at a particular site.

Analysis of the Changes

Given the above, it is evident that intelligence work has changed following the information revolution. This leads to the question of whether the age of information overload is helping intelligence agencies to deal with potential intelligence surprises, or whether it is actually making it more difficult to separate the grain from the chaff and to identify the bits of information that hint at the next surprise.

During the Yom Kippur War, for example, the IDF was caught unprepared for Egypt's use of advanced anti-tank and anti-aircraft missiles; this technological surprise cost the IDF losses in lives, infrastructure, and weapons. One of the missiles used by the Egyptians was the Soviet Sagger missile. Despite that the Military Intelligence Directorate had information about this missile at the time, it was kept highly classified and it did not reach the force-building entities or field forces. In other words, the threat theoretically had been recognized but no appropriate efforts were taken to prepare for it neither at the levels of intelligence, combat, or force buildup in order to develop the capability to defend against it.[25]

In Operation Protective Edge in 2014, the IDF was forced to deal with the threat of Hamas' attack tunnels, which the public and the military interpreted as a strategic surprise in terms of their widespread and efficient use. Despite the knowledge of the threat, the decision-making echelon did not fully understand the central role of the tunnels in Hamas' new military strategy and did not address them in terms of force buildup, combat, or their eradication. The state comptroller's report on Operation Protective Edge addressed the following points in which the intelligence was deficient in handling the tunnel threat:

- *Intelligence cooperation between the Military Intelligence Directorate and the Israel Security Agency regarding the tunnels and the division of responsibility between the agencies for what was happening in Gaza.* From the time the IDF and the Israel Security Agency (ISA) had left Gaza in 2005, and until 2015, Gaza had not been defined as a "target country" that

25 Effi Melzer (ed.) *Military Technology: Weapons and Intelligence* (Reut: Effi Melzer Ltd. – Military Research, Journalism and Publication, 2012), pp. 86–87.

required analysis, and the division of intelligence responsibility between the agencies had not been examined. As such, the ISA was responsible for collection of intelligence and prevention of threats in Gaza while the Military Intelligence Directorate, Southern Command, and the Gaza Division operated alongside it.

- *Inclusion of the EEI of the tunnels in the EEI of national intelligence, the Military Intelligence Directorate, and the ISA.* The tunnel threat was included in the national EEI only in 2009, and even then special intelligence attention was not devoted to it. As a result, there was no change in the attitude to the threat of the tunnels in the following years.
- *The collection efforts of the intelligence agencies regarding the tunnels*. There was not any joint intelligence collection efforts by all the intelligence agencies and the Military Intelligence Directorate. Even the ISA, which had invested a lot of resources in Gaza between 2008 and 2012, increased its collection efforts regarding the tunnels only in 2013.
- *The intelligence analysis of the tunnels threat in Gaza*. In 2012, the head of the Military Intelligence Directorate at the time determined that the Southern Command and the Gaza Division would deal with the intelligence assessment of the tunnels threat rather than the research department of the Military Intelligence Directorate. Thus, the IDF's main research unit had to suffice with the picture that emerged from the Southern Command and the Gaza Division, rather than deal independently with the matter.
- *The quality of the intelligence on the tunnels that was provided to the field forces.* Significant gaps were found in the intelligence transferred to the field forces as it related to the tunnels, which made it difficult for them to locate, neutralize, and destroy all the attack tunnels, and it limited their capability to thwart attacks launched from the tunnels into Israeli territory.[26]

The deficiencies listed above reveal significant intelligence gaps regarding Hamas' attack tunnels in the period prior to Operation Protective Edge, which affected the IDF's handling of the threat during the operation itself. One of the gaps was the fact that in the years following the Second Lebanon War, the national intelligence EEI focused mainly on the northern front, with most resources directed there. The issue of the tunnels in Gaza remained a

26 Office of the State Comptroller, "Operation 'Protective Edge': Decision Making in the Cabinet Regarding the Gaza Strip Before the Operation and at its Beginning: Dealing with the Tunnel Threat – Special Comptroller's Report," Part 2, 2017, pp. 13–19.

lower priority in the EEI, which affected the intelligence work on that issue and the existing knowledge at the onset of Operation Protective Edge. One of the lessons learned from the investigation of the tunnels in Protective Edge was that more investment must be made regarding collection and analysis of the threat posed to the tunnels along the northern front. In his report about Operation Protective Edge and especially concerning the intelligence handling of the tunnels threat in the Northern Command, the state comptroller wrote that "over the years since the Second Lebanon War, until around the time of Protective Edge, there were many collections and analysis operations regarding the Hezbollah organization, but only partial work was done regarding the tunnels infrastructure in Lebanon."[27]

The tunnels in Gaza put the focus on the subterranean field and gave it a higher priority in the EEI of national intelligence. The understanding that Hezbollah is apparently working at building tunnels to penetrate Israeli territory as part of its attack plans for the next war led to large collection efforts intended to provide intelligence about the tunnels. A special team was established, combining intelligence and technology factors, with the aim of obtaining high-quality, precise, and reliable intelligence that would help in planning actions to locate and eradicate the tunnels.[28] Some of the information came from the world of cyber and helped engineering forces during Operation Northern Shield locate and neutralize six Hezbollah tunnels that crossed into Israeli territory.

The surprise use of the Sagger missiles during the Yom Kippur War illustrates what the intelligence reality was like prior to the information revolution. It was characterized by the classic "intelligence cycle" conducted by distinct research and collection bodies and with limited capabilities to disseminate the intelligence to the field. The ability to provide real-time warnings of the missile threat was clearly limited at the time, and there were no advanced means to transmit intelligence to the field. Without any long and focused prior preparatory work, it was impossible to prepare forces for dealing with the existing threat.

In the period following the information revolution, intelligence forces improved access to information while the time frame for obtaining the information became shorter. The improvement was also reflected in the

27 Ibid., p. 19.

28 "Developing the Complete Answer to the Threat: Behind the Scenes in Operation Northern Shield," IDF website, December 6, 2018 [in Hebrew], https://bit.ly/2RBsjqY.

ability to respond to complex intelligence questions, which previously had left room only for analysts' assessments. The example of dealing with the threat of penetrating tunnels along the northern border illustrates how the proper focus, prioritizing EEIs, and the use of existing collection capabilities make it possible to obtain high-quality precise intelligence for carrying out operations to eradicate the developing threat.

The penetration of an Iranian UAV into Israeli airspace in 2018 was another example in which high-quality intelligence also provided a warning and enabled the IDF to prevent a surprise attack. On February 10, 2018, an IDF combat helicopter shot down an Iranian UAV that had been launched from the Tadmor area deep in Syria and had penetrated Israeli airspace, breaching Israeli sovereignty. The air defense systems identified the UAV at an early stage, and had been tracking it until it was shot down. The UAV's ground control station later was attacked in the area from which the UAV was launched.[29] We can assume that the other side had planned the penetration of the UAV for a long time and that Israeli intelligence apparently had prior information of the enemy's intention to execute the action. A surgical and precise attack on the ground control station would not have been possible without real-time intelligence of its precise location, which was made possible thanks to advanced collection capabilities used before and during the incident.

Although the information revolution and the period thereafter did not completely solve the uncertainty in various intelligence matters, intelligence analysts now have a greater possibility of obtaining missing information. As in the past, analysts must answer the proper questions that will lead them to resolving the intelligence gaps, but as table 1 below shows, the information revolution is having a marked effect on each of the stages in the intelligence process. This revolution also requires intelligence personnel to learn and acclimate themselves to existing capabilities.

In an age when the means of gathering intelligence can provide a response to almost any matter, we must choose the EEIs in which to invest efforts in collecting and processing information. This leads us to the importance of prioritizing EEI. In the past, when collection was more limited, certain EEIs simply were not answered. Today, the bottleneck affects the processing needed to deal with the immense amount of information that has been collected.

29 Yoav Zaitoun et al. "The IDF Shot Down an Iranian UAV that Penetrated Into Israel; Attack in Syria; An F-16 Crashed in Israeli Territory," *Ynet*, February 10, 2018, https://www.ynet.co.il/articles/0,7340,L-5102924,00.html [in Hebrew].

Without prioritizing the EEI, the ability to respond to each intelligence matter is almost impossible due to cost, manpower, and time considerations.

Table 1. The stages of intelligence research before and after the information revolution

	Before the information revolution	After the information revolution
Collection	Based on classic SIGINT and VISINT.[30]	Cyber as a new dimension; Big Data; increasing number of platforms and sensors.
Processing	Done by professionals—manpower and training; manual means and analog tools.	Development of automated tools to deal with massive amounts of data; technological developments allow information from various intelligence disciplines to be integrated.
Analysis	Clear distinction between analysts and collection personnel; the analyst "waits" to receive processed intelligence material.	Development of tools and applications make raw intelligence material accessible to the analyst; jointness between collection personnel and analysts; "technologists" as new intelligence professionals.
Dissemination	Partial transfer of information to the field; compartmentalization as an impediment.	Technological developments make the intelligence accessible in real time to fighters in the field.

As previously shown, the current blurring between collection and analysis personnel has lead to organizational changes intended to respond to intelligence needs. In an age where cyber takes up a significant share of intelligence work, a new environment has been created in which all parties must work together and share common knowledge and skill, such as the ability to search through pools of data, find the relevant information, and process it. Although collection personnel do not deal only with information collection as they did in the past, their role is different from that of "technologists."

30 SIGINT refers to signals intelligence, based on the collection of information transmitted through the broadcast of electronic signal while VISINT is visual intelligence obtained from various visual sources.

Collection personnel must have a basic understanding of the research topics being addressed by the analyst who works with them, and their work should be reflected in the creation of technological tools that will help the analyst ask the proper intelligence questions and find the proper responses. Similarly, the analyst must have a basic understanding and acquaintance with information technology and the ability to exhaust the information, as well as a basic understanding of networks and more. For example, the Military Intelligence Directorate is now thinking about "new military intelligence bases" that will provide a response for these joint frameworks. Jointly organizing the intelligence agencies will provide an opportunity to streamline work processes and will utilize the advantages of each one to improve the intelligence products and shorten their dissemination time.

The environment of the information age is rapidly changing, leading to innovation and changes on the part of the adversary as well. In addition, Israel faces a special challenge, since it must deal not only with external threats but also with internal ones, such as terrorist attacks or the "Knife Intifada" of 2016. General Herzi Halevi, former head of the Military Intelligence Directorate, argues that the coming decades will be characterized by a blurring of the line between the physical and digital dimensions. According to Halevi, whoever achieves supremacy in information and knowledge in the digital age will be the one to control the main processes.[31] He refers to it as "intelligence supremacy," that is, the ability to gather the missing intelligence information and turn it into knowledge about the enemy, in a way that will allow us to affect the adversary at the relevant time.

Winning wars in the age of the information revolution will require a different kind of intelligence, and the source of that intelligence will be, to a great extent, in the cyber dimension. Cyber capabilities can be learned and cyber tools are accessible, which enables their development by the other side as well. As the former head of the Military Intelligence Directorate argues, "the advantages of the digital revolution are also available to our enemies, and there is no reason to assume that they will rest on their laurels."[32] In the information age, when everything is open and accessible, the adversary is also able to develop learning capabilities, is more dynamic than in the past, and is therefore capable of surprising us with his abilities. Similar to the

31 Halevi, "Military Intelligence 2048 – Intelligence Supremacy in the Digital Age," pp. 26–27.

32 Ibid., p. 28.

O-RMA ("the other revolution in military affairs"),[33] which describes the reactions and developments of the other side in relation to the revolutions in military affairs, we can look at the information revolution and the period thereafter and argue that the adversary also lives in a global technological reality and enjoys the benefits of that same revolution. The adversary also learns and develops, recognizes the advantages of the opposing side, and tries to improve and attack the other side's weak spots. This poses a challenge for intelligence organizations, since access to information by all players may erode the traditional relative advantages that intelligence organizations previously had.[34]

Conclusion

We can point to three main trends that reflect technology's influence on intelligence agencies in the period following the information revolution. First, since the information revolution and the technological developments in the field of intelligence, we have gained a sharper understanding of how the process of classic intelligence work is changing and that we must adapt to new methods at the organizational level as well. Jointness between collection and analysis bodies, as well as changes in the capabilities required of the personnel, have created new work processes in the field of intelligence that differ from the past.

Second, the accessibility of intelligence has improved for the operational forces as a result of technological developments, which have enabled the secure and timely transfer of large quantities of different types of intelligence information. Improving the accessibility of the intelligence better serves the needs of operational forces and makes it easier for them to deal with unplanned incidents in real time. Moreover, the quality of the intelligence product and its connection to field operatives directly affect their ability to deal with surprises.

Third, technological developments in the use of intelligence have helped diminish room for surprise. The information age has significantly improved the ability to respond to the intelligence questions with technologies that have been incorporated into each stage of the intelligence cycle. We are

33 Itai Brun and Carmit Valensi, "The Revolution in Military Affairs of the Radical Axis," *Ma'arachot*, no. 432 (2010): 4–17.

34 D. P., "The Approach as a Guide to Technological Intelligence Force Buildup" in *Intelligence in Theory and in Practice,* no. 3 (May 2018*):* 137 [in Hebrew].

now in an era in which practically all information is open, accessible, and connected. While the level of uncertainty is declining, the challenge is now developing the skills that will enable us to attain the essential information. In contrast to the era before the information revolution, the likelihood of obtaining information today is exponentially greater today as a result of the deluge of information and the many ways of accessing it. Nonetheless, despite the efforts to make information accessible to the field echelons, there are still difficulties due to the compartmentalizing of some components of information. This requires some thought, mainly in terms of overcoming this compartmentalization so that it will not harm the preparation and readiness of the field echelons for any situation they may encounter.

The effects of the information revolution are an important and significant factor in the work of the intelligence agencies. They are apparent in all the cornerstones of intelligence work, as this article shows, while technological developments—a direct outcome of the information revolution—affect daily the ability of the intelligence agencies to provide precise information at the right time and place in order to warn and prevent the next surprise. It must be noted that while technology has significantly improved the intelligence processes, the adversary also continues to learn and improve, and we must therefore adapt in order to maintain our technological superiority.

In looking forward, where will we be in another decade, two decades, or even more? It is clear that currently the quantity of information available online is continuing to grow exponentially, and this trend will continue to influence intelligence work, challenge collection, processing, and analysis personnel, and require them to develop creative solutions that will provide answers to the questions of the EEI. Additional questions include what place will the analyst have in intelligence work, and how much time will be invested, for instance, in developing cyber tools in order to benefit collection and analysis, compared with the time invested in the analysis itself, in order to provide warnings? How many processes will become automated, and what place will the analyst have in preventing the next surprise? These questions are worthy of further study.

The importance of technology in the intelligence process will continue to develop and an increasing number of tasks will become automated and replaced by computer algorithms. This will help collection personnel deal with the large quantities of raw material—whether information from VISINT

or SIGINT—and will shorten the time currently required to process the information and disseminate it to its consumers. In the future, will the ability to warn against the next surprise remain in the hands of the human analyst, or will it be replaced in the future by computer algorithms? This question and others will continue to occupy intelligence personnel, and what may seem like science fiction today may become reality in the not-too-distant future. It is therefore worthwhile addressing this issue and preparing for its eventuality.

Cyber Influence Campaigns in the Dark Web

Lev Topor and Pnina Shuker

In recent years there has been a significant rise in the scope and intensity of information wars between the great powers and other forces in the international arena, and influence campaigns have become a legitimate tool in the hands of politicians, propagandists, and global powers. In this context, the professional literature has focused most on campaigns on social networks while it has almost ignored similar campaigns in the Dark Web where the current research tends to focus on criminal activity. The Dark Web was developed by the American Navy for intelligence purposes and was then promoted by the West as a public tool to protect privacy and anonymity. Today it provides fertile ground for deliberate leaks by countries that do not wish to publish certain information in the traditional media. These leaks are perceived as authentic, leading the media and other intelligence organizations to swallow the bait and investigate, and in some cases they even change their operations accordingly. The purpose of this article is to present the way in which the Dark Web is used in influence campaigns, particularly through deliberately leaking information.

Keywords: Dark Web, influence campaigns, propaganda, information wars, disinformation

Dr. Lev Topor is a senior strategic advisor and researcher on racism and cyber. Pnina Shuker is a Neubauer Research Fellow at the Institute of National Security Studies.

Introduction

In January 2019, tens of thousands of documents and emails from senior Russian government officials, leaders of the Russian Orthodox Church, and Russian oligarchs were leaked to the Dark Web. The leak appears to have been the outcome of activity by activist hackers ("hacktivists") who declared that they were not motivated by ideology but rather by the desire to ensure freedom of information: "We have no goal except to ensure that information is accessible to those who need it more than anyone—the people."[1] This incident shows how the Dark Web is being used to bypass the restrictions that totalitarian regimes place on freedom of expression. In addition, however, in recent years, many players on the international scene have been making use of the Dark Web to share deliberate, sometimes false, leaks in order to exercise political influence, highlighting the built-in tension that exists on the internet between the protection of privacy and the needs of national security.

Traditionally, the Dark Web has provided a convenient space for criminal activity, as well as for leaking and trading information. Recently the scope and intensity of the information wars conducted on the Dark Web between various elements in the international arena have increased significantly, with each side deliberately using leaks and disinformation to manipulate public awareness of the other side. The purpose of a leak may be purely military, or it may be intended to apply social or even commercial influence. For example, countries that do not wish to publicize certain things on traditional media can leak the information on the Dark Web, giving it the appearance of authenticity. Some media outlets have set up their own platforms to provide encrypted access as a way of encouraging leaks. Examples are WikiLeaks and Secure Drop, which are discussed in more detail below. The Dark Web is also a marketplace for malware, spyware, worms, and countless other malicious programs and files, as well as media encryption and cyber tools (such as PGP and other easy to use encryption guides).

This article aims to show how actors on the international stage are using the Dark Web to distribute propaganda and disinformation about their rivals, and how these actions can be translated into wide-reaching campaigns of influence. The article has three parts: The first part is a theoretical review of the manipulation of data in general and of influence campaigns in particular,

1 Stephan Jajecznyk, "The Dark Side of the Kremlin: Hacked Russian Documents Explained," *Al Jazeera*, February 25, 2019.

with several examples of important recent campaigns. The second part deals with the Dark Web, its characteristics, and chief uses. The third part, which synthesizes the findings of the first two, shows how the Dark Web is used to implement influence campaigns and its scope.

What Are Influence Campaigns?

An influence campaign is the coordinated, combined, and synchronized application of diplomatic, informational, military, and economic abilities, together with other national capabilities, whether in times of peace, periods of crisis, hostile situations, or following hostilities. The campaign seeks to influence the behaviors and decisions of target populations in other countries and persuade them to adopt positions that serve the interests of the campaign's initiators.[2] Campaigns to influence cognition are a familiar type of operation intended to serve a range of political, security, economic, and social ends. At the national level, influence campaigns are designed to achieve their aims, inter alia, by interfering with personal and economic security, undermining the public's trust in—and support for—national institutions and weakening social cohesion. The methods they use include active tampering with systems and processes; attempts to trigger actions or deter actions; obtaining information and using it to create messages; disseminating these messages and maximizing their effect. The channels for distributing messages include traditional media as well as new media, namely the internet and the social networks. Opinion leaders often serve as "unwitting agents" who make the messages more trustworthy and increase their reach.[3]

In recent years, there has been a marked rise in attempts by foreign elements (both governmental and non-governmental) to intervene in the election campaigns of rival countries using digital tools. Sometimes this involves cyberattacks on the computer systems supporting the electoral process (databases, software, and communications systems) in order to disrupt their operation or to distort or steal data. At the same time, extensive efforts are made to change the direction of public discourse in the target country and thus affect voting. The third type of influence campaign is a synthesis

2 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica: RAND Corporation, 2009), p. 2.

3 Ron Shleifer, "Psychological Warfare in Operation Cast Lead," *Ma'arachot*, no. 432 (August 2010): 19–20 [In Hebrew].

of the first two and uses cyber tools to penetrate the public consciousness. The possibilities are wide, ranging from attempts to undermine public faith in the democratic process, to interfering in support for specific parties or candidates. There have even been efforts to dissuade people from voting altogether, based on identity or socio-economic status.[4]

The main players behind these attempts at intervention in elections are authoritarian regimes, such as Russia, China, and Iran. Even some democratic-liberal governments, such as the United States, Britain, and also Israel, use these methods of influencing events in the international arena. For example, Russia has a long tradition of exploiting influence campaigns and has developed a systematic doctrine and operational capabilities for this purpose.[5] In this context, Russian methods include spreading false news on social networks by means of fake profiles; acquiring genuine profiles as a vehicle for political messages in support of pro-Russian candidates in elections worldwide, or to publish false or even incriminating information about Moscow's enemies, using Kremlin-owned media to manipulate news reports.[6] In the last six months alone, Russia has conducted influence campaigns for manipulating elections, including in Spain, Nigeria, Indonesia, and South Africa, among others, as well as in the elections to the European Parliament.[7]

China also makes widespread use of propaganda and influence campaigns, both as a way of shaping the image of the Chinese communist party and in undermining the stability of its rivals.[8] Reports have increasingly looked at China's attempts to interfere with elections in other countries, such as Sri Lanka, Malaysia, and Australia.[9] In addition, just before the US mid-term elections, the Trump administration announced that China, Iran, and Russia

4 Chris Tenove, Joran Buffie, Spencer McKay, and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (Vancouver: Center for the Study of Democratic Institutions, University of British Columbia, 2018), p. 2.

5 Dima Adamski. "The Art of Cybernet Operations: From the Viewpoint of Strategic Studies and a Comparative Perspective," *Eshtonot*, no. 11 (2015): 28–48 [in Hebrew].

6 Alina Polyakova, "Want to Know What's Next in Russian Election Interference? Pay Attention to Ukraine's Elections," Brookings, March 28, 2019; Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019.

7 Pnina Shuker, "Foreign Intervention in Elections Worldwide: Traits, Trends, and Lessons for Israel," *INSS Insights*, no. 1173, June 10, 2019.

8 Erica Pandey, "How China Became a Global Power of Espionage," *AXIOS*, March 23, 2018.

9 Prashanth Parameswaran. "China's Influence Operations in Asia: Minding the Open Door Challenge," *The Diplomat*, May 14, 2019.

together were trying to undermine the democratic process with an on-line propaganda campaign—including the spread of disinformation on social media—with the aim of deepening the ideological rifts in the United States and stirring up internal arguments about issues on the local agenda.[10] As part of its hostility to the United States, China is also trying to further its influence in Singapore: it was recently claimed that the Chinese communist party was contacting Singaporeans of Chinese origin, principally through the Chinese application "Wechat," in an attempt to influence politics and society in Singapore.[11] The Chinese are also reported to be using on an unprecedented scale the Facebook, Twitter, and YouTube platforms—all three banned in China itself—in order to defuse the fierce protests in Hong Kong against Chinese interference in local affairs.[12]

Iran is another country that does not refrain from using these methods. In August 2018, Twitter and Facebook deleted hundreds of accounts suspected of links to an Iranian disinformation campaign.[13] The content posted by these accounts was designed to highlight topics and narratives that suited Iranian foreign policy and promote its anti-Saudi, anti-Israeli, and pro-Palestinian agenda, and also to stimulate support for certain elements of US policy that serve Iranian interests, such as the 2015 nuclear treaty between Iran and the powers.[14] At the end of October 2018, a network of Facebook pages was found, which originated in Iran and was designed to influence public opinion in the United States and Britain.[15] There have also been increasing reports about Iranian cyberattacks and influence campaigns against Israel. At the end of January 2019, at a Cyber Tech conference, Prime Minister Netanyahu declared that Iran was trying to influence the elections in Israel by means of fake network accounts and was carrying out cyberattacks against Israel

10 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses," *Foreign Policy*, October 4, 2018.

11 Muhammad Faizal Bin Abdul Rahman, "Foreign Influence in Singapore: Old Threats in New Forms," *The Diplomat,* July 23, 2019.

12 Raymond Zhong, Steven Lee Myers, and Jin Wu, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters," *New York Times,* September 18, 2019.

13 Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation," *Washington Post*, August 21, 2018.

14 Adriane M. Tabatabai, "A Brief History of Iranian Fake News: How Disinformation Campaigns Shaped the Islamic Republic," *Foreign Affairs*, August 24, 2018.

15 "Facebook Is Fighting Fake News from Iran: 'We've Destroyed a Propaganda Network – A Million Users Were Exposed,'" *TheMarker,* October 27, 2010 [in Hebrew].

"on a daily basis."[16] Contrary to the known Russian efforts, which exhibit a relatively high level of sophistication, Iranian and Chinese attempts to influence events are poorly executed and fairly easy to track.

Elections all over the world in the last six months have taken place in the shadow of suspected influence campaigns. Indeed, in many cases the campaigns were identified, particularly the Russian ones. Analysis of these efforts shows that counter moves by media giants and governments themselves reduced the foreign attempts to use bots as a tool for influence on social networks. On the other hand, today it is possible to identify growing activity by human influencers. Moreover, efforts to influence via the established media are again playing a significant role as well as through instant messaging applications, such as WhatsApp and Telegram, which have a higher level of credibility. Information is transferred on these closed platforms among relatively limited groups of family and friends, giving the messages the appearance of reliability. Moreover, the end-to-end encryption technology used by these platforms denies even their administrators access to the messages sent, unless a user reports some content as problematic. These features make it extremely difficult to track and remove any false information.[17]

The Dark Web: Characteristics and Uses

The Dark Web has become one of the most talked about subjects in the cybersecurity community.[18] To understand the formation and development of the Dark Web and its unique features, a short review of the regular internet is necessary. The Surface Web was part of a communications project of the United States Department of Defense in the 1960s, known as the Advanced Research Project Agency Network (ARPANET). In 1983, the closed network under the Network Control Protocol (NCP) was changed to an open network, now referred to as the Transmission Control Protocol or the Internet Protocol—TCP/IP.[19] Opening up the network led to a massive expansion of activity—from just a few connections to many millions—and

16 Stav Namer, "Netanyahu: Iran Is Making Cyberattacks on Israel on a Daily Basis," *Ma'ariv,* January 29, 2019 [in Hebrew].
17 Shuker, "Foreign interference in Global Elections."
18 Mihnea Mirea, Victoria Wang, and Jeyong Jung, "The Not So Dark Side of The Darknet: A Qualitative Study," *Security Journal* 32, no. 2 (2019): 102–118.
19 George Hurlburt, "Shining Light on the Dark Web," *IEEE Computer* 50, no. 4 (2017): 100–105.

to a split into categories of the national network (Class A), the regional network (Class B), and the local network (Class C), laying the infrastructure for the public internet we know today. The internet now links huge numbers of computers and devices through nodes or access points.[20]

The ARPANET project was officially closed in 1989, leaving behind the public areas: database addresses (internet pages) and accessible network protocols, browsers for the general public, and an accessible language (for example, the HTML language). In order to make the internet accessible for all, the Internet Corporation for Assigned Names and Numbers (ICANN) organization was established, which supplied addresses and network numbers and attached names to IP addresses. The organization began to index nearly all the services and public information and invited technology companies to build publicly accessible databases, such as Google, Bing, AOL, Yandex.ru, and others.[21] The result was that large corporations and governments were able to shape search lists as they wished and thus control which information was accessible to the public, essentially giving birth to the Deep Web.[22]

The Deep Web refers to any kind of information that is not mapped by search engines and to which access is restricted but can be obtained through ordinary (infrastructure) browsers, such as dynamic internet pages, unlinked internet pages, internet pages that are not based on HTML, and other restricted databases. Many security elements also set up private networks (such as LANs) and deep networks, such as the army or police networks, to which the general public does not have any access. At the same time, the Deep Web also contains private information, such as financial databases, biometric databases, medical data, and so on. For example, when a user enters his own bank account, he is entering the Deep Web, although he gets there through the bank's home page, which is on the regular web.[23]

---

20 Mitch Waldrop, *DARPA and the Internet Revolution: 50 Years of Bridging the Gap* (Defense Advanced Research Projects Agency, 2018).

21 Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler, "The Deep Web," *Trend Micro*, 2015.

22 Lucas D. Introna and Hellen Nissenbaum, "Shaping the Web: Why the Politics of Search Engines Matters," *Information Society* 16, no. 3 (2000):169–185; Eszter Hargittai, "The Social, Political, Economic and Cultural Dimensions of Search Engines: An introduction," *Journal of Computer-Mediated Communication* 12, no. 3 (2007): 769–777.

23 Hurlburt, "Shining Light on the Dark Web," pp. 100–105.

The Darknet or Dark Web is part of the Deep Web, and, in fact, it is its most deeply concealed layer.[24] Users can only visit it by means of a special browser or using special network protocol definitions, so that most actions taken on it are completely anonymous. The unique features of the Dark Web, compared to the Deep Web, are the special protocols (rules) and the special infrastructure required in order to access and use it. The special infrastructure sometimes comes in the form of browsers that are programmed to access various protocols, such as Onion, Riffle, Freenet or i2p addresses and more, or as specific network definitions known only to authorized users.[25] Organizations, such as the military, intelligence, and the police and even businesses and a few individuals can set up Dark Webs, whose protocols and browsers will be unique and known only to their owners.[26]

The most widespread Dark Web is the Onion Route (TOR), which had been developed by US Navy laboratories to facilitate private anonymous communication between intelligence agents and was exposed in 2002. This network consists of thousands of internet sites that can only be accessed using the TOR browser. These sites are called "onion" sites after the onion suffix in their names and the onion image, which acts as a metaphor for the many layers hampering access to the core. Onion sites are not catalogued and no general browser can effectively find them. TOR operates in a way that communication between two points (e.g., the user's computer and the site the users wants to visit) is not transmitted directly but rather through several intermediate stations (IP addresses). Each station receives a unique means of decoding, only knows the next station in the chain, and does not know the final station or the source. The reason is that many of the servers are encrypted, so that the internet provider is able, in most cases, to discover the first node reached by the user but not the subsequent nodes.[27] The server receiving the call is also unable to locate any other nodes, apart from the

24 Gabriel Weimann, "Going Darker: The Challenge of Dark Net Terrorism," *Wilson Center*, April 27, 2018.

25 Dakota S. Rudesill, James Caverlee and Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box,* Ohio State Public Law Working Paper no. 314 (Ohio State University, Woodrow Wilson International Center for Scholars, 2015).

26 Ibid; Lev Topor, "Deep and Dark Webs – Liberty or Abuse," *International Journal of Cyber Warfare and Terrorism* 9, no. 2 (2019): 1–14.

27 Roi Goldschmidt, "Use of Anonymous Communications Networks on the Network for Criminal Purposes," Knesset Research & Information Center, January 2012 [in Hebrew].

node from which it receives the call for information/ interaction. In fact, this node also changes every few minutes. In this way, all the nodes are on a route that is protected in most cases from private or government surveillance.[28]

The main problem with TOR lies in its unique nature: It allows security and anonymity, but it is not hidden from the local network providers. Although they cannot discover the information and the destinations of network users, such as of western intelligence operatives in hostile countries, this problem can be solved by elimination, at least partially: Local network providers can discover that among a number of users in a specific neighborhood, for example, one or more users have unusual network traffic. In this way, the authorities can only see normal network traffic, and not see private and anonymous web surfing.[29]

Besides the special network traffic of the Dark Web, which, as stated, creates a confusing, hard to locate trail of several nodes, the TOR platform, in the form of an easy to use browser, can stop sites from gathering information about users. Privacy is sacred on the TOR network, and no site on it can collect information about location, types of hardware, software, or patterns of use. With the TOR browser, it is also possible to eliminate the use of JavaScript, HTML 5, media, images, icons, symbols and more. Thus, the Dark Web creates an interesting paradox: On one hand, it sanctifies privacy and anonymity, and on the other hand, it is used by criminals, terrorists and other hostile elements, who can trade information with a low signature.[30]

In addition, the Dark Web is a kind of marketplace for illegal activities, such as trading in cyber tools. For example, if a company wants to cause damage to a competitor, it can enter the Dark Web, buy an attack with ransomware, malware, or spyware, or activate a bot network or any other tool. In most cases, buyer and seller conduct the transaction with bitcoins, to maintain anonymity. The Dark Web also is used for trading in weapons and drugs and for distributing pornographic material.[31] Terror organizations can find it very convenient for their activities: For about a decade, much of the communication between the leaders of al-Qaeda all over the world took

28 Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (London: Global Commission on Internet Governance and Chatham House, 2015).
29 Topor, "Deep and Dark Webs – Liberty or Abuse."
30 Ibid.
31 Nyshka Chandran, "From Drugs to Killers: Exploring the Deep Web," *CNBC,* June 23, 2015; Cara McGoogan, "Dark Web Browser Tor Is Overwhelmingly Used for Crime, Says Study," *Telegraph,* February 2, 2016.

place on the Dark Web.[32] But the Dark Web also hosts entities working to foil terror attacks, such as internal security and intelligence organizations.[33] According to data from Webhose, about fifty percent of activity on the Dark Web is criminal in nature, which means that the other fifty percent is legal and legitimate.

Today, the Dark Web is increasingly being used as a tool for activists to organize protests against totalitarian regimes. It also hosts sites that mirror well-known internet sites, such as those providing news and information from the West, which can be accessed by people living under totalitarian restrictions. For example, the address facebookcorewwwi.onion leads to the "onion version" of the social network for users in countries where Facebook is blocked. Similarly, nytimes3xbfgragh.onion leads to the "onion version" of the *New York Times*. In November 2018 a former engineer from Facebook uploaded an "onion version" of Wikipedia—a Dark Web mirror version of the free encyclopedia, which is completely or partially blocked in various countries.[34] While totalitarian regimes deal with the problem of anonymity by means of arrests and interrogations, the US administration chose to flood the world with TOR, calling for the promotion of freedom of speech, human rights, anonymity, free and open communication, and opposition to all totalitarian regimes.

Potential Uses of the Dark Web for Influence Campaigns

Previously, when a power wished to influence another player in the global arena—a country, terror organization or specific individual—it made use of military or economic power. The cyber era has added a new dimension to the concept of "power," incorporating advanced cybernetic capabilities that are easy to operate and can overturn the traditional balance of power and even serve as "tie breakers." For example, a country might develop a secret military project that could be destroyed if cyber criminals leak the details on the web.[35] In July 2018, it emerged that an American hacker had

32 Weimann, "Going Darker."
33 Topor, "Deep and Dark Webs – Liberty or Abuse."
34 Amitai Ziv, "The Dark Side of the Internet: Drugs, Weapons, Cyber Attacks and Regime Opponents," *TheMarker*, July 18, 2018 [in Hebrew].
35 Joseph S. Nye. "Soft Power and American Foreign Policy," *Political Science Quarterly* 119, no. 2 (2004): 255–270; Ernest J. Wilson, "Hard Power, Soft Power, Smart Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 110–124.

tried to sell on the Dark Web the plans for sensitive military drones called MQ-9.[36] In the second trimester of 2019, a company in the military industry contacted one of the writers of this article with a request to locate a leak about it on the Dark Web, due to its concerns over the leak of sensitive plans by some of its employees.

Some of the Dark Web platforms that could be used for influence campaigns include leak platforms; passive data storage platforms; and trading platforms, which include offers of selling information, cyberattack tools and bots, as well as fake "involvement" in social networks.

Leak Platforms

In an age when it is possible to steal over a terabyte of data in a fraction of a second on a mobile storage device and to leak information from government, security, and business meetings anonymously in real time, it is not surprising that the frequency of leaks is increasing.[37] Leaks are often used by people opposed to controversial actions, particularly on matters relating to the military and security. At the same time, the local government can be the source of the leaks, either directly or through deception: Just as security forces and the police use agents who operate on the Dark Web (and the regular internet) or who pose as minors to trap pedophiles, intelligence organizations all over the world use the leak platforms by spreading a kind of "appeal" for leaks and offering payment in return. Moreover, many governments contact external suppliers, such as business intelligence companies or high tech companies in order to monitor, analyze, and operate certain elements on the Dark Web.[38] In this context, the Dark Web project can also be a large honey trap.[39]

Another obvious example of a leak platform is the free press website Wikileaks, which was set up in 2006 and since then has caused several media controversies after leaking hundreds of thousands of documents, items of information, and other material about contentious American activity. The site is located on the regular internet but recommends that users who wish to share leaked information resort to the Dark Web. They are referred to a link where they are asked to enter the details of the information and upload any

36 Ziv, "The Dark Side of the Internet."
37 Scott Shane, "The Age of Big Leaks," *New York Times*, February 2, 2019.
38 Chris Bing, "How the FBI Relies on Dark Web Intel Firms as Frontline Investigators," *Cyber Scoop*, April 13, 2017.
39 Topor, "Deep and Dark Webs – Liberty or Abuse."

supporting files, such as pictures or documents, although the site is under no obligation to verify the report.[40] Another leak platform is the Secure Drop system, which the Freedom of the Press Foundation developed and promotes. It provides media services and anonymous encrypted transfer of data. Press syndicates such as Associated Press, the Guardian, New York Times, Al Jazeera, and many others, use this system to share sensitive information.

Governments can use both the above platforms to leak information if they feel its publication on traditional media could be harmful. A prominent example was the information about the nuclear weapons held by Israel. Israel has not signed the international Non-Proliferation Treaty (NPT) on nuclear weapons, so any overt publication about its weapons could be problematic in terms of international law. At the same time, an anonymously initiated publicizing of an arsenal of strategic weapons could strengthen Israel's geopolitical status and serve as a signal to hostile countries. Thus, for example, there is a famous dedicated page on the Hidden Wiki site with information about the Israeli nuclear program, including its timeline, doctrine, policy, and methods of implementation. More about the Israeli nuclear program, as well as the Indian program and other controversial projects can be found in other Dark Web forums.

Passive Platforms for Data Storage

These are sites or forums for discussions where data is shared and stored. For example, leaked files can be uploaded to the DOXBIN site and saved until needed. On May 30, 2019, contact details of thirty employees of the FBI, including home addresses, telephone numbers, emails, family members, and so on were leaked from this site.

Other platforms where information (whether leaked or not) can be stored and discussed include the IntelExchange forum and the Stock Insider, where users who have been approved share information about trading on various stock exchanges and reveal speculative activity. Storage sites are not only used by malicious leakers but often also by government entities and intelligence organizations that wish to share information anonymously. They "stick" the files they want to share onto the storage sites, using a misleading name, and

40 David Leigh, Luke Harding, and Charles Arthur, *Wikileaks: Inside Julian Assange's War on Secrecy* (New York: Public Affairs, 2011).

then send a message to the traditional media (such as by a text message) using the same name.

Trading Platforms

Several anonymous sites offer to buy or sell classified information. Businesses often post requests for leaks about their competitors' activities, and there have been cases where journalists and intelligence personnel have offered to trade information. One such site is SellFile, where information and services are offered for sale with payment by bitcoin. In the case of influence campaigns, it is possible to purchase entire voter lists on the Dark Web, including contact details, as well as political inclinations. With this data, it is possible to target potential voters on social networks.

Not only information is traded on these platforms. Recently published research indicates that the Dark Web is becoming the main source for the sale and delivery of malware designed to infiltrate specific organizations and industrial sectors.[41] This malware may also be used in cyberattacks aimed at interfering with elections. Senior personnel in the US intelligence services estimate that it is highly probable that hackers will try to corrupt or even destroy databases holding voter registration details for the 2020 presidential elections by using ransomware. These kind of cyberattacks generally lock down the infected computers until a ransom is paid, usually in crypto currency. One example is the 2017 global cyberattack, NotPetya, attributed to Russia. The attack used ransomware to screen a technique of data deletion, which made the victims' computers completely unusable. This threat is particularly worrisome in view of its potential influence on voting outcomes. An attack of this kind, if not identified before the elections, could sabotage voting lists, cause enormous confusion and delays, deny many people the right to vote, and even raise questions regarding the validity of the results.[42]

Digital weapons, including malicious software such as EternalBlue and WannaCry—whose tracks lead to North Korea and have caused damage estimated at almost four billion dollars to business and government computer

41 Yossi Hatouni, "What Are the Most Popular Hacking Tools Offered for Sale on the DarkNet?," *People and Computers*, July 11, 2019 [in Hebrew].

42 Christopher Bing, "Exclusive: U.S. Officials Fear Ransomware Attack against 2020 Election," *Reuters,* August 26, 2019.

systems in several countries—are also available on the Dark Web at relatively low cost and could be used by hostile elements for cyber influence campaigns.[43]

In addition to malware and hacking tools, the large number of abandoned accounts on social media platforms are also an important and convenient target for hackers due to their many points of security vulnerability. Bot networks on Twitter, Facebook, and Instagram, designed to spread disinformation and increase "involvement"—by using shares and likes in order to create a misleading impression of public interest around certain content—are offered for sale on the Dark Web for very small amounts. Similar offers are made for separate packages of retweets, likes, and YouTube views.[44]

The three platforms surveyed above have three common uses: to increase the power of the leaking country, to damage the subject of the leaks, and to promote human rights in certain countries. Thus, the РосПравосудие site on the Dark Web has published about fifty million documents dealing with the Russian legal system, with personal details of judges, lawyers, prosecutors, and so on. The operators of the site claim that they are leaking the information as a means of exerting pressure on those who manipulate the law in favor of the regime, and—more importantly—to discredit those who participate in show trials with predetermined outcomes. At present, it is not clear who is behind this site—internal and external elements who seek to undermine Russia's status, or Russian citizens who understand the importance of a proper legal system.[45]

There are numerous examples of how the Dark Web has been used to influence elections. In 2016 the servers of the US Election Assistance Commission were hacked and stolen entry passes of its employees were discovered on the Dark Web.[46] That same year, Russian hackers invested about 95,000 dollars in cryptic currency to set up fake websites and social media accounts to be used for influence campaigns.[47] In early 2017, the US Justice Department revealed that in the framework of attempts to influence the 2016 presidential elections, Russian hackers had obtained access to

43 Ibid.
44 Dan Patterson, "The Dark Web Is Where Hackers Buy the Tools to Subvert Elections," *CBS News,* September 26, 2018; "Influence for Sale: Bot Shopping on the Darknet," *DFRLab*, June 19, 2017.
45 Topor, "Deep and Dark Webs – Liberty or Abuse."
46 Joseph Menn, "U.S. Election Agency Breached by Hackers after November Vote," *Reuters*, December 16, 2016.
47 Topor, "Deep and Dark Webs – Liberty or Abuse."

more than half a billion email accounts on the Yahoo site. The hackers also managed to break into 6,500 user accounts, including some who were targeted in advance by the Russian government, such as journalists and members of the opposition. Access to other accounts was auctioned on the Dark Web, apparently in order to increase the profit from hacking.[48] In 2017, about forty million records of American citizens were offered for sale on the Dark Web for only four dollars. The small amount requested reinforces the belief that the sale was not done for profit but rather for ideological reasons. Furthermore, within the context of the US mid-term elections at the end of 2018, a database of tens of millions of American voters was discovered for sale on the Dark Web. In addition to the voters' personal details, the database also contained information about their political views and which candidates they supported.[49]

These databases can be used to increase the accuracy of targeting potential population groups and the frequency of phishing attacks. In this context, attackers disguise themselves as service providers, such as banks, operating systems, or government institutions, in order to obtain personal details for use in influence campaigns.[50]

Prior to the 2019 elections in Israel, cyber tools were offered for sale on the Dark Web, which apparently had been developed by Ukrainian hackers and were designed to overcome the restrictions imposed by WhatsApp on the number of contacts who could receive messages simultaneously. The tools gave their owner the ability to take remote control of WhatsApp groups in Israel and plant video and text content. In addition, members of the chat group would receive the message from one of the other members of the group, suggesting that the message appeared trustworthy.[51] According to Ben Caspit, Israeli entities recently purchased for hundreds of thousands of dollars the option to send 15 million WhatsApp messages within 48 hours. The ability of Facebook to block this capability is limited, although hackers on the Dark Web will sell a counter defense, which attacks these messages

48 Ilan Geller, "Simple and Brilliant: How Russian Hackers Broke into Millions of Email Accounts without a Password," *Walla*, March 19, 2017 [in Hebrew].

49 Rafaella Geuchman, "Details of 62 Million American Voters Offered for Sale on the Darknet," *TheMarker*, November 6, 2018 [in Hebrew].

50 Patterson, "The Dark Web is Where Hackers Buy the Tools to Subvert Elections."

51 Ben Caspit, "The Threat to These Fateful Elections Comes from the Underworld of the Internet," *Maariv*, September 9, 2019 [in Hebrew].

as soon as they appear and creates enormous artificial demand that causes the system to collapse.[52]

Conclusion

The aim of this article was to draw attention to the Dark Web as an additional channel for implementing cyberattacks and influence campaigns and to explain how the various players achieve their aims. The importance of the Dark Web as a platform for attempts to influence election campaigns has increased in parallel to the growing number of revelations about foreign interference in the elections of various countries, and especially with Russian involvement. Naturally, this has led to a rise in the attempts of governments and media giants to protect themselves against the known techniques of these efforts. In this context, the use of bots to influence social media has perceivably dropped while activity on instant messaging applications has increased. There is also a significant rise in activity on the Dark Web, which provides greater privacy and anonymity than the regular internet, and, as a result, exposing and fighting its influence campaigns therefore presents a greater challenge. Apart from the technological challenge, there is also a conflict between the need to protect public discourse and to maintain the principle of free speech, which the Dark Web aims to promote.

This article surveyed the three main types of leak platforms on the Dark Web: platforms calling for leaks of information, such as WikiLeaks or Secure Drop; passive platforms, such as IntelExchange, DOXBIN or the Stock Insider, where leaked data is stored; and trading platforms, such as SellFile, which offer information for sale and receive requests for information. Malware, spyware, bot networks, and cyber and media encryption tools all can be acquired on the Dark Web for using in influence campaigns, which can be done easily and anonymously.

These tools and the three platforms described are being used by countries and organizations to exercise influence in cyberspace, as shown in the above examples. Although the reliability of the information flowing over the Dark Web is controversial, this is often irrelevant to the entities seeking to influence how people vote; the mere fact of the leak serves their main purpose—to sow doubt and undermine the existing order. Given the relatively low cost of the capabilities offered for sale on the Dark Web and the difficulty of

52 Ibid.

tracking the source of leaks, we can expect a growth of both supply and demand for these tools.

The presence of democratic regimes on the Dark Web and how they use it is another interesting issue. On one hand, they have to deal with the subversive activities of terrorist organizations and totalitarian regimes, as well as with crime, which means there is no alternative to being involved in the Dark Web, as a "know your enemy" tactic. On the other hand, the use that democratic regimes make of the anonymity of the Dark Web appears problematic: Democratic regimes are not exempt from the tough international game, but the methods they use are important, particularly when they claim to be more "ethical." It can be assumed that the democratic administration that launched the Dark Web also makes the most extensive use of it, as a senior US official hinted to one of the authors at a conference in Washington DC in September 2019.

Another ethical question raised here is whether democratic governments confine their use of the Dark Web to actions against their international enemies, or do they also target rivals at home? Members of parliaments all over the world, including members of the Israeli Knesset, leak information from meetings and sometimes face charges for doing so. On the other hand, leaking on the Dark Web offers far greater anonymity, as well as the ability to cause chaos in the political system.

Social Change Through Computerized Accessibility of Legal Rules

Michal Tadjer, Michael Bar-Sinai, and Mor Vilozni

This article presents a self-help software system that makes rights accessible through an on-line interview. The interview is based on a formal model of the relevant jurisprudence and does not require the involvement of a service representative, only a user who wants to understand his or her rights. In addition, the article provides a methodology for building models and interviews for similar social contexts and describes building a model for workers' rights according to Israeli law, upon completing their employment. In addition to conducting interviews, these models can be used to create diagrams and perform legal queries. This kind of system can fulfill a central role in empowering disadvantaged populations, as it enables people to asses their rights in a user-friendly manner, which is personalized to the situation of the interviewee and not overburdened with large amounts of information that it is difficult to navigate. PolicyModels—the system presented here—can be used in different contexts, such as modeling privacy requirements in databases.

Keywords: Information sharing, software tools, computational models, information security, labor law, workers' rights

Adv. Michal Tadjer has worked as an attorney on issues of labor and immigration since 2003 in the framework of non-profit social change organizations. Michael Bar-Sinai is a post-doctoral fellow at the computer science department of Ben-Gurion University, a fellow at the Institute for Quantitative Social Science at Harvard University (IQSS), and also established CodeWorth.io. Mor Vilozni is a senior software engineer at CodeWorth.io.

The work described here was funded in part by the Israel Innovation Authority, through the Innovation in the Public Sector track.

Introduction

Each day, dozens of workers congregate at the crowded offices of Kav LaOved. These workers come from different backgrounds and countries and speak different languages. Each day is organized so that a specific population of workers is seen by a different set of volunteers. Thus, for example, volunteers who speak Tigrinya and Arabic work at the organization on days designated for receiving asylum seekers, while Thai translators are in the office on days specifically designated for migrant agricultural laborers. The Israeli staff includes Amharic and Russian speakers. The workers ask for information, assistance, and advice, and often legal assistance, in order to understand and exercise their rights. At the center of the room is a counter with informational pamphlets on labor laws, national insurance, health insurance, visas for asylum seekers, information for caregivers, and sexual harassment. Since the workers have trouble finding the right pamphlet for their problem, they are obliged to wait in the long and growing line.

A person whose rights have been violated must pass through several stages before being able to submit a lawsuit. The stages are known as naming, blaming, and claiming.[1] The first stage is naming the violation; that is, giving it a legal definition; the second stage is placing blame, which is mainly understanding who is the party responsible for the violation of rights and taking a stand against it; and the third stage is legal recourse, in which the claims and insights are translated into legal language. This process is lengthy and time consuming, especially for victims who belong to disadvantaged populations.[2] Experience shows that the chances of counteracting a violation and restoring the situation to its previous state (such as in an illegal dismissal) or of filing a lawsuit without fear of exceeding the statutes of limitation for the offense are greater when the first two stages of the process occur quickly after the violation.

We looked for an easy and direct way to provide workers with self-access to the information needed for independently conducting the "naming" and "blaming" stages. A software system called PolicyModels has offered a possible solution. This system enables the creation of a formal model of a legal domain that can be processed in various ways. The term "formal model"

1 William Felstiner, Richard Abel, and Austin Sarat, "The Emergence and Transformation of Disputes: Naming, Blaming, Claiming," *Law and Society Review* 15, no. 3 (1980): 631.

2 Yuval Elbashan, "Access to Justice for Disadvantaged Populations in Israel," *Aley Mishpat* 3 (2004): 501–503 [in Hebrew].

comes from the field of software engineering and refers to a well-defined mathematical description of a certain system (such as set theory or graph theory). Navigation apps, such as Waze, are an example of software tools that are based on a formal model of the built environment. This model allows them to provide their users with directions for reaching a specific destination or with information on all of the gas stations within three kilometers of their current location.

Daily experience at Kav LaOved shows that people, particularly those who are members of marginalized populations, do not know how to describe in legal terms what has happened to them. Therefore, when we dealt with rights connected to the termination of employment, we did not refer to the termination in the model as "dismissal," "resigning" or "resigning under circumstances of dismissal." Instead, we used "the work has ended." From this simplified state, which anyone can understand, a series of questions begins, phrased in simple language and designed to be translated into all languages. Legal conclusions and recommendations for action in various areas are derived from answers to these questions, and the institutions that the person should contact in order to address the situation are determined and named. For example, termination of employment has implications for all areas of life, based upon the person's status in the State of Israel: the law for the termination of employment of a migrant worker in an employer-bound track[3] is different than the law for the termination of employment for an Israeli worker who is pregnant. The former must quickly deal with the issues related to his work permit in order to move to a different employer; the latter will need to contact the commissioner for the Employment of Women Law at the

3 The employer-bound arrangement was created by the authority of the Interior Minister, according to Section 6 of the Entry into Israel Law. This section grants the Interior Minister the authority "to determine conditions for providing a visa or residence permit and for the extension or replacement of a residence permit," and the authority "to determine for a visa or residence permit conditions whose fulfillment shall be a condition for the validity of the visa or of the residence permit." The Foreign Workers Law, 1991, Law Book 1349 (hereinafter: "Foreign Workers Law") states that "a person shall not accept a foreign worker for employment unless the commissioner or an Interior Ministry worker acting on his behalf has permitted the employment of the foreign worker by that employer in writing, and in accordance with the conditions of the permit" (Section 1.XIII(a)) [in Hebrew]. For a description of this arrangement—"Regulation for transfer from employer to employer"—which was determined in 2002, see High Court 4542/02, *Kav LaOved v. Government of Israel*, rulings book 61(1), p. 346, paragraphs 7, 9–11, from the ruling of Justice Levy (2006) [in Hebrew].

Ministry of Labor, Social Affairs and Social Services, and must know that her dismissal is invalid unless the commissioner permitted the employer to do so.

We tried to estimate all of the possible legal implications of a certain situation, especially as they apply to disadvantaged populations who have difficulty gathering the information by themselves and for whom the power relations as they relate to their matters are extremely unequal, while also addressing their needs in a quick, accessible, independent, and personalized manner. This personalization is a significant improvement over websites that have made information about rights accessible (such as the website Kol Zchut),[4] which are based on textual descriptions of rights. While the descriptions tend to simplify the legal terms, the users still needs to read a large amount of text, especially about legal situations or rights that are not relevant to their individual cases. In addition, translating these websites into other languages requires considerable effort even more so than the legal models discussed here. This is important, as the nature of Kav LaOved's work also necessitates translation into a relatively large number of languages.

This rest of article is organized as follows: First, we discuss the objectives of the project of modeling termination-of-employment rights, upon which this article is based. The section "The transition from the legal field to a computer model" details the challenges in creating a formal description of legal rules and suggests a way to address these challenges. In the section on the PolicyModels system, we provide a general description of the software system that we used to create the legal model and to carry out interviews. Finally, the section on "Method for building policy models" offers a general methodology for building models for making rights accessible.

Objectives

The project is intended for use in the field of workers' rights, and it aims to give the computerized tool a significant role in balancing the inherent inequality that exists between workers and employers.[5] The provision of

4 See https://www.kolzchut.org.il.

5 Judy Fudge, "Labour as a 'Fictive Commodity': Radically Reconceptualizing Labour Law," in *The Idea of Labour Law* ed. Guy Davidov and Brian Langille (Oxford University Press, 2011), pp. 120, 124; Paul Davies and Mark Freedland, *Kahn-Freund's Labour and the Law* 3rd ed. (London: Stevens and Sons, 1983), p. 18: "The main object of labour law has always been, and we venture to say will always be, to be a countervailing force to counteract the inequality of bargaining power, which is inherent and must be inherent in the employment relationship. Most of what we call protective legislation . . . must be seen in this context. It is an attempt to infuse law into a relation of command and subordination."

assistance to workers with limited bargaining power in the labor market is "the moral basis and the founding narrative" of labor law,[6] and, in the words of the National Labor Court, "labor law is a law of 'inequality,' whose purpose is to compensate for the weakness of workers vis-à-vis employers."[7]

Upon this traditional basis of labor law, contrary processes are taking place. Over the past decade, globalization and transformations in Israel's economy and society have led to significant changes in the labor market. International corporations are influencing the local economy more than before; many organizations are undergoing processes of change; the demand for economic efficiency is growing, while values like organized labor and social solidarity have been marginalized; the migration of workers and factories has become routine; the state is advancing processes of privatizing public services in the name of economic efficiency; individualism is growing stronger and free competition is becoming a basic constitutional right;[8] non-Israeli workers are participating in the labor market in increasingly large numbers, influencing employment norms in many industries and they themselves are also influenced by immigration policies, which in turn deeply influence both their labor rights and bargaining power.[9]

On the other hand, public access to information is increasing, and social networks now serve as a primary source of information.[10] Kav LaOved increasingly has recognized the importance of this tool specifically for isolated populations with language barriers and thus operates several

6 Brian Langille, "Labour Law's Theory of Justice," *The Idea of Labour Law*, p. 101, footnote 83, and p. 105. However, the central idea presented in this article is that a new purpose needs to be formulated for labor law instead of the traditional purpose.

7 National Labor Court hearing 340/2–35, Kozolovitz v. Ordan Ltd., *Rulings of the Labor Court,* 12, no. 1 (1981), p. 200 [in Hebrew].

8 See, among others, Ruth Ben-Israel, "The Management Prerogative of the Employer," *Tel-Aviv University Law Review* 25 (2006) [in Hebrew]; Ruth Ben-Israel, "Social Justice in the Post-Labor Era," in *Distributive Justice in Israel*, ed. M. Mautner (Ramot Publishing House, 2000) [in Hebrew]; Aeyal Gross, "How Did 'Free Competition' Become a Constitutional Right," *Tel-Aviv University Law Review* 23 (2000) [in Hebrew].

9 Guy Mundlak, "Workers or Foreigners in Israel? The Infrastructure Contract and the Democratic Deficit," *Tel-Aviv University Law Review* 27, no. 2 (2003): 423 [in Hebrew].

10 The Pew Research Center compared the use of social networks in the United States in 2005 versus 2011. The study shows that during these six years, the number of social media users increased considerably. In 2005, only eight percent of internet users reported using social media; as of 2011, two-thirds (65 percent) of adult internet users used social media sites—more than two times the figure for 2008, when only 29 percent reported that they used a social network.

dedicated Facebook pages for the various communities of workers in different languages. For example, the Facebook page dedicated to migrant workers in the caregiving industry has more than 48,000 members (two-thirds of the number of migrant workers in this industry in Israel), and each post receives hundreds of shares, comments, and questions. The more isolated a population is, the more important access to information and the power of technology seemingly become for creating community—albeit a virtual one—which eases social isolation and serves as an accessible point of contact for information and advice. In this context, it should be noted that women increasingly are using social media and studies note the role of this use in the gendered power relations.[11] The amount of information available, however, makes it difficult for workers to find independently information that is relevant to them, and their fellow virtual community members are generally not professional enough to help them with this.

We will briefly relate to the "media richness" theory,[12] a perspective that allows for examining different media according to their ability to convey information. The basic assumption is that the more opaque the information is, the more important it will be to choose a richer medium, with the richest one being face-to-face communication. However, the "paradox of richness" holds that a "rich" medium of communication can transmit too much information (some of which is irrelevant), distracting from the main message and interfering with understanding the situation. This paradox could also explain the meager use of the information pages at the offices of Kav LaOved that are packed with information. In most cases, a worker in distress does not have the capacity to find the "needle in the haystack."

Is the worker's situation really so unclear that an in-person meeting with a Kav LaOved volunteer is necessary? The model that we suggest here claims that there is another way. In consumer decisions, the internet influences

11 In its research, the Pew Research Center consistently finds a pattern in which women use social media more than men in the same countries.

12 John Carlson and Robert Zmud, "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions," *Academy of Management Journal* 42, no. 2 (2017): 153–170; Vivian Sheer and Ling Chen, "Improving Media Richness Theory: A Study of Interaction Goals, Message Valence and Task Complexity in Manager-Subordinate Communication," *Management Communication Quarterly* 11, no. 1 (2004): 76–93; Richard Daft and Robert Lengel, "Information Richness: A New Approach to Managerial Behavior and Organizational Design," *Research in Organizational Behavior* 6 (1984): 191–233.

consumers more than anything;[13] our goal in this project is to maximize the internet's ability to help workers in distress.

The Transition from a Legal Field to a Computer Model

Law and technology are part of "culture."[14] Similar to literature and law, "these are two different cultural phenomenon that have a complex relationship, and despite the difference—they need one another and complement one another."[15] A discussion of the difference between legal rules and a technological model is beyond the scope of this article. It is a known secret that the legal field is not set up for unambiguous structuring, and it is no accident that legal decisions are written over the course of dozens and hundreds of pages. The legal field is composed of primary legislation, directives (secondary legislation), case law that has been set out in court, and even procedures of government ministries. Legal interpretation of a person's situation requires clarifying information from his or her life events and giving them a legal headline, before turning to interpretation.

Technology also contains interpretation choices that can be biased,[16] such as hidden assumptions regarding the abilities of users, which can prevent certain people from using a computer system. One example is design that does not take into account people who are colorblind. In cases where the system's designers let technology make decisions by itself, for example via artificial intelligence techniques or computer learning, real algorithmic discrimination

13 Brian Solis, "Report: The Rise of Digital Influence and How to Measure It," BrianSolis, March 21, 2012, https://www.briansolis.com/2012/03/report-the-rise-of-digital-influence/.

14 See the comprehensive discussion of law as culture in Menachem Mautner, "Law as Culture, Towards a New Research Paradigm," in *Multiculturalism in a Democratic and Jewish State*, ed. Menachem Mautner, Avi Sagi, and Ronen Shamir (Tel Aviv: Ramot Publishing House, 1998), pp. 545–587 [in Hebrew]; Menachem Mautner, "Invisible Law," *Alpayim* 16 (1998): 45–72 [in Hebrew].

15 Shulamit Almog, *Law and Literature in the Digital Era* (Nevo Publishers, 2007), p. 5 [in Hebrew].

16 Kate Crawford and Tarleton Gillespie, "What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint," *New Media and Society* 18, no. 3 (2016): 410–428; Sandra Petronio, Jess Alberts, Michael Hecht, and Jerry Buley eds., *Contemporary Perspectives on Interpersonal Communication* (Madison, Brown and Benchmark, 1992), pp. 318–358; Janet Bavelas, "Some Problems with Linking Goals to Discourse," in *Understanding Face-to-Face Interaction: Issues in Linking Goals and Discourse*, ed. K. Tracy (Hillsdale, NJ: Lawrence Erlbaum, 1984), pp. 119–130.

can result. In such cases, a computer system can even demonstrate racist[17] or misogynist[18] behavior.

In order to answer the question of which rights and obligations result from a certain personal situation (such as in the termination of employment of a migrant worker after a heart attack), there must be a willingness to let go of distinguishing between what is set in law, and therefore is ranked higher, and what is determined by the Interior Ministry procedures, which have never undergone judicial review. The law presented in a computer model cannot be complex, as it is in court rulings, petitions, and lawsuits. Working on a computer model requires a willingness to simplify the legal field, make it accessible, and to let go of the hierarchies within it; it must be adapted to a computerized tool with all its limitations, while understanding that these limitations, in the spirit of the "paradox of richness" mentioned above, are also its advantages.

The PolicyModels System—Recognition, Description, Characteristics

The PolicyModels system used here allows for building a formal description of legal rules in a certain field and calculating how they relate to a specific case.[19] The system was originally developed in order to enable researchers to handle sensitive databases without violating laws related to privacy and without requiring expertise in privacy fields or the relevant technologies.[20] Later, this system was used to model the unemployment benefits period in Israel's National Insurance Law.[21]

---

17 Latanya Sweeney, "Discrimination in Online Ad Delivery," *ACM Queue – Storage* 11, no. 3 (April 2, 2013); Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias," *ProPublica*, May 23, 2016,https://www.propublica.org/article/machine -bias-risk-assessments-in-criminal-sentencing.

18 Amit Datta, Michael Carl Tschantz, and Anupam Datta, "Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination," *Proceedings on Privacy Enhancing Technologies* (2015): 92–112.

19 Michael Bar-Sinai, Latanya Sweeney, and Merce Crosas, "DataTags, DataHandling Policy Spaces and the Tags Language," *IEEE Security and Privacy Workshops* (San Jose, CA, 2016), pp. 1–8.

20 Latanya Sweeney, Merce Crosas, and Michael Bar-Sinai, "Sharing Sensitive Data with Confidence: The Datatags System," *Technology Science*, October 16, 2015, http://techscience.org/a/2015101601.

21 Michael Bar-Sinai and Rotem Medzini, "Public Policy Modeling using the DataTags Toolset," *The Network for European Social Policy Analysis*, 2017, http://mbarsinai.com/files/inii/ESPAnet17-Final.pdf.

When given a policy model, the PolicyModels system can present an interactive interview that applies it to a specific case. In addition, the system can draw flow and structure charts of the model and can identify all of the cases in which a certain condition holds true (for example, all the cases in which a worker can sue her employer). The system's structure enables carrying out additional analyses as needed.

The system itself is composed of a core software component ("library") and several tools. The core software component enables computer programs in which the software is included to work with policy models. Two programs have been developed around this core component: one is used for developing the models, and the other is a website that can perform interviews based on the models. The PolicyModels system has been released under an open source, industry-friendly license (Apache v2.0). This license allows anyone to read the system's source code and to develop additional systems based upon it, including commercial systems, without having to pay. These licenses prevent vendor lock-in and thus maintain the bargaining power of its users, who can switch software providers if they wish. In addition, these licenses allow programs to be written by volunteers and encourage the creation of communities of users and developers.

Below we will present the PolicyModels structure, as well as the existing tools for developing these models and for making them accessible.

Policy Model

As already stated, a policy model is composed of two parts: a policy space and a decision graph. The **policy space** describes all of the possible situations in which a person can be within the legal context that the model describes. It is a multidimensional space, in which each point describes one possible situation according to the law. Each dimension in the policy space describes a single legal aspect, and each coordinate in a given dimension describes a possible condition of this aspect. For example, the coordinates for the aspect of "age group" can be "before working age," "of working age," "voluntary pension age," and "pension age" (in this order). The dimensions of the space are ordinal; that is, the coordinates are in a certain order, but there is

no significance to the distance between them.[22] This order enables phrasing rules formally, such as "from working age on, a worker is entitled to X."

The greater the number of dimensions, the more precise the description of a given legal situation will be. However, this increases the number of questions that must be answered during the on-line interview. Thus, an effective policy space will include enough dimensions to describe all of the relevant aspects of the situation, but no more than this. For example, in the policy space of the model for termination-of-employment rights, it is relevant to specify whether the worker has a disability, but there is no point specifying what the disability is. This is because the details of the disability do not affect the worker's rights when his employment ends.

A typical policy space contains a large number of dimensions: the termination-of-employment rights model mentioned above contains 62 dimensions; the model of unemployment benefits according to the National Insurance Law contains 13 dimensions. For people used to a three-dimensional world, it is difficult to work intuitively with such a large number of dimensions. Against this backdrop, we developed several displays that make multidimensional policy spaces more accessible. In addition, the language for describing the policy spaces of PolicyModels includes means to hierarchically group the dimensions; for example, dimensions related to rights are in one group and those related to the situation are in another group. This hierarchy helps the builders of the model to organize the space for their work but does not substantially affect the space, because when the calculations are carried out, the system ignores the groups and relates only to the dimensions themselves.[23]

The **decision graph** is the second part of the policy model. Here too, the term "graph" is taken from the computer sciences, and it describes a mathematical structure that is made up of points ("vertices") and possible lines between the points ("edges"). It is possible to move between two vertices only if they are connected with an edge. It is customary to describe a graph visually using a group of circles connected with arrows. The circles describe the graph's vertices, and the arrows describe the edges. The calculation in

22 In this, the dimensions described are different from discrete dimensions, which use whole numbers, have an order, and for which distance is significant, and from continuous dimensions that use real numbers.

23 For details on the algorithm that enables the system to ignore the groups, see Bar-Sinai and others, "DataTags, Data Handling Policy Spaces and the Tags Language," *IEEE Security and Privacy Workshops (2016)*, https://doi.org/10.1109/SPW.2016.11.

the PolicyModels system starts with a designated vertex in the decision graph, and from there it continues along the edges of the model's decision graph. When the computer reaches a new vertex, it carries out an action that depends on the type of that vertex. This action can be, for example, updating the location in the policy space, presenting a question to the user, or running another part of the graph.

PolicyModels' decision graphs are able to find the location of a certain person's legal status in the model's policy space. They create synergy between the computer and the person, in which the computer handles the well-defined parts (for example, maintaining the locations in the policy space and the decision graph), while the person handles the parts that require knowledge of the details of the case or answers to "soft" questions, such as "does the termination of employment result from a significant violation of the worker's rights?" This division of responsibility between the person and the computer enables the PolicyModels system to overcome the built-in challenge of computers dealing with complex legal cases, as it does not rely on computerized judgment of "soft" questions, which are human in nature.

It is important to note that the interviewee's answers do not directly change the case's location. Such changes are carried out by the computer when it reaches vertices that instruct it to change the location. The person's answers can navigate the computer to such vertices in the decision graph. This separation between the person's answers and the change of the location in the policy space enables the builders of the graph to ask the person questions in a language that he understands but to manage the situation in formal terms. In addition, a person can be asked a number of guiding questions before changing the case's location in the space. In this sense, the shared computation process is similar to a conversation between a vehicle owner and a mechanic in a garage: the mechanic asks questions that the vehicle owner understands; for example, do you hear knocks from the engine at high speeds. In accordance with the answers, the mechanic makes a note for himself of whether to check the spark plugs, the engine head gasket, or the timing belt—terms that are too obscure for the average vehicle owner.

The process represented by a decision graph is not necessarily the only one possible. For example, the order and type of questions appropriate for an expert in labor law would be different than the order of questions appropriate for a layman in this field. Different decision graphs can work with the same

policy space. In terms of the system and its formal definitions, the important factor is the result of the interview—the coordinate in the policy space that describes the case, which is reached at the end of the interview. The process of reaching this coordinate is not important for later processes, such as the recommendations presented to the interviewee.

The decision graph can be very large; the current version of the graph in the termination-of-employment rights model includes 216 vertices. In order to enable effective work with this many vertices, the vertices can be grouped by topic; the graph can be divided into several sub-graphs; and the description of the graph itself can be separated into a number of files.

Texts and Translation

As presented so far, the policy model mainly contains data structures—the policy space and the decision graph. These structures contain considerable information but include very little text intended for humans. This text is maintained separately in "localization packages." These include a long text for each question, names and explanations for each value and each dimension in the policy space, and a translation of the model's meta-data (title, explanatory text, and so on). The texts for questions can include links to external sites, tables, and highlights. The values in the policy space represent concepts that are not always comprehensible to people who are not familiar with the field of the model, such as "in lieu of advance notice"[24] or "final pay." Therefore, the explanations for each value and dimension include three levels: the name of the dimension; a short explanation that appears in a text bubble above the value when the user moves the cursor over it; and a detailed explanation that can include several paragraphs, links, and tables.

A single policy model can include a large number of "localization packages." Thus, it is possible to make a single model accessible to speakers of different languages. Similar to translating programs, writing a new "localization package" requires little technical knowledge; thus, translators do not need to undergo extensive training in order to perform this translation.

24 This is a situation in which the employer waives the worker's work for the duration of the advance notice period, and instead pays full wages for this period.

User Privacy

During the interview, the user provides the system with personal information. Thus, it is worth addressing the topic of maintaining the privacy of users. The principles of Privacy by Design,[25] which have guided us in writing this system, state that user information must only be saved if it is required for the user's benefit. Thus, for example, users are not required to identify themselves to the system before the interview, as their first name, last name, or visa number do not affect the rights to which they are entitled by law. Although the system's default is not to save the interview and its results, for certain models, the system's administrators can ask to save statistics for use, for example, in order to understand which questions confuse users. While such statistics allow restoring an entire interview session, they do not connect that session to a specific person and instead use a random identifier created by the server.

Verifying the Policy Model

During the interview, the system takes the user through the decision graph, such that with each question, the interviewee chooses one answer that is the most appropriate to the case in question. It is also possible to choose all the answers for each question. In this method, the program runs through the decision graph independently without the help of an interviewee, and when it reaches a vertex with a question, it chooses one answer. From there, it continues to the next question and chooses the answer to it, and so forth until the interview ends. In this way it is possible to check the results of all possible interviews in the model.

This method, borrowed from the field of formal verification of software, enables asking broad queries about the policy model. For example, it is possible to ask in which cases a woman of working age would be eligible immediately for unemployment benefits. The answer to this question verifies that the policy model matches the law. If the model accurately describes the law, the answers to this question enable discovery of cases that the law does not cover.

25 Ann Cavoukian, "Privacy by Design [Leading Edge]," *IEEE Technology and Society* 31, no. 4 (2012).

Limitations of the Model

The main limitation of modeling polices with the PolicyModels program is the requirement that the dimensions of the space be ordinal and have a finite number of coordinates. Thus, open questions cannot be asked; the answers must come from a predetermined group of answers. For example, it is not possible to ask the interviewee his age (a numerical answer), but only what age group he belongs to and the interviewee must choose from a limited list. Similarly, dates cannot be input.

The program can be expanded to include numerical dimensions, and we are planning to explore this direction in the future. However, it is already possible to overcome the limitation described above in two ways: the first is by dividing the numerical field into ranges between which the law in question distinguishes. For example, instead of asking the interviewee for his numerical age, it is possible to ask him whether he is of working age or pension age; the second method is, at the end of the interview, to direct the interviewee to a rights calculator that was written especially for the field modeled. This calculator will receive the results of the interview and then ask the interviewee for the relevant numbers and carry out the final rights calculation. This method, for example, enables precise calculation of the severance pay to which the worker is entitled.

The Method of Building Policy Models

In this section of the article, we offer a method for building policy models, based on our experience in creating several of them. Policy models are similar to small computer programs, and thus, the process suggested is based on software engineering methodologies. We do not claim that this is the only method of building such models, or even the best method (assuming that there is such a thing); rather, our intention is to offer a sufficient method in order to allow others to start writing models and to initiate discussion on the issue. First, we will discuss the challenges facing teams wishing to write policy models; then we will examine the existing tools; and finally, we will suggest a methodology.

Policy models are legal-technological hybrids. Building a policy model for a certain legal field requires expertise in two areas—the legal field and the PolicyModels system—and poses the challenge of fruitfully combining them. Thus, a model-building team will usually be made up of two experts

from different backgrounds who will not be familiar with the complementary field. It is important to note that the level of expertise necessary in each field is different. Legal expertise requires deep understanding of the legal field, in addition to remaining up-to-date in it (for example, being familiar with recent rulings). In contrast, a person with basic training in computer programming can use PolicyModels after a relatively short amount of study; indeed, computer science students have succeeded in using the system after reading the training documents. Therefore, we estimate that a programmer with little experience can build models after one day of self-teaching. Clearly, the programmer's efficiency will increase with the more experience accumulated.

"Cultural" differences between computer programmers and jurists are another challenge that must be bridged, especially at the beginning of the work process: Many computer programmers have difficulty coping with obscure fields, such as the legal field, which have a range of contradictory opinions; jurists, for their part, must become accustomed to thinking about legal situations in formal terms, such as the policy space and decision graphs.

The PolicyModels system offers several tools that help address these challenges. First, it is possible to automatically create diagrams of the policy space and of the decision graph. These diagrams are user-friendly or, at least, less threatening than the textual code of the model. Second, the web-based system that is used for conducting the interviews can collect comments before the model is published, with the help of private links and an internal system of comments. Third, the modeling language itself supports the possibility of marking certain sections as "to do." The system is able to produce a detailed report of these parts and also automatically identifies parts of the policy space that the decision graph does not make use of.

In addition to these tools, the model's development team can use existing tools for software development, such as version and task management systems. These systems enable saving versions of the model at different times, examining different possibilities based on an existing version, connecting between tasks and updates to the model, and discussing updates to the model before accepting them. The possibility of working with these systems stems from the fact that the PolicyModels system is based on textual code and not on a special, closed file structure. An example of a popular open source

system is GitHub,[26] which we used when developing the termination-of-employment rights model.

The policy development methodology suggested here is based on an iterative software development process.[27] In this process, the model is developed over a number of rounds ("iterations") and at the end of each round, a working model is created, which can be presented to experts and users. With each progressive round, the model addresses the law more accurately.

There are four stages of development. First is the initial preparation stage. Before the work begins, a focused meeting should be held in which the modeling staff present the capabilities and limitations of PolicyModels, and the jurists survey the law in the field in question. For example, before developing the termination-of-employment rights model, we held a meeting that lasted four hours and included legal experts from Kav LaOved and the project's software engineering team. In this meeting, we presented a survey of both the relevant laws and the PolicyModels system, and we chose appropriate fields for modeling.

The second stage is the development. As part of this stage, a sub-field is chosen from within the field that is being modeled and the level of detail for building the model is planned. For example, in the first stage, broad areas are modeled with a low level of detail; in more advanced stages, specific areas are modeled more in depth. Automatic reports detailing which specific areas have not yet been completed can serve as a tool for choosing a sub-field for the next iteration.

In this stage, the legal knowledge relevant to the field is surveyed, including laws, directives, interpretations, and so forth. Based on this survey, an initial version of the policy space is built. Areas that are not fully detailed need to be marked as "to do" so that they appear in reports as requiring further detail. In this stage, the decision graph is written. Here too, parts that are not fully detailed are marked as "to do." Computer-generated diagrams of the decision tree are very useful at this stage in order to ensure that the order of questions in the interview accurately reflects the intention of the developers. This stage usually also includes changes in the policy space and sometimes also in other parts of the tree. Detailed texts are written for the new questions, dimensions, and values.

26 "Built for Developers," *GitHub*, July 2019, https://github.com.

27 Craig Larman and Victor Basili, "Iterative and Incremental Development: A Brief History," *IEEE Computer* 36, no. 6 (2003): 47–56.

The third stage is the testing stage, in which the newest version is uploaded to the server and defined as "private," so that only authorized users can see it. This version is tested with several cases. Feedback from experts in the field is collected, by presenting the interview or sending a link and listing comments in the system. The model is updated according to the feedback.

The fourth and final stage is when the final version is released. The model is uploaded to the server and defined as public to enable all internet users to use it.

From our experience in developing the model for termination-of-employment rights and the model for unemployment rights according to the National Insurance Law, we learned that a series of weekly meetings between the legal expert in the field and the PolicyModels programmer is a relatively effective way to build the model. The length of each of these meetings ranges between two and three hours, and sometimes even more—depending on how much time the staff members have and their stamina.

Conclusion

One of the objectives of developing the model described in this article was to examine its ability to simplify legal information and make it accessible to disadvantaged populations. The assumption was that a series of simple questions could lead to identifying the user's unique legal situation. Such a questionnaire has an advantage, especially for populations that are not used to reading long texts and filtering information, and thus are reluctant to browse text-based websites that aim to make rights information accessible (such as Kol Zchut, mentioned above).

We found that a model can be built, and even though it presents a rather superficial picture of the legal situation, its personalization is useful for the user. That being said, this modeling has a disadvantage, which lies in its oversimplifying of the legal picture and in its inability to address the nuances of interpretation that are quite common in the legal field. Therefore, a field or sub-field should be chosen in which there is a reasonable level of legal agreement (disagreements between jurists tend to be more common than between engineers; this is a cultural difference that engineers are surprised by, but must also get used to). In addition, modeling legal fields that require the use of open questions is more difficult and could even require additional processing of the results by a designated system or by a human expert.

The transition from law to a format of unambiguity and simplicity, which is required in using a computerized tool, is undoubtedly complex and is not suitable for all fields of law. It is necessary to choose a specific situation, whose legal conclusions are relatively simple, and to remember that this is a tool and not a definitive answer. Thus, in cases where our questionnaire indicated severe harm, such as sexual assault or exploitation, we refer the interviewees to the proper aid services. It is worth emphasizing that the very acts of identifying the offense and locating the right institution to contact are part of the solution.

The requirement to choose one correct way of addressing a situation often helps to focus agitated workers, who are in a state of confusion and stress. It also defines for themselves and for those assisting them the right that has been violated. Every jurist who has volunteered or worked at aid organizations for disadvantaged populations knows that the critical task, in many cases, is to understand—in the midst of all the experiences, feelings, and narratives—the legal issue at stake that requires and permits treatment. Modeling the law using the method offered here may therefore benefit both the workers and those volunteering to help them.

The Use of Biometric Technologies—Normative and Legal Aspects

Limor Ezioni

The development of technology that can identify a variety of physical and emotional characteristics and specifically of biometric technologies has reached a level of maturity and prevalence that require an explicit legal and normative examination of all aspects of their use. The unbridled rush to develop these technologies in Israel and abroad has neglected to address the legal and ethical aspects. This article examines the development of biometric technologies and the ethical and legal aspects of their use. Israel has great interest in the economic development resulting from biometric applications, and this article therefore proposes an international process that aims to create a legal and ethical discussion of the important questions that arise from the broad deployment of biometric technology. In this way, the State of Israel will continue shaping the norms in this field in the future.

Keywords: Biometrics, facial recognition, privacy, databases

Introduction

In December 2018, the British newspaper the *Guardian* published an article about the use of biometric tools in a performance by the singer Taylor Swift, which included hidden cameras for facial recognition in order to compare photographs of the audience with a database composed of photographs of stalkers—compulsive fans of the singer who may pose a security threat for

Dr. Limor Ezioni, Adv., is a criminal law specialist, a senior lecturer at the Academic Center of Law and Science, and a senior researcher in the Cyber Security Program at the Institute for National Security Studies.

the object of their admiration. The security challenges created by stalkers are not to be taken lightly; the singer has a number of known stalkers, against whom restraining orders have been issued, and one has even threatened to rape and murder her. The problem in this context is that the cameras were used without the audience knowing about them or their function.[1]

There were, of course, events that preceded the use of the hidden cameras at Taylor Swift's concert. In April 2019, it was reported that an American youth was suing Apple after being falsely arrested by the company, which employed facial recognition technology in its stores and therefore harmed the privacy of its shoppers.[2] Police arrested the youth in New York after another person had used his pictureless ID and other stolen details to steal from the company's stores in New Jersey, Delaware, and Manhattan. The company used the ID details it had in order to find a picture of the youth, which was then compared with the images produced by the facial recognition technology installed in its stores, leading the company to file a complaint against him with the police. The police then discovered that the youth had been a victim of fraud and was not the real thief.

In the youth's lawsuit against the company, he argued that the connection Apple had made between the stolen items and his true identity, including a photograph of his face that was fed into the stores' security systems, harmed his fundamental rights, without the company having the authority to do so. As a result of the lawsuit, legal experts debated whether the lawsuit had a strong foundation and if, indeed, Apple had contravened the law. Some even claimed that this case realized the vision of George Orwell, with a technology company capable of becoming "Big Brother" and monitoring everyone.

Biometric facial recognition technologies have developed significantly over recent years and are used by security companies in different capacities, which include identifying terrorists in crowded places (train stations, airports, and so forth) by comparing images to existing biometric databases and allowing efficient and controlled entry of crowds to large areas.

This article examines the ethical and legal dilemmas resulting from the employment of biometric technologies in a variety of capacities, by looking at various aspects of the existing legal framework. It is evident already that

1 Laura Snapes, "Taylor Swift Used Facial Recognition Software to Detect Stalkers at LA Concert," *The Guardian*, December 13, 2018.

2 Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest," *Bloomberg*, April 23, 2019.

the development of biometric technologies and biometric databases has reached a stage of maturity and prevalence that require an explicit legal and normative examination of all aspects of their use.

Theoretical Background

The advancement of biometric identification technology has led to a wide range of uses in the private and public spheres. Many workplaces have begun adopting biometric applications as they enable employers to save resources and increase security; however, employees are frequently hesitant to permit the use of biometric data, due to concern that it could be misused.

Darrell Carpenter and colleagues examined three aspects of the use of biometric technologies in the context of privacy. First, they surveyed how the employees of a company that installed biometric systems understood the responsibility of privacy; second, they examined the feeling of vulnerability that biometric systems create; and third, they looked at the notion of the lack of trust in the company. The results indicated that the company was able to diminish the concerns about harming privacy in all three dimensions by including the employees in the drafting of the rules of use for these systems.[3]

Another study examined the use of biometric applications in the healthcare sector, specifically of genome data in the context of cancer and rare diseases, which also has secondary uses that may have been more broadly distributed.[4] The study surveyed the extent to which one can obtain the authority to use private biometric information (in this context, information concerning the mapping of the personal genome) and showed that patients may choose to store genetic information online so that healthcare professionals have access to it. The study addressed the need to ensure that the identity of those who can access the information is properly verified in order to protect patient privacy throughout the process of storing and using the information. According to the study, verification of identity has two functions: preventing impersonation and proving the intent of the use of the information. These are essential steps

3 Darrell Carpenter, Alexander McLeod, Chelsea Hicks, and Michele Maasberg, "Privacy and Biometrics: An Empirical Examination of Employee Concerns," *Information Systems Frontiers* 20, no. 1 (February 2018).

4 Atsushi Kogetsu, Soichi Ogishima, and Kazuto Kato, "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy and Trustworthiness," *Frontiers in Genetics* 9 (June 1, 2018).

in ensuring that medical research and exchange of healthcare information are used for appropriate ethical purposes.

Anton Alterman has examined the ethical aspects of biometric identification.[5] He argued that there is both a private and a public interest in biometric identification: they create a balance as there is a kind of tradeoff between the private and the public in using biometric technology for identification purposes. His main conclusion was that the general right to privacy includes the right to control the information that is collected by biometric components and this should be an overriding right. This means that the decision to allow other parties to access personal biometric information must be carefully made, taking into consideration a number of factors, including the accessibility of the information at the expense of losing control over it, information security, and the risks of misuse of the information.

The increasing use of biometric identification makes it necessary for an individual to assess the extent to which he is prepared for his personal information to be sent to other parties in order to receive better and more rapid service. The question addressed is to what extent a person can control the use of his biometric information. Alterman proposes that anyone who is requested to provide biometric information should also be informed of its results and impact in terms of the improved service as a result of rapid biometric identification while at the same time being made aware of the potential risks involved.

In Israel, in 2011, a unit was established in the Prime Minister's Office to develop the field of biometric applications, following the passage of the "Inclusion of Biometric Means of Identification and Biometric Data in Identifying Documents and Databases Law." Later the unit was placed under the responsibility of the National Cyber Directorate.[6] Israel also established a national biometric database, with the goal of preventing impersonation and identity theft. The website for the National Biometric Database Authority states that "in the current situation, and even in a situation of smart biometric documentation but without a biometric database, a person can still impersonate someone else and obtain a number of certificates with different identities

5 Anton Alterman, "'A Piece of Yourself': Ethical Issues in Biometric Identification," *Ethics and Information Technology* 5 (2003): 139–150.

6 The National Cyber Directorate's web page about the Biometric Identification and Applications Unit (in Hebrew) was launched in May 2018. See https://www.gov.il/he/departments/news/bio_aboutbiometric.

simultaneously. This is because in the absence of a biometric database, the Population Authority has no way of ensuring that a person requesting a certificate is not an impersonator."[7] In this context, a distinction must be made between a biometric system that enables identification by cross referencing a person's data with a broad database, which searches for a match within that database (for example, identifying a criminal by a fingerprint, photograph, or DNA) and a system that verifies one's identity by examining a person's biometric details that have been previously sampled (such as passing through the biometric passport line at the airport).

There is a lively debate surrounding all aspects of the use of biometric applications, and even more so regarding the very establishment of the National Biometric Database. Omer Teneh shows the extent to which the Biometric Database Law in Israel could risk harming the right to privacy, should the collection of biometric data not be done for a worthy purpose that is consistent with the values of the State of Israel. According to Teneh, biometric systems create ethical problems as a result of how the information is used. For example, when it is integrated into other system, such as security and tracking cameras, the security purposes of the biometric database could disproportionately harm fundamental values, such as privacy and a person's right to autonomy over his own person. In addition, the development of technology erodes the right to privacy in a permanent and continuous manner, as the technology companies gather a lot of information about internet users through search engines, browsing information, location data, social media connections, and more, enabling identification through irrefutable biometric information. According to Teneh, even though biometric systems may have a positive impact on the right to privacy, enabling identification by using minimal information may also have negative implications on the right to privacy when a person's identity is minimized to "a collection of biometric data."[8]

7 See the National Biometric Database Authority website (in Hebrew) at https://www.gov.il/he/departments/general/target_goals.

8 Omer Teneh, "The Biometric Database Law: Risks and Opportunities," *The Law*, 17, no. 2 (5773–2013) [in Hebrew].

The Biometric Database Authority in Israel has adopted a code of ethics.[9] The code sets forth that the Authority bears practical responsibility for the lawful processing, maintenance, security, and accessibility of the biometric data. The Biometrics Database Authority is also required to maintain the privacy of those whose biometric data it possesses and to prevent any unlawful use. The code of ethics also states that the Authority and its employees must ensure that all activities within the National Biometrics Project are carried out with the goal of serving the public good, ensuring human dignity, and maintaining citizens' rights according to the principles of a democratic society. The code also establishes that the Biometric Database Authority will operate on the basis of minimal biometric data, with it being required for designing ID cards and passports, protecting personal identity, and thwarting the use of counterfeit ID cards and passports.

Israel is not alone in this area as other countries also have established biometric databases. In April 2019, the European Parliament decided to establish a biometric database that could become the largest in the world.[10] The objective is to enable better control over state borders in the European Union. The European biometric database—known as the Common Identity Repository (CIR)—intends to store approximately 350 million identities and will include details such as names, dates of birth, passport numbers, and other identifying details, alongside biometric details, such as fingerprints and facial scans. This data will be available to border authorities and enforcement personnel in EU countries. Even though the European Parliament and the European Council promised "proper protective means" to protect individuals' right to privacy and to regulate enforcement authorities' access to the data, it remains unclear what protective means are being put to practice.

The General Data Protection Regulation (GDPR) of the European Union has posed a challenge for EU authorities in dealing with biometric data. Raul Sanchez-Reillo and others examined the question of how European regulations

9 "The Biometric Database Authority – Code of Ethics," State of Israel, Ministry of the Interior, Biometric Database Authority, 2015. For more information on the ethical aspects of biometric identification, see Annemarie Sprokkereef and Paul De Hert, "Ethical Practice in the Use of Biometric Identifiers within the EU," *Science and Policy* 3 (2007): 177–201; Emilio Mordini and Carlo Petrini, "Ethical and Social Implications of Biometric Identification Technology," *Annali dell'Istituto Superiore di Sanita*, 43 (2017): 5–11.

10 Catalin Cimpanu, "EU Votes to Create Gigantic Biometrics Database," *ZDNet*, April 22, 2019.

could be adopted to protect biometric data.[11] They describe the challenges and recommend a series of measures intended to protect the acquisition and use of biometric information. The process is based on eleven stages, which include determining a level of protection according to the sensitivity of the data; building an isolated work environment in order to minimize the risk of unauthorized access and of direct attacks on the network; using local applications instead of internet-based ones; and deleting or removing of data after its use is completed.

The Development of the Use of Biometric Applications and Their Legal-Ethical Aspects

The use of biometric applications is developing quite rapidly. An article published in the *New York Times* describes the ease with which facial recognition systems can be established in the public space.[12] According to the article, the notion that it is possible to maintain privacy by moving through the public space is mistaken as the facial recognition systems that most cities operate via the existing camera networks threaten that privacy. The article also shows the ease with which people can be monitored without their knowledge. For example, pictures of people in one of the city parks in New York City were collected over a period of nine hours; the pictures were then run through an Amazon facial recognition service, which recognized 2,750 people.

The integration of facial recognition technology with regular CCTV technology, which is installed on street corners, in stores, and in businesses, has enhanced its use and has created a world in which citizens are intensively and permanently monitored.[13] Britain is a leader in implementing this technology; in recent decades, it has installed millions of street cameras. The development of biometric identification systems now makes it possible to use these cameras to identify people and establish monitoring systems at

11 Raul Sanchez-Reillo, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, and Helga C. Quiros-Sandoval, "How to Implement EU Data Protection Regulation for R&D in Biometrics," *Computer Standards & Interfaces* 61 (January 2019): 89–96.

12 Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine," *New York Times*, April 16, 2019.

13 For more information on the harm to privacy and the mitigation of crime through the use of CCTV cameras, see Andrei Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks and Mitigations," *TrustED '16*, Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (New York: ACM, 2016), pp. 45–54.

negligible costs. In practice, these activities have no legal restrictions, with facial recognition technologies being almost unregulated. Moreover, there is no legal framework regulating the use of cameras that rely upon facial recognition technology, nor is there a supervisory mechanism regarding the installation or use of this technology. As a result, the commensurate use of these tools has not been examined, nor is there any balance between the values of freedom and privacy and those of security.

The British use of CCTV cameras has been subjected to increasing criticism, due to the absence of any public discourse regarding the developing technology and the lack of any legal basis for its use. In this context, several important questions have been raised, such as the infringement of citizens' privacy and the degeneration into the "Big Brother" phenomena.[14] A report published in Britain in 2018 argued that the use of this technology constitutes as an unprecedented threat to the privacy and freedom of citizens and may even undermine their basic rights in public places. The report also stated that Metropolitan Police in Britain only had a 2 percent accuracy in its facial recognition system, while the rate of false warnings has reached 98 percent, meaning an innocent person is often wrongly identified as a monitored person.[15]

The United Nations also joined the criticism and published a report that condemned the use of facial recognition applications during a demonstration in South Wales. The report, written by Joseph Cannataci, who was appointed by the UN Human Rights Organization to examine the issue, claimed that the demonstration was peaceful, and the use of the technology was disproportionate to the level of threat to public safety.[16]

Attempts to address this issue in Israel have led to the establishment of the unit of biometric applications within the Prime Minister's Office and later to the legislation of the Biometric Database Law that was approved in March 2017.[17] One of the goals of the law is to attend to the serious problems concerning identification documents, such as passports and ID cards. The law's objective is to establish regulations that would enable the verification

14 Michael Friedewald and Ronald J. Pohoryles, eds., *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies* (Routledge, 2016).

15 "Face Off – The Lawless Growth of Facial Recognition in UK Policing," *Big Brother Watch*, May 2018.

16 Chris Burt, "UN Privacy Rapporteur Criticizes Accuracy and Proportionality of Wales Police Use of Facial Recognition," *Biometric*, July 3, 2018.

17 For an in-depth discussion of the advantages and disadvantages of the biometric database, see Karine Nahon, "Private Voice: The Politics of the Biometric Database," in *Law, Society, and Culture* 9, part 2 (2019): 217 [in Hebrew].

of identity and identification of Israeli residents, using biometric means and data. This data would be included in identification documents and stored in the central biometric database, making it difficult to counterfeit the documents, produce double documents for the same person, or use a stolen identity. One of the arguments against the law was that the collection of biometric data does not help to mitigate counterfeiting, and that, at the very most, the data would only be useful for the identity verification of the document holder. It was also argued that it would have been sufficient to create documents that would be difficult to counterfeit.[18]

In terms of using cameras in Israel's public space, the Privacy Protection Authority published a document in 2012 that recognized the problematic nature of expanding the use of closed-circuit systems for a variety of needs.[19] These included crime prevention, traffic direction, and the collection of other visual information. The implementation of the "Violence-Free City" program and the initiative to equip police officers with bodycams led to additional developments on the matter. In 2017, given the technological development and the challenges it posed, the Privacy Protection Authority published a revised draft of the directives in order to receive public comments.[20] Its purpose was to clarify the position of the Registrar of Databases regarding the applicability of the Privacy Protection Law in regards to monitoring cameras in public spaces, particularly when the photographs that they record are stored in databases.

The new draft directive addressed a variety of aspects, including the requirements that cameras in the public space are to be used properly and proportionally and after testing less offensive alternatives; before installing the systems, the scope of their public exposure should be examined and that measures should be taken to minimize it; and cameras and the information recorded by them should only be used for the purpose for which they were installed, on condition that the benefit of using the cameras outweighs the harm to privacy that they cause. The directive also states that the installation of cameras in areas where children are present shall require the explicit agreement of the parents. The directive also restricts the placement and

18 Teneh, "The Biometric Database Law."

19 "Guide Number 4.2012 of the Registrar of Databases – Use of Security and Monitoring Cameras and the Collection of Pictures Recorded By Them," Ministry of Justice, Privacy Protection Authority, October 21, 2012.

20 "The Use of Monitoring Cameras and Databases of the Photographs Recorded by Them," Ministry of Justice, Privacy Protection Authority, September 11, 2017.

number of cameras used, and also requires that cameras be placed only in relevant spaces in order to prevent the photographing and storage of data from spaces that are irrelevant to the stated purpose.

In addition, the Privacy Protection Law allows those who were photographed the right to view the photographs or video recordings that concern them. This law and the Privacy Protection Regulations (Information Security), require that the information recorded and stored by the camera systems be secured. The directive from 2017 relates in detail to aspects of biometric identification and their comparison with databases but explicitly lacks mentioning the restrictions of this technology and its effect on citizens' freedom and privacy.

Engineers and algorithm experts rarely rely on social research, nor the other way around. Thus, biometric applications are considered a mysterious "black box" that contain unique information about people and conduct, as well as comparative and matching identity verification processes. The combination of mathematical calculations and biological data apparently provides technical and scientific-objective legitimization to the field of biometric applications. In this context, we must remember that biometric technologies are increasingly involved in automatic decision-making, without human intervention. As a result, the ethical dilemma increases regarding social screening, which could lead to discrimination based on external biological characteristics.

Conclusion

The development of biometric technologies to identify a variety of physical and emotional characteristics has reached a level of maturity and prevalence, which require explicit legal and normative examination of its use. The non-stop rush to develop these technologies in Israel and abroad has neglected these aspects. Israel has a high level of interest in the economic development of biometric applications, and therefore it would be wise for the relevant authorities (the Ministry of Justice, the Privacy Protection Authority) to lead an international process of developing an ethical and legal discussion on the important questions that are raised by the distribution of this technology, particularly biometric technology. In this way, the State of Israel will be able to continue to shape this field in the future.

In the past, biometric technology was restricted to security and enforcement needs. However, the current situation is different. Biometric applications are

increasingly prevalent in both the civilian and commercial sectors. The broad distribution of biometric applications makes it extremely important to address the ethical problems inherent in the development and use of this technology. We are obligated to research and develop knowledge regarding the ethical and legal implications of its use for civilian and commercial organizations, and the question of privacy is a key issue that must be examined. Despite the spread of biometric technology, there is very little empirical research on applicative biometrics and ethics in the civilian and commercial sectors. The development of knowledge therefore requires examining the potential damage that could be caused by biometric monitoring.

The field of biometrics should not be seen only as a technological development; rather, we must deepen our understanding of its legal and ethical implications in order to formulate a sophisticated legal and regulatory framework that can better deal with the different challenges expected in this field in the future.

Cyber, Intelligence, and Security

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for ***Cyber, Intelligence, and Security***, a new peer-reviewed journal, published three times a year in English and Hebrew. The journal is edited by Gabi Siboni, head of the Cyber Security Program and the Military and Strategic Affairs Program at INSS.

Articles may relate to the following issues:

- Global policy and strategy on cyber issues
- Cyberspace regulation
- National cybersecurity resilience
- Critical infrastructure cyber defense
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Cyber incident analysis and lessons learned
- Techniques, tactics, and procedures (TTPs)

Articles submitted for consideration should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to 120 words and up to ten keywords. Articles should be sent to:

Gal Perl Finkel and Gal Sapir
Coordinators, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-50-7478315
galp@inss.org.il | gals@inss.org.il