The Iranian Cyber Threat

The Institutions and Praxis of Iran's Cyber Strategy

Chuck Freilich

Memorandum
230

January 2024

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

THE IRANIAN CYBER THREAT

CHUCK FREILICH

MEMORANDUM 230, JANUARY 2024

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

THE IRANIAN CYBER THREAT

CHUCK FREILICH

This study draws on Charles (Chuck) Freilich, Matthew Cohen, and Gabi Siboni, *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power* (Oxford University Press, 2023). Permission to use this material is acknowledged with gratitude.

INSTITUTE FOR NATIONAL SECURITY STUDIES

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006.

The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda.

INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public.

INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the authors' alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organizations and individuals that support its research.

Institute for National Security Studies
(a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556 Israel

info@inss.org.il
http://www.inss.org.il/

Editor: Ela Greenberg
Managing Editor: Omer Weichselbaum
Cover: Shay Librowski
Graphic design: Michal Semo Kovetz, TAU Graphic Design Studio

Printing: Digiprint Zahav Ltd., Tel Aviv

January 2024
ISBN: 978-965-7840-00-9

CONTENTS

EXECUTIVE SUMMARY

Iran was one of the first states to formulate a coherent national cyber strategy, including the establishment of the necessary state institutions and development of the requisite technological capabilities. Its interest in the cyber realm was first sparked by two primary developments: first, the effective use that the opposition made of the internet to foment and sustain the mass demonstrations following the rigged presidential elections in 2009, and second, the dramatic Stuxnet attack against Iran's nuclear program in 2010, reportedly a joint US–Israeli operation. Ever since, Iran's cyber capabilities have grown steadily, and it is now commonly ranked at the top of the second tier of global cyber powers.

This memorandum presents a comprehensive and up-to-date analysis of Iran's cyber strategy, institutions, and especially praxis. In the absence of a formal statement of Iran's cyber strategy, the study draws on the limited open-source information available, some partial statements by Iranian officials, the broader literature on Iran's national security, and its observable behavior in both the cyber and kinetic realms. To this end, the memorandum presents a detailed account of essentially all the significant cyber operations that Iran has conducted from 2010 through December 2023.

For Iran, the cyber realm poses both major challenges and important advantages. Iran views the cyber realm with concern, as a subversive means of propagating Western values and empowering domestic opposition, and thus posing a threat to the regime. Conversely, it has also proven to be an effective means of shaping public opinion and exerting popular control.

In contrast with Israel's Arab adversaries in the past, Iran does not seek Israel's defeat in the near-term, which it knows is beyond its capabilities. Instead, Iran has adopted a long-term strategy of attrition, designed to sap Israel's military strength, erode its international standing, and undermine its societal resilience, thereby leading to its ultimate collapse. Iran similarly recognizes that it cannot pose a significant conventional threat to the United

States and other actors. Cyber has thus come to constitute an increasingly important component of Iran's strategy of asymmetric conflict. It is also particularly suited to Iran's strategic culture, which emphasizes ambiguity, deniability, and the use of proxies.

Iran conducts cyber operations both separately and in tandem with more traditional means of asymmetric conflict, such as terrorism and guerrilla warfare, to offset the advantages of its more powerful adversaries and to further augment and amplify its use of these asymmetric means. Cyber is a particularly important instrument for Iran, because its leading adversaries are far more dependent on the cyber realm than it is and therefore more vulnerable to attack.

Israel and the United States are Iran's primary adversaries in the cyber realm, and it conducts an ongoing, largely below-the-radar, cyber conflict against them. Iran's cyber operations also attack countries throughout Europe, the Middle East and beyond and has attacked targets of virtually every type. Iran has further adopted a full spectrum and flexible military doctrine; in other words, Iran reserves the right to take both offensive and defensive action, by whatever means it deems appropriate—kinetic or cyber. Iran's cyber operations constitute a complementary capability, not a stand-alone one, designed to buttress its diplomatic, economic, and military capabilities, and to strengthen its deterrence.

Iranian enmity toward the United States, Saudi Arabia, and others is deep; in Israel's case, it is fundamental and likely immutable. Without detracting from the depth of this enmity, much of Iran's cyber activity, like its behavior in other realms, has been reactive. As noted, Iran first built up its cyber capabilities largely in response to the Stuxnet attack; it prepared and conducted a number of attacks before and after the 2015 nuclear deal, using cyber means to respond to the assassination of Qassem Suleimani, a senior leader of the Revolutionary Guard, by the United States in 2020; and reportedly engaged in an ongoing exchange of cyber blows with Israel in recent years.

To assess the effectiveness of Iranian cyber operations to date, they have been divided into four primary categories: disruptive/destructive attacks, espionage operations, information operations, and mixed attacks, which combine some or all of the different types.

Disruptive/destructive attacks: Iran has already demonstrated its ability to cause significant economic disruption and to potentially damage critical national infrastructure in Israel, the United States, Europe, the Middle East, and elsewhere. Attacks against Israel's water supply and air traffic control systems have demonstrated the potential for lethal harm.

However, most of the disruptive/destructive attacks that Iran has conducted to date have been unsophisticated, and the defenses put into place have usually proven sufficient to prevent significant damage. Indeed, Iran has focused most of its attacks on poorly defended targets, thereby indicating that it may believe that important Israeli and Western targets are defended at a level beyond its capabilities. Conversely, the unsophisticated website defacement and disruption attacks, which constitute the bulk of Iranian attacks, have caused considerable inconvenience and have incurred significant financial costs.

Iran's ability to conduct effective and sustained military cyber operations cannot be adequately assessed based on its public record, and Iran has yet to manifest cyber capabilities at a systemic level. It may, however, be withholding its most advanced capabilities for the "appropriate" circumstances. What is clear is that the cyber realm does provide Iran with an important toolkit for conducting under the radar, disruptive, and destructive operations, which are harder to attribute to it.

Espionage operations: The very nature of espionage makes it difficult to draw clear-cut conclusions regarding the effectiveness of Iran's cyber operations in this area. At a minimum, they have been numerous and, in some cases, have yielded considerable classified information. Some attacks have collected intelligence regarding various states' defense industries, weapons

development programs, military capabilities, and more specifically about Israel's nuclear policy and US, Western and Israeli political and strategic thinking. Iran has also conducted cyber espionage operations for purposes of terrorism or in preparation for future destructive or information attacks.

Iran has also made particularly effective use of cyber operations for political surveillance and suppression, targeting dissidents both in Iran and abroad. Control of Iran's cyber realm has helped the regime suppress repeated rounds of demonstrations and ensure its ongoing stability.

Information operations: Cyber information operations are an integral and growing part of the regime's ongoing efforts to disseminate propaganda and gain support for its theocratic beliefs and policies, within Iran, the region, and worldwide. Cyber information operations have provided Iran and its proxies with a variety of platforms for reaching vast numbers of people directly, instantly, and at minimal cost.

Some of these operations have sought to create and exacerbate domestic divisions among Iran's adversaries, affect electoral processes, and undermine societal resilience of the targeted states. Iran's repeated cyberattacks against the US elections in 2020 are a case in point. Some operations have been designed to disrupt relations between foreign states and foment potentially severe crises; in one case, an Iranian website that disseminates false information even sought to create a nuclear crisis between Israel and Pakistan. Still other Iranian cyber information operations have caused financial and reputational damage to a variety of governments and firms around the world.

Cyber information operations have contributed to the ability of Iran and its proxies to create international pressure on Israel to prematurely halt or curtail military operations, before it can achieve its objectives. As such, these operations have adversely affected Israel's ability to conduct effective military operations and maintain its international standing.

Combined attacks: Most of the attacks that Iran has launched since 2020 have combined elements of disruption or destruction, with espionage and

information operations, and have often been disguised as ransomware attacks. Iran has leveraged these attacks to further amplify its offensive cyber capabilities, or compensate for their shortcomings, and their growing use has yielded higher payoffs. The use of ransomware attacks primarily for purposes of information operations, as opposed to financial gain, is unique to Iran's confrontation with Israel.

Iran's cyber praxis, to date, sheds light on three critical quandaries of interest to both cyber practitioners and theorists. First, cyber has proven to be not just an effective means of asymmetric warfare for Iran but also has been conducted with little risk of escalation. As evinced by the numerous cyberattacks detailed throughout this study, Iran's adversaries have rarely chosen to escalate in response to them.

Second, the contention that most Western and Israeli targets of importance may be defended at a level that is beyond Iran's capabilities—if, indeed, true—lends support to those who have maintained that the cyber realm is increasingly becoming defense, rather than offense dominant. Some even believe that Iran's ability to cause significant harm to sophisticated cyber actors has actually diminished. Be that as it may, advanced countries make effective use of some of the same asymmetric military advantages that cyber proffers to Iran, while also wielding their more powerful kinetic capabilities, thus enjoying the advantages of both worlds.

Third, whereas one school of thought contends that the cyber realm strengthens weaker actors, by providing them with additional asymmetric means to counterbalance the superior power of their adversaries, another posits that the sophisticated technological capabilities required for effective cyber operations have actually strengthened the advanced states even more. Iran has certainly made growing use of its cyber capabilities, but Israel, the United States, and other Western countries appear to wield cyber tools with greater socioeconomic and military efficacy. The Iranian experience seems

to lend more weight to the latter viewpoint. The bottom line may be a net overall gain in state power for already advanced actors.

Iran's praxis further demonstrates that it has not adopted a policy of "no first use" in the cyber realm. Conversely, there is no indication that Iran has integrated its cyber and nuclear strategies, that it believes that systemic cyberattacks constitute an escalatory rung below the nuclear level, and that it considers both to be a part of one overall national security strategy.

The number of Iran's cyber operations and their degree of sophistication have grown, and Iran has demonstrated the ability to disrupt, destroy, distort, sabotage, or undermine critical national infrastructure, commercial interests, military capabilities, domestic politics, societal resilience, and international diplomacy. Iran's capabilities will likely continue to improve, both due to its own indigenous capabilities as well as Russian and Chinese assistance. If one assesses the Iranian cyber threat according to the number of important and successful attacks that have taken place to date and their actual consequences, the threat should be considered significant, albeit limited. If, however, one bases the assessment on the potential for future disruption and damage, a growing threat should not be discounted.

Israel's public and private sector cyber strategy was one of the first of its kind, based on decisions adopted between 2011–2015. Much has changed in the interim, however, and a significant update is warranted. The Israel Defense Forces formulated an operational cyber doctrine, but not an overall military cyber strategy, and it has been now eight years since it decided to establish a unified cyber command, which was then suspended, pending further review. No statutory forum today below the cabinet is actively responsible for determining and coordinating military and intelligence cyber priorities and integrating the civil and military cyber strategies. These issues must be rectified if Israel is to maximize its cyber capabilities.

Stand-alone defeat of an adversary, in the traditional sense of preventing it from continuing to wage a conflict or undermining its psychological will

to do so, is not usually achievable in the cyber realm. Instead, Israel should seek "cyber superiority"; that is, the ability to impose a level of disruption or damage on an adversary that it cannot tolerate, or to reduce the severity of attacks against Israel to a level at which Israel can continue to function without significant disruption. To achieve cyber superiority, Israel will have to pursue a cumulative mixed-domain advantage through the gradual, additive application of the full range of capabilities available to it (cyber, kinetic, diplomatic, and economic). It also means cultivating a national pool of highly talented cyber professionals, of which Israel suffers from a considerable shortage. Israel must also formulate a national strategy to counter Iranian cyber information operations. The United States, United Kingdom, and France, among other democracies, have begun addressing this threat, and Israel can learn from their experience.

The Iranian nuclear program remains the greatest military threat to Israel's national security. The "Begin Doctrine," the preventive component of Israel's counter-proliferation strategy, has not been implemented to date against Iran, at least not in the classic sense of an air strike. The numerous kinetic and cyberattacks that Israel has reportedly conducted to sabotage the Iranian program may be a new means of implementing the doctrine. One way or the other, Israel must ensure that it has the kinetic and cyber capabilities to prevent Iran from ever gaining an operational nuclear capability.

Finally, the United States is Israel's primary partner in the cyber realm. Unlike most areas of bilateral military cooperation, Israel's cyber capabilities are primarily homegrown, and it has much to offer the United States, beyond just gain. It is important that Israel seek to expand its cyber cooperation with the United States to the extent possible, but in a manner that minimizes the risks to its freedom of independent action. Cyber dialogue should be formalized in new and expanded memoranda of understanding.

THE IRANIAN CYBER THREAT

The Islamic Republic of Iran must become among the world's most powerful in the area of cyber.

—Ali Khamenei, Supreme Leader of Iran

Beginning in the early 2010s, Iran was one of the first states to formulate a coherent national cyber strategy, including the establishment of the necessary state institutions and development of the requisite technological and operational capabilities. Iran's cyber capabilities have grown steadily over the years, and it is today commonly ranked together with North Korea at the top of the second tier of global cyber powers, behind the United States, Russia, China, the United Kingdom, and Israel. Its cyber capabilities will likely continue to grow and improve, both due to Iran's own homegrown expertise and Russian and Chinese assistance

As with other authoritarian regimes, Iran's attitude toward the cyber realm is somewhat ambivalent. Iran perceives it as a subversive instrument for the promotion of pernicious Western values and domestic opposition and thus as a threat to regime stability and survival. Conversely, it has also proven to be an effective means of disseminating regime propaganda, shaping public opinion, and exerting popular control. Cyber has also become an important component of asymmetric conflict, which Iran conducts, separately, or in tandem, with terrorism and guerrilla warfare, to counter its more powerful adversaries. Indeed, cyber has gained an important place in Iran's overall national security doctrine, and it has become one of the most active offensive actors in the cyber realm today.

Israel and the United States are Iran's primary adversaries in the cyber realm. Ever since 2010, Iran has reportedly engaged in an ongoing exchange of cyber and kinetic blows with Israel and, to a lesser extent, with the United States. It has also conducted a broad array of cyber operations against

countries throughout the Middle East and around the globe. These attacks have demonstrated the importance of the cyber realm for Iran's pursuit of its political and military goals, without having to resort to direct physical aggression, and so far without significant risk of further escalation. Cyber espionage attacks have yielded significant information and have served as a means of terrorist recruitment. Cyber information operations have been used to promote the regime's objectives vis-à-vis other states, as well as to quell domestic opposition.

This study is designed to present a comprehensive and up-to-date analysis of Iran's cyber strategy, institutions, and especially praxis. In so doing, it presents a detailed account of essentially all cyber operations of importance that Iran has conducted in the areas of disruptive and destructive attacks, cyber espionage, and cyber information operations, primarily from 2010 through 2023.

Iran has not published a formal statement of its overall national security strategy nor has it has done so in the cyber realm. The analysis below thus draws on the limited information available, based on some partial official statements and the literature on Iran's national security thinking in general, together with its observable behavior in both the cyber and kinetic realms.

The study has five parts. Part 1 presents a brief overall background on cyber, the cyber threat, and what makes cyber different from other realms of conflict. Readers who are well-versed in these areas may wish to skip directly to Part 2, which addresses Iran's cyber strategy and the institutions and capabilities it has developed to implement it. Part 3 focuses on the primary cyberattacks that Iran has reportedly conducted against actors in the Middle East, the United States, and around the world. Part 4 describes the Iranian cyber threat to Israel. Part 5 assesses the actual impact of Iran's attacks to date and presents a series of policy conclusions.

PART 1:
CYBER—AN OVERVIEW

The Iranian cyber threat is just one facet of the astonishing information revolution that has swept the world in recent decades. In just two days, the international community creates as much data as it did from the beginning of time up until 2003. In 2019 nearly half the homes around the world had a computer. In 2021 there were some 15 billion mobile phones, and more than 26 billion devices were connected to the internet in 2022.[1] Each computer and phone presents a technological and societal advance but also a potential portal for malicious cyber activity. The artificial intelligence (AI) revolution is just beginning.

Personal data of more than 11.5 billion people were stolen in over 9,000 cyberattacks between 2005–2019. The cost of global cybercrime, $8.4 trillion in 2012, is expected to double by 2025.[2] Ransomware attacks, in which victims must pay to regain access to maliciously encrypted systems, are now a primary form of cybercrime and increasingly of politically motivated attacks, as well.

1 Statista, "Share of households with a computer at home worldwide from 2005 to 2019"; "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)"; Josh Howarth, "80+ Amazing IoT Statistics (2023-2030)," *Exploding Topics,* March 16, 2023.

2 Mike Isaac and Sheera Frenkel, "Facebook Security Breach Exposes Accounts of 50 Million Users," *New York Times*, September 28, 2018; Brian Fung, "Uber Reaches $148 Million Settlement over its 2016 Data Breach, which Affected 57 Million Globally," *Washington Post*, September 26, 2018; Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times*, October 3, 2017; Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*, September 7, 2017; The Economist, "The Big Data Breach Suffered by Equifax Has Alarming Implications," September 16, 2017; Statista, "Estimated Cost of Cybercrime Worldwide 2017-2028."

The World Economic Forum has ranked large-scale breaches of cybersecurity as one of the five most serious risks the world faces.[3]

Cyberattacks on the military could have a particularly severe impact. Cyberattacks could disable weapon systems or distort their accuracy, disrupt communications, or affect troop and societal morale. Successful cyberattacks on critical nonmilitary targets could potentially have systemic effects on a state's war-fighting capabilities. Tamir Pardo, the former head of the Mossad, believes that "cyber has become the equivalent of a silent nuclear weapon, the ultimate weapon that can simply take countries apart. Armies were designed to defend national borders, but borders have become meaningless and the battlefield has largely shifted from the military arena to the civilian."[4] Indeed, cyberattacks on civil infrastructure and other critical capabilities could be even more destructive than nuclear attacks. As devastating as nuclear bombs are, their effects are localized, or they could be regional when used in combination with other military means. The lethal effects of cyber weapons may be slower but could be systemic.[5] In effect, cyberattacks can constitute war by other means.

If a cyberattack were to successfully shut down a state's electric grid, for example, or significant parts thereof, it could effectively bring both its economy and military to a standstill and potentially shape the outcome of a conflict. Targeted cyberattacks against water, communication, and transportation systems could cause mass fatalities due to exposure to the cold, dehydration,

3 U.S. Department of Homeland Security, "Cybersecurity Strategy," (2018), 2; Shoshana Solomon, "Israeli Entrepreneur Calls for NATO-Style Cybersecurity," *Times of Israel*, January 31, 2018.

4 Tamir Pardo, interview with author.

5 Joseph S. Nye, *The Future of Power: Its Changing Nature and Use in the Twenty-first Century* (New York: Hachette Book Group, 2011), 212; Jeremy Straub, "Hackers Could Kill More People than a Nuclear Weapon," *LiveScience.com*, August 27, 2019; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (HarperCollins, 2010).

car crashes, and severe traffic mishaps. They could derail trains, shut down traffic lights, or takeover commercial airliners in mid-flight. Cyberattacks could gain control of monitoring systems at nuclear reactors, refineries, or chemical plants, and cause them to shut down—or far worse. Attacks against financial institutions could transfer money between accounts, or eliminate checking, savings and investment balances, leading to economic turmoil. Population and land registries, university databases, agricultural and food distribution chains, automotive, electronics, and pharmaceutical manufacturing systems, as well as emergency response systems could all be disrupted or erased.

The impact of cyber on intelligence collection and operations has been particularly pronounced. In the past, intelligence agencies were forced to devote enormous resources to the development of just a single asset. In 2020 Russian malware infected tens of sensitive targets, including defense ones, in the United States, Canada, Mexico, the United Kingdom, Belgium, Spain, the United Arab Emirates, and Israel.[6] Chinese-affiliated hackers have conducted massive cyberattacks against technology firms and financial institutions in the United States, Japan, and Europe, estimated to be worth trillions of dollars.[7]

The cyber realm has become an important means of maintaining domestic order. The "Great Firewall of China" is used to control and surveil domestic users' access to the internet. China also uses AI, facial recognition software, and cell phones to conduct global surveillance against its political opponents. Russia has centralized domestic internet traffic and created chokepoints designed to seal the country off from the global web. Iran has used cyber surveillance campaigns to spy on dissidents abroad and to suppress domestic

6 David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *New York Times*, January 2, 2021.

7 Zolan Kanno-Youngs and David Sanger, "U.S. Accuses China of Hacking Microsoft," *New York Times*, July 19, 2021; Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age* (New York: Public Affairs, 2017), 8.

opposition.[8] Many designers and manufacturers of software and hardware used for nearly all electronic devices (computers, smartphones, medical devices, cars, missiles, aircraft, and so forth), are located in authoritarian states, raising the potential for these entities to install hidden code in their products for espionage or destructive purposes.

Cyber-information operations, especially against Western electoral processes, have been particularly effective. Chinese cyber operations targeted the presidential campaigns of Barack Obama and John McCain as early as 2008 and Joe Biden's campaign in 2020.[9] The Russian attack on the American presidential elections in 2016 was probably the most prominent cyber operation ever conducted. It may also have been part of a broader strategic effort, conducted in 19 countries, to split the Western camp, weaken NATO, and undermine faith in democratic processes and institutions.[10]

Although cyberattacks have been lethal only in one known case, they have repeatedly caused physical damage, and their capacity to have both a lethal and physical effect is growing. Even if most cyberattacks fail, their sheer numbers mean that a few isolated successes may suffice to undermine public confidence in a specific national or international system. Cyber technology, expertise, and weapons are readily available for purchase on a flourishing online black

8 Segal, *Hacked World Order*, 7–9; U.S. Cyberspace Solarium Commission, *Report* (March 2020), 9-10, 17; Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs* (May/June 2020); Ronen Bergman and Farnaz Fassihi, "Iranian Hackers Found Way Into Encrypted Apps, Researchers Say," *New York Times*, September 18, 2020.

9 David E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Crown, 2018), 18; Tim Starks, "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says," *Politico*, September 10, 2020.

10 Daisuke Wakabayashi and Scott Shane, "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election," *New York Times*, September 27, 2017; Craig Timberg and Tony Romm, "New Report on Russian Disinformation, Prepared for the Senate, Shows Operation's Scale and Sweep," *Washington Post*, December 17, 2018; Julian Barnes, "Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says," *New York Times*, December 21, 2018.

market. Low-level capabilities are inexpensive, and some of the sophisticated ones are capable of penetrating even well-protected governmental and commercial systems. Information stolen both from governments and private entities are available for purchase. One firm even provides a database with the location and internet addresses of hundreds of millions of vulnerable computers around the world, along with target packages.[11]

The dependence of technologically advanced state-actors on cyber in all areas of modern life provides otherwise weaker state and nonstate adversaries with a variety of opportunities to cause harmful effects. Cyberattacks are particularly attractive because they are generally cheaper than kinetic ones, provide an otherwise hard to achieve degree of anonymity and deniability, and do not require territory or national infrastructure. Ongoing attacks against poorly defended commercial and governmental networks could slowly erode a national economy and public morale and force an adversary into unwanted concessions. Most actors such as these do not, however, have the capabilities required to penetrate highly defended targets. Doing so requires the ability to put together multiple professional teams, with different skillsets, to tailor attacks to specific target systems. This is a time-consuming and resource-intensive process.[12]

11 Shane Harris, *@War: The Rise of the Military-Internet Complex* (Eamon Dolan/Mariner, 2014), 103–105; Chris Bing, "Chinese-authored Spyware Found on More than 700 Million Android Phones," *Cyber Scoop*, November 15, 2016; Jeremy Hsu, "U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks," *IEEE Spectrum*, March 26, 2014; Stan Schroeder, "CIA, FBI, NSA: We Don't Recommend Huawei or ZTE Phones," *Mashable*, February 14, 2018; The Economist, "The WannaCry Attack Reveals the Risks of a Computerised World," May 20, 2017; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data* (Santa Monica: Rand Corporation, 2014), ix, 370.

12 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 63 (2010): 66; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 378–379, 396–397; Ivanka Barzashka, "Are Cyber-Weapons Effective?" *The RUSI Journal* 158, no. 2 (2013): 51; Trey Herr, "PrEP: A

Terrorist organizations have used the cyber realm for operational planning, recruitment, training, fundraising, communications, espionage, propaganda, and information operations. Al-Qaeda, the Islamic State, and other terrorist organizations have expressed a clear desire to use cyberattacks as a means of causing direct physical harm.[13]

Why Cyber is Different

A few quick definitions. *Computer Network Attacks* (CNA) disrupt, damage, deny, deface, or even destroy computer systems and networks, (i.e., cyber sabotage) and may be used for deterrent purposes. *Computer Network Exploitation* (CNE) attacks refer to clandestine penetrations of computer and communications systems, designed to collect, alter, or delete information (i.e., cyber espionage) for purposes of intelligence operations and domestic suppression. *Computer Network Influence* (CNI) attacks or cyber information operations manipulate information and communications to influence the perceptions of individuals, groups, or the general public, whether domestic or foreign. They can be used to promote political objectives, disrupt electoral processes, and even undermine a government's legitimacy and effectiveness.

In many ways, cyberattacks are akin to kinetic ones in the physical realm and can be addressed by applying similar approaches and strategies. They do, however, have a number of characteristics that warrant categorizing them as a separate realm of conflict with special treatment.

The first important difference between kinetic and cyberattacks is the speed at which they occur. Cyberattacks happen instantaneously, making

Framework for Malware & Cyber Weapons," *Cyber Security Policy and Research Institute*, George Washington University (March 12, 2014): 8.

13 Lin, "Offensive Cyber Operations," 66; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 378–379, 396–397; Barzashka, "Are Cyber-Weapons Effective?" 51; Herr, "PrEP," 8; Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 123; Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs* 5, no. 3 (2013): 21.

it difficult to prepare defenses, other than automated ones, and denying decision-makers the time needed to formulate a careful response. Conversely, some stages of sophisticated cyberattacks take place at human speed, over months and years, including planning for attacks, intelligence collection, the development of code tailored to specific target systems, and operational preparation.[14]

Even technologically advanced and powerful states do not have a monopoly over the use of force in the cyber realm. Kinetic attacks can only be carried out by a state actor, or terrorist organization; anyone with a computer can launch a cyberattack and cause some degree of harm. Some of the highly advanced computing capabilities that once belonged solely to state actors and major corporations are now readily accessible to all. Weak states or a well-funded nonstate actor can develop outsized military cyber capabilities and possibly achieve unprecedented effects.[15]

Unlike all other weapons, whether conventional or unconventional, cyber weapons have no geographic limitations, essentially neutralizing time and space. They can be launched simultaneously around the globe, against virtually an unlimited number of targets, crossing borders without states even knowing that their networks have been used and their sovereignty violated.[16]

14 Clarke and Knake, *Cyber War*, 31; Ben Buchanan *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford, 2017), 42.

15 Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* 38, no. 2 (2013): 36; Jonathan Silber, "Cyber Vandalism – Not Warfare," *Ynet*, January 26, 2012; Robert Bebber, "Information War and Rethinking Phase 0," *Journal of Information Warfare* 15 no. 2 (2016): 39–52; F. J. Cilluffo and J. R. Clark, "Building a Conceptual Framework for Cyber's Effect on National Security," *Journal of Information Warfare* 15, no. 2 (2016): 7; Segal, *Hacked World Order,* 12.

16 Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy," *Georgetown Journal of International Affairs* 27, no. 3 (2016): 77–84; Clarke and Knake, *Cyber War*, 31; Kello, "The Meaning of the Cyber Revolution," 22.

The impact of all weapons systems, even nuclear ones, are localized; cyberattacks, however, may have systemic or nation-wide consequences. A kinetic attack by a state or nonstate actor can destroy a bank, hospital, radar, or military communications facility. A cyberattack, in contrast, could wipe out an entire financial or health system, impair and disrupt an enemy's early warning and command-and-control systems, and undermine its ability to respond. A nation-wide disruption of an adversary's electric grid, or even just a regional one, could cause social, economic, and military havoc.[17]

Cyberattacks, unlike kinetic ones, rarely cause direct physical damage or loss of life, and espionage can be conducted from afar, without risking lives. Cyber weapons can further be targeted with a degree of precision that is difficult to achieve with kinetic attacks, thereby minimizing collateral damage even against targets that are deeply embedded among civilians. The effects of cyber weapons can intentionally be temporary or reversible. The indirect effects of cyber weapons, however, can cause widespread physical and lethal damage.[18]

Attribution of a kinetic attack by a state or nonstate actor is usually straightforward. Cyberattacks can be more easily disguised and can even cause damage without leaving traces. A target may not even know that it has been attacked. In recent years, however, states and even private firms have

17 Constance Douris, "Cyber Assault on Electric Grid Could Make U.S. Feel Like Post-Hurricane Puerto Rico," *Forbes*, February 6, 2018.

18 Thomas Rid, *Cyber War Will Not Take Place (*London: C. Hurst and Co, 2013), viii; Jan Trobisch, *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm* (School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2014), 4; David E. Sanger, "Why Hackers Aren't Afraid of Us," *New York Times*, June 16, 2018; George Perkovich and Ariel (Eli) Levite, eds. *Understanding Cyber Conflict: 14 Analogies* (George University Press, 2017), 45, 116; Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2018): 382.

greatly improved their technological and forensic intelligence capabilities and consequent ability to attribute attacks.[19]

Essentially all conventional and unconventional weapons can be used against a broad variety of targets. In contrast, sophisticated cyber weaponry (in reality, just computer code) is target-specific and even minor changes to the targeted system can render the weapons useless. Code developed to attack a surface-to-air missile system, for example, may be of no use against another system of this type or an air-to-air system.[20]

Intelligence agencies had to go to great lengths and risks in the past to collect classified and, at times, even unclassified information. With the aid of big data systems, they can now process enormous quantities of unclassified information, each piece of which is unimportant, but which, in combination, can provide critical data. States have long conducted information operations; cyber provides a variety of platforms for reaching vast numbers of people around the world or highly targeted sub-groups, directly, immediately, and at minimal cost.

19 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: INSS, 2012), 32–33; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation, 2009), xiv-xv; Clarke and Knake, *Cyber War,* 45, 51; Silber, "*Cyber Vandalism – Not Warfare*"; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 7.

20 Martin C. Libicki, "Second Acts in Cyberspace," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 137; Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Brookings, 2019), 121.

PART 2:
IRAN'S CYBER STRATEGY, INSTITUTIONS, AND CAPABILITIES

In the early 2010s, two primary factors led Iran to rapidly develop its heretofore limited cyber capabilities. The first was the effective use of the internet by the Iranian opposition to foment and sustain the mass demonstrations following the rigged presidential elections in 2009. The regime ultimately succeeded in suppressing the protests but also gained a healthy appreciation of the threat that the new technology posed to its stature and stability.[21] The second factor was the dramatic Stuxnet attack against Iran's nuclear program in 2010, reportedly a joint US–Israeli cyber sabotage operation. Stuxnet, the first known case of a cyberattack that caused physical damage, demonstrated Iran's extreme vulnerability and led to a severe national shock. In response, Iran rapidly accelerated the development of its then only nascent cyber capabilities.[22]

Experts concur that Iran's cyber capabilities have progressed considerably ever since but they disagree on its actual level of sophistication. Some believe that Iran has not developed a sophisticated cybersecurity ecosystem, suffers from a severe brain drain, and has not achieved the level of professionalism required of an advanced actor. These experts believe that important American, European, and Israeli targets are defended at a level that exceeds Iran's

21 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Carnegie Endowment for International Peace, 2018), 10–11; Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," in *Cyberspace and National Security – Selected Articles*, ed. Gabi Siboni (Tel Aviv: Institute for National Security Studies, 2013), 81–103; Kristina Kausch and Lior Tabansky, "Cybered Conflict in the Middle East," Mediterranean Dialogue Series No. 15 (Konrad Adenauer Stiftung, 2018), 9; Gabi Siboni, Léa Abramski, and Gal Sapir, "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy," *Cyber, Intelligence and Security* 4, no. 1 (2020): 22.

22 Sanger, *The Perfect Weapon,* 46–49; Segal, *Hacked World Order*, 5; Sam Jones, "Cyber Warfare: Iran Opens a New Front," *Financial Times*, April 26, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

capabilities. Some experts believe that Israel's presumed sophisticated cyber defenses have diminished Iran's ability to cause significant damage to Israel and that it remains a third-tier cyber power. If true, this would explain why most Iranian cyberattacks to date have focused on the "low hanging fruit," i.e., poorly defended sites that it attacks with comparatively unsophisticated means.[23]

Others believe that Iran is now at the top of the second tier of global cyber powers, with aspirations to join the frontrunners. The 2022 US Worldwide Threat Assessment stated that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."[24] A former head of Israel's National Cyber Directorate (INCD) maintains that Iran is one of the five most active states in the cyber realm and that it is one of the few states that conducts attacks not just for intelligence and influence purposes but for destructive ones as well.[25]

Proponents of this latter approach maintain that Iran has actually invested heavily in its cyber ecosystem, including schools and universities. By 2016 Iran was reportedly spending over $1 billion annually on its cyber capabilities, compared, for example, with $2 billion by the United Kingdom, one of the world's leading cyber powers. According to Iranian data, Iran's cyber budget jumped twelvefold during between 2013–2021 and a five-year plan discussed in 2020 raised the possibility of a further increase in Iran's digital economy from 6.5 percent of GDP to 10 percent by 2025. As of the late 2010s, some 18

23 Anderson and Sadjadpour, *Iran's Cyber Threat,* 13, 14, 31, 35–36, 52; International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," Research Papers (June 28, 2021); David Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks Against Israel," *Times of Israel*, August 13, 2015.

24 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2022), 1.

25 Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019; Jones, "Cyber Warfare"; Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," (2021), 14.

percent of Iranian university students were reportedly studying computer science, and compulsory military service was used as a means of channeling technologically sophisticated graduates to the state security apparatus, including the Ministry of Intelligence and the Islamic Revolutionary Guard Corps (IRGC).[26]

In 2012 Iran was one of the first states to establish the institutions necessary to implement a national cyber strategy. The Supreme Cyber Space Council was charged with responsibility for planning and implementing an integrated national cyber strategy.[27] The National Cyber Center coordinates Iran's overall cyber activities, gathers and disseminates relevant information and policy directives, and oversees policy implementation. The National Passive Defense Organization is responsible for defending critical national infrastructure and the Cyber Defense Command coordinates the military's (Artesh) cyber operations. The Maher Information Security Center is Iran's computer emergency response team. The Committee for Identifying Unauthorized Sites and FATA (Persian acronym for the Police for the Sphere of the Production and Exchange of Information) serve as cyber police, monitoring internet usage both for purposes of domestic suppression and countering cybercrime.[28] All of the above is in

26 Jones, "Cyber Warfare"; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; International Institute for Strategic Studies, "Cyber Capabilities"; Pierre Pahlavi, "Digital Hezbollah and Political Warfare in Cyberspace," *National Interest*, October 31, 2022; Michael Sulmeyer, *Cyberspace: A Growing Domain for Iranian Disruption* (Washington DC: Center for Strategic and International Studies, 2017), 38.

27 The Council's membership includes the president, speaker of the Parliament, head of the Islamic Republic of Iran Broadcasting, commander of the Armed Forces, commander of the IRGC, minister of defense, minister of information and communications technologies, and others.

28 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities" (January 13, 2020); Jordan A. Brunner, "The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency," *Jurimetrics Journal* 57 no. 3 (2017): 397–431; Ersin Cahmutoğlu, *Iran's Cyber Power* (Ankara: iRAM: Center for Iranian Studies, April 2021), 14–15; Giacomo Spadoni, "IRGC Cyber-Warfare Capabilities," (International Institute for Counterterrorism, 2019).

addition to the long-existing Ministry of Intelligence and Security, responsible for signals intelligence and the Ministry of Information and Communications Technology.

By 2015 the IRGC had reportedly recruited thousands of personnel and had become the dominant cyber actor in Iran. Its Electronic Warfare and Cyber Defense Organization bears primary responsibility for offensive cyber operations. The IRGC also provides operational direction and support for the cyber operations of Iranian proxies, such as Hezbollah.[29]

The Basij, a paramilitary force under the IRG and that is responsible for domestic order, claims to have 1,000 cyber battalions around the country. The Basij outsources cyberattacks to some 50 different hacktivist groups, which operate independently, compete for contracts, and have their own modus operandi and targets. Some of the better known of these groups are the Iranian Cyber Army, Islamic Cyber Resistance Group, and the Ashiyane Digital Security Team. Other examples are the various "Kittens" groups.[30] Flying Kittens gather intelligence on foreign governments and corporations of interest; Magic Kittens target domestic dissidents; Domestic Kittens target dissidents in Iran, the United States, United Kingdom, and more; Charming Kittens use social networking platforms to reach various targets; and Cutting Kittens produce website penetration tools. Basij cyber activities are coordinated by the Basij Cyber Council. Some of these activities are also conducted through three "institutes": Mabna, Rana, and Nasr. Mabna assists Iranian universities

29 Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities"; Brunner, "The (Cyber) New Normal"; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 82, 87–88; Cahmutoğlu, *Iran's Cyber Power*, 14–15.

30 The "Kittens" names, like those of most cyberattacks, have been assigned by the leading global cyber security firms as a means of identification. Most of these groups are also known by various other terms. Charming Kittens, for example, are referred to as APT 35, and other groups have different APT numbers. Static Kittens are also known as MuddyWater.

and scientific and research organizations to gain access to foreign scientific resources.[31]

As in other areas of asymmetric warfare, Iran takes a variety of measures to camouflage its cyber operations and maintain plausible deniability. Malware that has been publicly attributed to Iran is frequently abandoned upon exposure. Membership in the above groups changes continually, leading to a blurring of the lines between them. The IRGC reportedly employs trusted intermediaries to outsource contracts to them, as a means of further masking its tracks, at times employing several contractors for a single operation. The command structure between the IRGC, Basij, and hacktivist groups is fluid, making their activities particularly unpredictable and difficult to assess. This obscurity is further exacerbated by the opaque nature of Iran's decision-making processes and of the control the regime exercises over the security apparatus. At a minimum, the hacktivist groups appear to enjoy tacit approval from Iran's political and security establishments.[32]

Iran's cyber strategy evolved in three primary stages. Stage 1, from 2009–2011, was the wake-up call and initial response to the demonstrations following the 2009 elections and to the Stuxnet attack the year after. Stage 2, from 2012–2018, saw the establishment of the above cyber institutions, the beginning of cyber cooperation with Russia and China, and the transitioning from largely defensive cyber operations to offensive ones—primarily for intelligence purposes. In Stage 3, from 2019 to the present, Iran built a bank

31 Jones, "Cyber Warfare"; Congressional Research Service, "Iranian Offensive Cyber Attack Capabilities"; Anderson and Sadjadpour, *Iran's Cyber Threat,* 17; International Institute for Strategic Studies, "Cyber Capabilities and National Power"; Tom Brewster, "Persian Paranoia: America's Fear of Iranian Cyber Power," *The Guardian*, August 29, 2014; Cahmutoğlu, *Iran's Cyber Power*, 15; Gordon Corera, "Iran 'Hides Spyware in Wallpaper, Restaurant and Games Apps,'" *BBC News*, February 8, 2021.

32 Jones, "Cyber Warfare"; Sulmeyer, *Cyberspace*, 39; Dorothy Denning, "Explainer: How Iran's Military Outsources its Cyberwarfare Forces," *Navy Times*, January 23, 2020; Anderson and Sadjadpour, *Iran's Cyber Threat,* 13.

of infrastructure, defense-related, and other targets around the world, and further expanded its offensive operations. This has been especially true in the areas of information operations and in many cases of combined CNA, CNE, CNI, and ransomware attacks.[33] As will be seen, much of Iran's cyber activities over the years have been of a reactive nature, in response to attacks it attributed to Israel or the United States.

For Iran, the United States has posed the greatest threat to its national security and the only existential threat to the future of the Islamic Republic. Israel is perceived as a severe and particularly active threat, but not an existential one.[34] Other states in the region, especially in the Gulf, are also considered significant threats, although somewhat mitigated by the recent easing of tensions in the spring of 2023. Iran's threat perception and national security strategy are rooted in a nearly all-pervasive sense of weakness and vulnerability, stemming from the failed chapters of Iranian and Persian history, and the recognition that Iran's limited conventional capabilities are no match for those of its primary adversaries.

This deep-seated sense of weakness has led to the resolve not only to deter and defend Iran against its enemies but also to develop effective offensive capabilities with which to promote its interests and to extend its influence abroad. Asymmetric warfare has long comprised a critical component of Iran's national security strategy, designed to offset the advantages of its more powerful adversaries, and cyber has gained an important role therein. Cyber is particularly suited to Iran's strategic culture, which emphasizes ambiguity,

33 Danny Citrinowicz and Jason Brodsky, "Iran's Cyberspace Evolution," *The Dispatch*, April 12, 2022; Boaz Dolev and David Siman-Tov, "Iranian Cyber Influence Operations Against Israel Disguised as Ransomware Attacks," INSS Special Publication, January 27, 2022.

34 Ali Akbar, "Iran's Regional Influence in Light of its Security Concerns," *Middle East Policy* 28 no. 3–4 (2021); Raz Zimmt, "The Israeli Threat—The View From Iran," *Bein HaKtavim*, Dado Center for Interdisciplinary Military Research, forthcoming fall 2023.

deniability, and the use of proxies.[35] To this end, Iran has developed offensive cyber capabilities for purposes of disruption and destruction, espionage, and information operations.

For Iran, the internet and cyber realm, as a whole, are a mixed blessing. They constitute subversive instruments for the propagation of Western values and domestic opposition, and thus pose potential threats to the regime's stability and survival—Iran's foremost objective. At the same time, the internet has also proven to be an effective means of shaping public opinion and of exerting popular control. To this end, and much like its authoritarian models—China, Russia, and North Korea—Iran has created a sizable and effective cyber propaganda machine for disseminating regime policies and Shiite dogma in Iran and abroad.[36]

Iran has succeeded in gaining relatively effective control over its national cyberspace. Following the Chinese model, Iran established a separate national intranet, the National Information Network (NIW). The NIW project began in 2009, when the regime directed domestic companies to begin moving network activities to servers and data centers situated in Iran itself, with the objective of ultimately hosting all Iranian websites there. Iran reportedly also developed an independent email service, operating system, search engine, and other tools for use on the NIW. Although the NIW was formally completed

35 Ariane M. Tabatabai, *Iran's Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran's Influence Operations* (Washington DC: Alliance for Securing Democracy, 2020), 3, 8; Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman and Littlefield, 2017), 41; Kausch and Tabansky, "Cybered Conflict in the Middle East," 8; Micah Loudermilk, "Iran Crisis Moves Into Cyberspace," Policy Watch 3151, *Washington Institute for Near East Policy* (July 9, 2019); Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–82; Anderson and Sadjadpour, Iran's Cyber Threat, 12.

36 Loudermilk, "Iran Crisis"; Sulmeyer, *Cyberspace*, 34–35; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 35.

in 2016, the work is ongoing, and a new cloud infrastructure project and data center were inaugurated in 2020.[37]

The NIW has enabled Iran to more effectively counter foreign cultural and political influences, monitor and identify sources of malicious activity, and reduce its vulnerability both to external cyberattack and domestic opposition. In 2019, at the height of the protests that year—possibly the greatest challenge the regime had faced until then—the NIW shut down internet access throughout Iran for a week. In so doing, the regime prevented the opposition from further mobilizing and was able to hide evidence of the extraordinary measures taken to suppress it, including the reported killing of hundreds and jailing of thousands.[38] The NIW was used once again, to considerable effect, in suppressing the even more severe protests in late 2022, following the killing of a young woman who had refused to cover her hair with a scarf, as required by Iranian law. The internet and cellular access of millions of Iranians was disrupted to frustrate efforts in organizing the protests and to slow their momentum.[39]

Iran has conducted cyber operations designed to promote its primary national objectives, the most important of which, by far, is ensuring the stability and longevity of the Islamic Republic. Additional objectives include preserving Iran's Islamic values and strictures; defense of its territorial integrity and population; promoting socioeconomic growth and the welfare of the Iranian people; propagating Iran's theology and influence throughout the region; achieving regional hegemony; maintaining strong international ties

37 Mahsa Alimardani, "Iran Declares 'Unveiling' of its National Intranet," *Advox*, September 2, 2016; Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 81–103.

38 Lily Hay Newman, "How the Iranian Government Shut Off the Internet," *Wired*, November 17, 2019; Carol Morello and Missy Ryan, "U.S. Says Iranian Forces May Have Killed More Than 1,000 Protestors," *Washington Post*, December 5, 2019.

39 Vivian Lee, "Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage," *New York Times*, September 29, 2022; Benoit Faucon, "Iran Restricts Internet Access as Women's Rights Protests Spread," *Wall Street Journal*, September 22, 2022.

and recognition as an important global power; countering US efforts to contain Iran, especially regarding the nuclear issue; undermining American influence in the region;[40] and countering, weakening, and ultimately destroying Israel.

International Cooperation

Cooperation with foreign actors, chiefly Russia and China, has contributed significantly to Iran's cyber capabilities. In 2015 Russia and Iran concluded their first cyber cooperation agreement, soon followed by a number of more substantive ones. An IRGC cyber defense system, reportedly developed with Russian and possibly Chinese assistance, may have become operational in 2015.[41] In 2016 Russia and Iran agreed to cooperate on "de-monopolizing…unilateral Western domination" of software, a possible indication of Iran's interest in a Russian alternative to Microsoft's Windows and Office software. In 2017 a memorandum of understanding (MoU) on information and communications technology (ICT) cooperation included "internet governance, network security… and international internet connection." At Iran's initiative, a bilateral committee on media cooperation was established in 2018 to combat "Western media terrorism." The committee had been formed as part of another MoU that provided measures designed to promote favorable mutual media coverage, increase coproduction of content, counter Western media narratives, and broaden cooperation on means of targeting foreign audiences.[42]

In 2019–2020 bilateral Russian and Iranian working groups were established to provide Iran with capabilities designed to track citizens through facial recognition and other technologies; promote cooperation in 5G networks and AI; and increase Russian investment in Iranian cyber firms, including possible multilateral investments with Turkey and Azerbaijan. In 2020 an

40 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8; Anderson and Sadjadpour, *Iran's Cyber Threat,* 42.

41 Cyber Threat Brief, *Flash Critic*, November 29, 2015.

42 John Hardie and Annie Fixler, "Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms," *C4ISR*, February 8, 2021.

agreement was reached to counter "increasing information pressure from the West…designed to discredit Russia and Iran."[43]

An even broader bilateral "Information Security Cooperation Pact" was signed in 2021. The pact reportedly covered cybersecurity and technology transfers, including measures to detect cyberattacks; suppression of domestic dissent; diplomatic coordination in the UN and other multilateral forums to promote international cyber norms and law that were in accord with Russian and Iranian interests; and possible provision of advanced Russian surveillance software to Iran for hacking phones and computers of dissidents and adversaries. Without direct evidence, it was thought that Iran may have passed some of the technologies and methodologies acquired from Russia to Hezbollah and other allied militias.[44]

The war in Ukraine has led to a further deepening of strategic cooperation between Iran and Russia, and various reports indicate that this may encompass the cyber area as well. Details are scarce, and it is unclear to what extent this cooperation goes beyond previously existing agreements. One possible indication is the apparent involvement of Russian-affiliated hackers in Iranian cyberattacks against Israel, as part of the annual #OpIsrael and Jerusalem Day campaign (see below).[45]

Chinese firms have also invested heavily in Iran's cyber infrastructure. In 2021 China and Iran concluded a major 25-year strategic cooperation agreement that provides, inter alia, for Chinese assistance in building

43 Hardie and Fixler, "Russia-Iran Cooperation"; Setareh Behroozi, "We are in Iran for Cooperation, not to Sign Memorandums: Russian Official," *Tehran Times*, June 24, 2019.

44 Omree Wechsler, "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East," *Council on Foreign Relations*, March 15, 2021; Morgan Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack Landscape," *IronNet*, September 15, 2021; Hardie and Fixler, "Russia-Iran Cooperation"; Dov Lieber, Benoit Faucon, and Michael Amon, "Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows," *Wall Street Journal*, March 27, 2023.

45 Lieber, Faucon, and Amon, "Russia Supplies Iran"; Avi Davidi, "Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy," *Times of Israel*, April 18, 2023.

Iran's 5G telecommunications infrastructure; access to China's new global positioning system, Beidou; and help in asserting greater Iranian control over its cyberspace, possibly by further strengthening the NIW. China may have also agreed to provide Iran with new cyber capabilities, including those necessary for intelligence collection.[46] Chinese firms have sold camera and AI capabilities to the IRGC and Basij militia. The technology was initially designed for traffic enforcement but was repurposed during the mass demonstrations in late 2022 to enforce Iran's dress code for women and to identify and arrest demonstrators.[47]

46 Farnaz Fassihi and Steven Lee Myers, "Defying U.S., China and Iran Near Trade and Military Partnership," *New York Times*, July 11, 2020; Farnaz Fassihi and Steven Lee Myers, "China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast," *New York Times*, March 27, 2021; Eyal Pinko, "Iranians Developing the Cyber Capabilities of Hezbollah," *Israel Defense*, March 30, 2021; Golnaz Esfandiari, "Iran to Work With China to Create National Internet System," *Radio Free Europe*, *Radio Liberty*, September 4, 2020.

47 Benoit Faucon and Liza Lin, "U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup," *Wall Street Journal*, February 4, 2023; Michael Lee, "Chinese Facial recognition Technology Helping Iran to Identify Women Breaking Strict Dress Code: Report," *Fox News*, January 12, 2023.

PART 3:
MAJOR IRANIAN CYBERATTACKS AROUND THE WORLD

The following section presents the major attacks that Iran has conducted to date against states around the world, while attacks against Israel are presented in the next section.[48]

Disruptive and destructive (CNA) attacks: Some of the earliest attacks attributed to Iran were carried out by the Iranian Cyber Army, a collection of IRGC-affiliated hackers. In 2009, in response to the mass demonstrations that erupted following the presidential elections held that year, the Iranian Cyber Army launched a number of web defacement and DDoS (distributed denial of service) attacks against websites and news outlets affiliated with opposition groups.[49]

In 2012–2013, apparently in response to the Stuxnet operation, an Iranian hacking group launched DDoS attacks against 46 major American financial institutions, including J.P. Morgan, Chase, Wells Fargo, and American Express. Known as the "Abadil" attacks, they were launched on 176 different days and locked customers out of their accounts. The immediate cost was mostly reputational: diminished customer faith in the ability of these institutions specifically and of the American banking system generally to provide secure financial services. The long-term cost to the American financial industry, however, was immense, as these and other financial institutions were forced to spend billions of dollars on highly sophisticated cyber defenses.[50]

In 2012 Iran launched one of the most destructive cyberattacks ever, against Saudi Arabia's national oil company, Aramco. The "Shamoon" attack

48 In a few of the attacks presented in this section, Israel was also a target, but a secondary one.

49 United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022), 5–8.

50 Sanger, *The Perfect Weapon,* 50; Loudermilk, "Iran Crisis"; United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022).

erased data from 30,000 computers and 10,000 servers, nearly obliterating Aramco's corporate information structure and bringing the company to the verge of collapse. Aramco was unable to process automated transactions, employees had to process billions of dollars' worth of oil trades manually, and for a few days the company was even forced to give oil away for free. A similar attack was conducted shortly thereafter against Qatar's natural gas authority, and the Shamoon malware subsequently resurfaced on a number of occasions, erasing data from thousands of computers in Saudi Arabia's Civil Aviation Agency and other organizations in 2016; targeting 15 Saudi government agencies and organizations in 2017; and targeting energy and telecommunications firms, and government agencies in 2018.[51]

In 2013 the Iranians succeeded in gaining control over the floodgates of a dam in New York. Although the attack was subsequently found to have been of limited consequence, it generated deep concern at the time over Iran's ability to damage critical infrastructure and had considerable impact on American thinking. By 2021 US intelligence concluded that Iran had, indeed, developed the ability to conduct effective attacks against critical US infrastructure.[52]

The 2015 nuclear deal (the Joint Comprehensive Plan of Action [JCPOA]) was a focus of particular Iranian cyber activity. Prior to its signing, Iran reportedly prepared attacks against American and European electric grids, water plants, transportation systems, financial institutions, and more.[53] Another attack

51 Sanger, *The Perfect Weapon,* 51–52; Reuters, "Aramco Says Cyberattack Was Aimed at Production," *New York Times*, December 9, 2012; Sulmeyer, *Cyberspace*, 37; Denning, "Explainer"; U.S. Cyberspace Solarium Commission, *Report*, 12; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22.

52 Shimon Prokupecz, Tal Kopan, and Sonia Moghe, "Former Official: Iranians Hacked into New York Dam," *CNN*, December 22, 2015; Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016; Sanger, *The Perfect Weapon,* 47–48; Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," (2021), 14.

53 Siboni and Kronenfeld, "Iran and Cyberspace Warfare," 31; Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace," 22; Brewster, "Persian Paranoia"; Courtney Kube, Carol E.

destroyed data on the networks of a Las Vegas casino, owned by a prominent American Jewish supporter of Israel and outspoken critic of the nuclear deal. The US withdrawal from the deal in 2018 and the ensuing policy of "maximum pressure" against Iran spurred renewed attacks, including ones that erased computer data from over 200 firms dealing with infrastructure, aviation, manufacturing and engineering in the United States, United Kingdom, Germany, Saudi Arabia, India, and elsewhere.[54]

In 2019, in what may have been tests of their ability to cause widespread disruption in the future, suspected Iranian hackers attacked Bahrain's National Security Agency, Ministry of Interior, First Deputy Prime Minister's Office, Electricity and Water Authority, and Aluminum Bahrain, one of the world's biggest smelters. The attacks were reportedly similar to the Shamoon malware attack against Saudi Aramco. In 2020 Dustman malware, which also had similarities to Shamoon, was used to attack Bahrain's national oil company. In this case, only a portion of the firm's computers were temporarily disrupted.[55]

In 2021 Intelligence Group 13, a secretive Iranian cyber unit, planned an attack against critical infrastructure in a number of Western countries, although it is unclear whether it actually intended to conduct the attack at the time, or if it was collecting information for future use. Some of the attacks were designed to cause disruption, including of the automatic gauges of gas

Lee, Dan De Luce, and Ken Dilanian, "Iran Has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials," *NBC News,* July 20, 2018.

54 Anderson and Sadjadpour, *Iran's Cyber Threat,* 40; Tabatabai, *Iran's Authoritarian Playbook,* 17; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *New York Times*, February 18, 2019; Raphael Satter, "AP Exclusive: Iran Hackers Hunt Nuclear Workers, US Targets," *AP*, December 13, 2018.

55 Bradley Hope, Warren P. Strobel, and Dustin Volz, "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran," *Wall Street Journal*, August 7, 2019; Catalin Cimpanu, "New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company," *ZDNet*, January 8, 2020; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks Capabilities*, Special Report (January 2020), 31.

station tanks, which could have caused them to explode; of ballast systems in cargo ships, which could have caused severe damage; and of maritime communications.[56]

In 2021 Iranian hackers attempted to damage computer systems at Boston Children's Hospital, one of the largest pediatric centers in the United States. Had the attack succeeded, it could have affected both ongoing and emergency medical care. The motives for the attack are unclear, but it may have been part of a broader ransomware campaign by hackers affiliated with Charming Kittens (a.k.a. APT34). Separately, hundreds of targets in the United States, United Kingdom, Australia, Canada and Russia were attacked, including power plants and other critical infrastructure sites. The victims appear to have been targets of opportunity, whose computer systems were found to be vulnerable to attack, rather than carefully chosen ones.[57]

Turkey's attempts to normalize relations with the United Arab Emirates, Saudi Arabia, and Israel in 2021 were the apparent motive for spear phishing attacks by Static Kittens (a.k.a. MuddyWater) against high-profile governmental and private Turkish websites. Seemingly legitimate text messages from the Turkish Ministries of Health and the Interior were used to lure targets into downloading malicious links. The attacks may have been a continuation of earlier attacks against Turkish electric firms and universities, conducted from 2015 onward.[58] A number of Iranian ransomware attacks against governmental

56 Yonah Jeremy Bob, "Secret Iran Hacking Plans Against West Revealed – Report," *Jerusalem Post*, July 27, 2021.

57 Dustin Volz, "FBI Chief Blames Iran for Cyberattack on Boston Children's Hospital," *Wall Street Journal*, June 1, 2022; David Braue, "Iranian Hackers Targeting Australian Infrastructure," *ACS*, September 26, 2022; Nassim Khadem, "Australians Urged to be Vigilant Against Continued Cyber Attacks From Iran's Regime," *Australian Broadcasting Company*, January 24, 2023.

58 Menkse Tokyay, "Iran-Linked Hacker Group Targets Turkey's Cyber Network," *Arab News*, February 17, 2022.

and commercial targets in India, including defense, education, and banking systems, took place in 2022.[59]

In 2022 Iran lashed out at Albania, in what may have been the most destructive cyberattacks against a NATO ally since a Russian attack against Estonia 15 years earlier. Albania had become the subject of Iranian ire in 2014, when it agreed, at the request of the United States, to give asylum to the Mujahedin-e Khalq.[60] The hackers, probably Charming Kittens, had already penetrated Albanian government servers a year earlier but now launched a series of wiper attacks that crippled computer systems and deleted information belonging to Albania's intelligence service, police, and border guards. The identities of over 1,000 undercover police informants were also leaked on Telegram, along with the personal banking data of over 30,000 people and the email correspondence of a former Albanian president.

Albania responded by severing diplomatic ties with Iran, the first known case of a cyberattack that led to an outcome of this nature. The Iranian hackers then launched a second wave of attacks, disabling systems and deleting information used for border and customs control, including data on everyone who had entered or left Albania during the previous 17 years. The hackers also leaked the names, email addresses, and phone numbers of 600 Albanian intelligence officers; details of an Albanian intelligence operation; and email correspondence between Albanian government ministries and embassies. Albania considered invoking NATO's Article 5 provision for mutual defense—the first time it would have been invoked over a cyberattack—but ultimately decided not to. As of early 2023, Iranian intrusions into Albanian systems were ongoing.[61]

59 Sana Shakil, "Cyber Attacks by Iran Hackers on Rise," *New Indian Express*, March 6, 2022.

60 A leading Iranian opposition group that advocates overthrow of the regime.

61 Andrew Higgins, "A NATO Minnow Reels From Cyberattacks Linked to Iran," *New York Times*, February 25, 2023; Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," *Politico*, October 5, 2022; United Against Nuclear Iran, "The Iranian Cyber Threat," (September 2022); Mark Pomerleau, "US Cyber Forces Wrap Up

Espionage (CNE) attacks: In 2011 Iranian hackers breached the Dutch digital certificate authority, DigiNotar. The attack enabled them to spy on the encrypted communications of tens of thousands of Iranian citizens.[62]

In 2011, in "Operation Newscaster," using Twitter, Facebook, and other social media sites, Iranian hackers created a series of phony profiles of journalists who had close ties to government officials. They also set up a fake news site, to gather potentially sensitive information regarding the US–Israeli relationship, the nuclear negotiations then underway with Iran, weapons development programs, and defense issues in general. Over 2,000 computers were compromised, mostly in the United States, including hundreds of current and former senior defense, foreign affairs and other officials. Officials from over 10 US and Israeli defense contractors were also targeted. The attack was only discovered in 2014.[63]

In 2013–2014 an Iranian attack gained control over 16,000 computer systems in the United States, United Kingdom, and elsewhere. Another attack breached the networks of airlines, energy, and defense firms and the intranet of the US Navy and Marine Corps.[64]

Between 2013–2017 Iranian hackers successfully penetrated the computer systems of 320 universities, mostly in the United States, but also some elsewhere, including Israel. The accounts of more than 100,000 academics

Deployment to Albania in Response to Iranian Cyberattacks," *DefenseScoop*, March 23, 2023; Fjori Sinoruka, "FBI: Iranian Hackers Accessed Albanian Systems Over Year Ago," *Balkan Insight*, September 22, 2022; United States Institute for Peace, "Albania Cuts Ties With Iran Over Cyberattack," September 12, 2022.

62 Sue Halpern, "Should the U.S. Expect an Iranian Cyberattack?" *New Yorker*, January 6, 2020.

63 Ellen Nakashima, "Iranian Hackers Are Targeting U.S. officials Through Social Networks, Report Says," *Washington Post*, May 29, 2014; Nicole Perlroth, "Cyberespionage Attacks Tied to Hackers in Iran," *New York Times*, May 29, 2014; Stephen Ward, *Insight Partners*, May 28, 2014; Pierluigi Paganini, "Past and Present Iran-Linked Cyber-Espionage Operations," *InfoSec*, February 20, 2017.

64 Segal, *Hacked World Order*, 151.

were attacked, of which approximately 8,000 were successfully breached, and vast quantities of data and intellectual property were stolen.[65] A further attack against 76 universities in the United States, Israel, and other countries—only uncovered in 2018—sought access to unpublished research and intellectual property.[66]

Another attack, which began in 2014 and continued until its exposure in 2019, used social engineering to steal sensitive information from more than 1,800 accounts of American aerospace and satellite technology firms.[67] Between 2014–2020 a major cyber espionage campaign, reportedly capable of breaching the encrypted messaging systems of Telegram and WhatsApp, targeted Iranian dissidents, opposition groups, and religious and ethnic minorities in Iran, the United States, Canada, the European Union, and more.[68]

In 2015 an Iranian-affiliated attack sought to gain permanent access to the information systems used by members of Germany's Bundestag and their staffs. The attempted infiltration affected the Bundestag's operations for several days and yielded a significant amount of information. Other attacks at the time involved data collection about critical German infrastructure, such as power plants and other utilities.[69]

65 U.S. Department of Justice, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guards Corps," Press Release, March 23, 2018.

66 Anthony Cuthbertson, "Iranian Hackers Attack UK Universities to Steal Research Secrets," *The Independent*, August 24, 2018.

67 Rachel Weiner, "Iranian Men Accused of Hacking U.S. Aerospace Companies," *Washington Post*, September 17, 2020.

68 Bergman and Fassihi, "Iranian Hackers Found Way." Particularly prominent targets included the aforementioned Mujahedin-e Khalq (MeK); the Azerbaijan National Resistance organization, which promotes the rights of Iran's large Azeri minority; residents of Iran's restive Sistan and Baluchestan province; Voice of America journalists; and a human rights organization.

69 BBC News, May 13, 2016; Laurens Cerulus, *Politico*, May 22, 2020.

At the height of the negotiations leading to the 2015 nuclear deal, Iranian hackers breached the personal email accounts of the American negotiating team and other US officials, congressional critics of Iran and members of the media. Following the US withdrawal from the agreement in 2018, Iran conducted cyber espionage operations against senior Treasury, State, and Defense Department officials who were involved in the imposition of sanctions. It also stole corporate secrets from 200 infrastructure, aviation, manufacturing, and engineering firms.[70]

In 2016 Iranian hackers conducted a series of attacks against internet service providers and telecommunications firms in the Persian Gulf, which later expanded to government agencies in the United States and 12 European countries. In 2016 the Mabna Institute launched intrusions into the networks of at least 320 universities in 21 countries, including the United States, Australia, Canada, China, Germany, Japan and Israel, and nearly 50 private firms around the world. The attack provided access to confidential research materials.[71]

In 2017 Iranian hackers compromised the login details of 1,000 British members of Parliament and their staffs, over 1,000 Foreign Office officials, and 7,000 police officers. The same hackers targeted the Australian Parliament in 2019, as part of a multi-year cyber espionage campaign, as well as governmental, diplomatic, and military websites in Canada and New Zealand.[72]

In 2018–2019 Iranian-affiliated hackers, posing on LinkedIn as recruiters from Cambridge University and other institutions, sent "job offers" to employees

70 Corey Dickstein, "Military Warns of Iranian Hackers Targeting American Troops With Fake Job Website," *Stars and Stripes*, October 4, 2019; Anderson and Sadjadpour, *Iran's Cyber Threat,* 31, 40; McMillan, "Iranian Hackers Have Hit Hundreds of Companies"; Loudermilk, "Iran Crisis"; Perlroth, "Chinese and Iranian Hackers Renew Their Attacks."

71 Spadoni, "IRGC Cyber-Warfare."

72 Perlroth, "Chinese and Iranian Hackers Renew Their Attacks"; Ewen MacAskill, "Iran to Blame for Cyber-Attack on MPs' Emails – British Intelligence," *The Guardian*, October 13, 2017; Steven Erlanger, "British Parliament Hit by Cyberattack, Affecting Email Access," *New York Times*, June 24, 2017; Ken Dilanian, "Iran-Backed Hackers Hit Both U.K., Australian Parliaments, Says Report," *NBC*, February 28, 2019.

at a variety of Middle Eastern governments, utilities, energy firms and other, designed to lure them into downloading malware. In 2019 the Rana Institute planned and may have carried out an attack on airline and travel booking sites, to gain access to passenger manifests and personal data. Most of the targets were apparently Iranians suspected of anti-regime activities, but some may have been Israeli. Remix Kittens (a.k.a. APT39) also conducted a similar attack.[73]

In 2019 local governments in the United Kingdom, as well as banks and the postal system, were hacked and the identities of thousands of employees stolen, possibly in preparation for more severe attacks on the targets in the future. In another attack, the Elfin group (a.k.a. APT33), which specializes in websites with known vulnerabilities, used spearfishing attacks to gain access to at least 40 governmental and research institutions, as well as commercial and industrial firms in Saudi Arabia, the United States, and elsewhere. The attacks were apparently for purposes of espionage but may have also been in preparation for future destructive ones. In another attack, the Elfin group manipulated or hijacked organizational Domain Name Systems (DNS)[74] to target thousands of employees in Saudi, German, Indian, British, and American oil and gas producers, heavy machinery manufacturers, telecommunications and internet infrastructure providers, and governments.[75]

In 2019 Microsoft blocked 99 websites that had been used by Iranian hackers to conduct multi-year CNE attacks against government agencies, businesses, and individuals in Washington, DC. That year, Iranian hackers also sought to gain access to Pentagon information systems by setting up a website ostensibly designed to serve the needs of military veterans returning to civilian life but which actually downloaded malware onto their computers.

73 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 34–35, 40.

74 A core piece of internet infrastructure, which serves as the web's directory or "phone book" and is critical to its operation.

75 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 36–38, 41.

US Cyber Command and the Department of Homeland Security grew so concerned over Iranian cyberattacks against American governmental and commercial targets, that they issued a special public warning in mid-2019.[76]

In 2020, shortly after the US-targeted killing of Qassem Suleimani, the head of the IRGC's al-Quds Force, Iranian hackers renewed their attempts to penetrate the US power grid; Refined Kittens (a.k.a. APT33) began a password-spraying campaign to target American electricity, oil, and gas firms;[77] and a related group sought access to similar firms by exploiting vulnerabilities in VPN (virtual private networking) software. The attacks may have been designed to lay the ground for future destructive attacks.[78]

In 2020 Charming Kittens conducted a phishing attack designed to gain access to the emails, cloud storage drives, calendars, and contacts of 20 individuals and organizations. The targets included two Human Rights Watch staffers, a woman's rights activist, an advocate for Lebanese refugees, an American anti-Iranian advocacy group, diplomats, academics, and politicians. In the attack against one of the Human Rights Watch staffers, the person received a fake WhatsApp message from someone who had worked at a Lebanese think tank. In the attack against the American anti-Iranian advocacy

76 Dickstein, "Military Warns of Iranian Hackers"; Ellen Nakashima and Spencer Hsu, "Microsoft Says it Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates," *Washington Post*, March 27, 2019; Zak Doffman, "U.S. Military Warns Outlook Users to Update Immediately Over Hack Linked to Iran," *Forbes*, July 3, 2019; U.S. Department of Homeland Security, "CISA Statement on Iranian Cybersecurity Threats," *CISA.gov*, January 3, 2020.

77 In password-spraying attacks, the hackers guess hundreds or thousands of common passwords to gain access to user accounts.

78 Andy Greenberg, "Iranian Hackers Have Been 'Password-Spraying' the US Grid," *Wired*, January 9, 2020; Garance Burke and Jonathan Fahey, "AP Investigation: US Power Grid Vulnerable to Foreign Hacks," *Associated Press,* December 21, 2015; Kube, Lee, De Luce, and Dilanian, "Iran Has Laid Groundwork"; Industrial Cyber, "New Dragos report Reveals Iranian Hackers Targeting U.S Power Grid Amid Tensions Between Two Nations," January 13, 2020.

group, United Against Nuclear Iran, the attackers registered a domain that mimicked the real one.[79]

A number of other cyber espionage attacks took place in 2020: A multi-year intelligence collection operation was uncovered that targeted academics, travel and communications firms, government sites, as well as Iranian dissidents and journalists in over 30 countries in North America, Asia, Africa, and Europe; Iranian-affiliated hackers stole "highly protected and extremely sensitive" communications from defense contractors, think tanks, NGOs, universities, and the Afghani and Saudi governments; and Iranian hackers breached the email accounts of several prominent participants at the Munich Security Conference, the preeminent annual gathering of national security officials, as well as of participants at the G20 summit, presumably to gain insights into their strategic thinking. Chancellor Angela Merkel's email was also hacked.[80]

In 2021 two cyber espionage operations targeted 1,200 Iranian dissidents, members of opposition groups, and Kurds in Iran, the United States, United Kingdom, and elsewhere. The first of the two reportedly used an Iranian blog site, Telegram channels, and text messages to lure some 600 victims from seven different countries, into downloading malicious software. The second had actually begun as early as 2007 and spied on dissidents and others in 12 countries, including Sweden, Denmark, the Netherlands, United States, Iraq, and India.[81]

79 Tzvi Joffre, "Iran-Backed Hackers Targeting Activists, Journalists, Politicians – HRW," *Jerusalem Post*, December 5, 2022.

80 Weiner, "Iranian Men Accused of Hacking"; FBI Boston, "FBI Releases Cybersecurity Advisory on previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies," September 17, 2020; AP, "Microsoft Says Iranian Hackers Targeted Conference Attendees," October 28, 2020; Kate Connolly, "Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel," *Guardian*, May 13, 2020.

81 Corera, "Iran 'Hides Spyware"; Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

In 2021 the same hackers who had posed as recruiters from LinkedIn and Cambridge University three years earlier—seeking to lure targets into downloading malware—now posed as employees of hospitality, medical, airline, and other firms and used Facebook accounts for those purposes. In a clear indication of the scale of the effort required, the hackers conducted ongoing conversations for months at a time with some of their American, British, and European targets.[82] Later that year, Iranian "recruitment" efforts grew particularly dangerous: German, Swedish, and Dutch targets were sent "job offers" with malware attachments, but in this case, the hackers sought sensitive expertise and technology needed to build weapons of mass destruction.[83]

In 2021 Iranian hackers posed as academics from a leading British university to invite experts from the United States and United Kingdom to a conference on Middle Eastern security. Clicks on the "registration link" provided the hackers with access to the victims' computers and with information about their countries' foreign policy, especially regarding the Iranian nuclear issue.[84]

In 2022 Iranian-affiliated hackers successfully penetrated a civilian branch of the US federal government, possibly the Department of Homeland Security, in what may have been intelligence collection in preparation for future destructive attacks. In 2023 Charming Kittens successfully penetrated critical American infrastructure, including multiple seaports and transportation and energy systems. Here, too, the intrusions may have been in preparation for

82 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

83 Tim Stickings, "Berlin Security Service Blames Iran for Cyber Attack on German Companies," *National News*, May 12, 2021; Nakashima and Hsu, "Microsoft Says it Has Found Iranian Hackers."

84 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

future disruptive attacks, possibly in retaliation for US and/or Israeli attacks against Iran.[85]

In 2023 Charming Kittens also impersonated two senior, real-life, experts from Britain's prestigious Royal United Services Institute (RUSI), as a means of establishing contact with nuclear weapons specialists at American think tanks. The phishing attack, which installed malware on the victim's system, was highly targeted, and focused on less than 10 individuals, as part of an effort to gain intelligence on American foreign policy making.[86]

IRGC-affiliated hackers have developed fake mobile apps, similar to Apple Store or Google Play, as a means of disseminating spyware for purposes of surveillance and domestic suppression. The main targets are Iranians, but these apps potentially expose millions of users worldwide to IRGC surveillance. Fake Telegram, Kik, and PlusMessenger apps have been used to exfiltrate data and capture audio and video from 660 largely military targets in the Middle East.[87]

Twenty hacking groups from China, India, North Korea, Pakistan, Russia, and Vietnam, including ransomware operators, spyware vendors, and state-sponsored actors, received command-and-control services from an Iranian affiliated firm in 2023.[88] These services were presumably provided, among other reasons, as a means of gaining intelligence regarding the groups' activities.

Information (CNI) attacks: Iran is increasingly using cyber information operations as a means of achieving its strategic and political objectives.

85 Carly Page, "Iran-Backed Hackers Breached a US Federal Agency that Failed to Patch Year-Old Bug," *Yahoo News*, November 17, 2022; Tim Starks, "An Iranian Hacking Group Went on the Offensive Against US Targets, Microsoft Says," *Washington Post*, April 18, 2023.

86 Derek Johnson, "Iranian Hacking Group Impersonating Nuclear Experts to Gain Intel from Western Think Tanks," *SC Media*, July 6, 2023.

87 Spadoni, "IRGC Cyber-Warfare"; King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks*, 33.

88 Ionut Arghire, "Iran-Run ISP 'Cloudzy' Caught Supporting Nation-State APTs, Cybercrime Hacking Groups," *Securityweek.com*, August 1, 2023.

These operations are conducted in tens of countries and languages, through numerous news websites, social media, YouTube, and more.[89]

Phony websites produce, propagate, and amplify messaging specifically tailored to American, Latin American, African and Middle Eastern audiences. Iran is portrayed on these sites as a responsible and well-meaning member of the international community that supports the oppressed against an aggressive US-led camp, comprised of Israel, the Gulf states, and Europe. Iran's power is said to stem from the righteousness of its faith, values, and policies, in contrast with Western hypocrisy and American reliance on economic coercion and military force. Special attention is devoted to propagating Shiite theology, the Iranian revolution, and regime policies, as well as support for Shiite movements in the region, Nigeria, Thailand, India, and elsewhere.[90]

In 2011 Iran began an information operation on social media, promoting Iranian positions and those US policies that accorded with Iran's interests, including the need for a nuclear deal, as well as anti-Saudi, anti-Israeli, and pro-Palestinian messaging. In 2018, following the murder of Saudi journalist Jamal Khashoggi, Iran created bots, fake news sites, and Twitter profiles to further disrupt US–Saudi ties and generate international pressure on Saudi Arabia.

In 2018 three major Iranian information operations were exposed. The first, "Ayatollah BBC," had already been underway for about six years. Fake Iranian websites were created to masquerade as some of the major Western radio stations that broadcast in Persian, such as BBC and Voice of America, in order to discredit them, while blocking the real sites on Iranian search

89 Clint Watts, "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide," *Microsoft.com,* May 2, 2023; Jack Stubbs and Christopher Bing, "Exclusive: Iran-Based Political Influence Operation – Bigger, Persistent, Global," *Reuters*, August 28, 2018.

90 Tabatabai, *Iran's Authoritarian Playbook*, 3, 6–8, 18; Danny Citrinowicz and Ari Ben-Ami, "The Iranian Information Revolution: How Iran Utilizes Social Media and Internet Platforms to Incite, Recruit and Create Negative Influence Campaigns," *European Eye on Radicalization*, Report 30, July 2022.

engines. Allegedly "independent" news websites, which spread incitement and disinformation about the real ones, were also established. A second operation, which also lasted some six years, consisted of tens or even hundreds of fake news websites and reached a global audience. Each site masqueraded as a local media organization and, in some cases, linked phony headlines to visual and other materials that were unrelated to them. The third operation, launched immediately after the murder of Khashoggi, was directed at a Saudi audience and designed to promote anti-regime sentiment.[91]

In 2019 another information operation was launched, similar in nature to those listed above, but masquerading this time as major print news organizations, including the *Guardian* and the *Independent*. In this case, however, the phony websites included only one fake article at a time, thereby amplifying its impact,[92] compared to the numerous fake articles in the above operations.

In 2019 a large number of fake Twitter accounts in the name of real American citizens, including a number of Republican political candidates, were created to disseminate negative content about Israel and Saudi Arabia. In some cases, the hackers made use of photographs and content taken from the actual accounts of the political candidates, making it difficult to distinguish them from the phony ones. In 2019–2020 millions of people on Facebook, Twitter, Instagram, and YouTube were exposed to a broad-ranging social media campaign critical of the US withdrawal from the nuclear deal, as well as its policies toward Israel, Yemen, and Syria.[93]

91 David Siman-Tov and Ohad Zaidenberg, "Influence Operations: A Combination of Technological Attacks and Content Manipulation," *INSS Special Publication*, March 11, 2021 (Hebrew).

92 Siman-Tov and Zaidenberg, "Influence Operations."

93 King Faisal Center for Research and Islamic Studies, *Iran's Cyberattacks,* 35; Tabatabai, *Iran's Authoritarian Playbook*, 14; Jack Stubbs and Katie Paul, "Facebook Says it Dismantles Disinformation Network Tied to Iran's State Media," Reuters May 5, 2020; Ellen Nakashima, Josh Dawsey, and Matt Viser, "China, Iran Targeting Presidential Campaigns With Hacking

In 2020 the United States seized 92 domains used by the IRGC to conduct information campaigns around the world. Four of the domains posed as ostensibly legitimate news outlets that sought to influence US domestic and foreign policy. The "American Herald Tribune"—a fake Iranian website—actually paid Americans to write articles supportive of Iran's positions, which were then repeatedly referenced, or published in Iranian media, to generate the impression of broad public support for Iran's positions in the United States. In 2020, shortly after the assassination of Qassem Suleimani, the senior leader of the IRGC, Iranian hackers took over the website of a US agency responsible for the distribution of government publications and inserted a picture of a bloody President Trump. Still other information campaigns focused on ethnic and sectarian groups in Iraq, Lebanon, the Persian Gulf, Syria, and Afghanistan.[94]

Iranian information operations have repeatedly sought to promote discord among and between Iran's adversaries. To this end, Iran has used social media in the attempt to further aggravate already existing American racial, socioeconomic, and political tensions, often drawing parallels between them and Iran's own bitter experiences with the United States. In 2020, following the killing of a Black American by a police officer, who pressed his knee against the man's neck until he asphyxiated, President Rouhani claimed that the United States had its knee on Iran's neck, too. Supreme Leader Khamenei and other Iranian leaders repeatedly shared on Twitter their approval of

Attempts, Google Announces," *Washington Post*, June 4, 2020; Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation," *Washington Post*, August 21, 2018; Craig Timberg and Tony Romm, "It's not just the Russians Anymore as Iranians and Others Turn Up Disinformation Efforts Ahead of 2020 Vote," *Washington Post*, July 25, 2019; Jay Greene, Tony Romm, and Ellen Nakashima, "Iranians Tried to Hack U.S. Presidential Campaign in Effort that Targeted Hundreds, Microsoft Says," *Washington Post*, October 4, 2019.

94 Kate O'Flaherty, "DoJ Unveils Iran Disinformation Campaign—Seizes 92 Domains Violating U.S. Sanctions," *Forbes*, October 9, 2020; Halpern, "Should the U.S. Expect an Iranian Cyberattack?"; Tabatabai, *Iran's Authoritarian Playbook*, 18, 20.

the Black Lives Matter movement, asserting that the Iranian and American peoples both have been victims of American oppression and hypocrisy; that the United States has freely criticized other countries' human rights practices, while at the same time American ethnic and religious minorities, women, and the LGBTQ community have to fight for their rights. Iranian leaders have also asserted that Europe's silence regarding US human rights violations, all while criticizing Iran's human rights record, manifests Western hypocrisy.

Iran has also repeatedly attempted to influence the American elections. Social media accounts linked to Iran sought to boost the campaign of candidate Bernie Sanders during the 2016 presidential primary elections, because his opponent, Hillary Clinton, was considered more hawkish toward Iran. During the 2018 midterm elections, Iranian hackers impersonated American voters and political candidates on over 7,000 fake Twitter accounts. During the 2020 elections, Iran intervened even more directly in the attempt to sway the outcome in favor of Joe Biden. Iran feared that the reelection of Donald Trump, the outspoken Iran-hawk who had withdrawn from the nuclear deal and imposed severe sanctions on it, could lead to the American pursuit of a regime change in Tehran. Posing as far-right Trump supporters and using email addresses they had gained from a misconfiguration in a voter registration database, IRGC hackers sent out tens of thousands of intimidating emails to Democratic voters in three swing states. "You are currently registered as a Democrat," they warned "and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on election day, or we will come after you." Further playing on fears that Trump himself had stoked, by claiming that mail-in ballots were subject to fraud, the IRGC hackers also sent out emails with misleading videos designed to undermine voter confidence in the electoral process.[95]

95 Julian E. Barnes and David E. Sanger, "Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn," *New York Times*, October 21, 2020; Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. Government Concludes

Iranian efforts to undermine confidence in the integrity of the electoral process continued even after the elections were over. Pioneer Kittens broke into a system that was used by a municipal government to publish election results; the attack could not have affected the outcome, but it could have enabled incorrect reporting of the results, thereby creating the impression that the electoral system had been tampered with and undermining public confidence in it. More ominously, "Enemies of the People," an Iranian-affiliated website, published death threats against elections officials, state governors, the director of the FBI, and a senior cyber official in the Department of Homeland Security, who had refuted Trump's claims of voter fraud.[96]

Iran may have been behind a website called the "Mapping Project," which shows the locations of Jewish organizations and law enforcement and security agencies in Massachusetts. The website threatened the Jewish community

Iran Was Behind Threatening Emails Sent to Democrats," *Washington Post*, October 22, 2020; Ellen Nakashima, Amy Gardner, and Aaron Davis, "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims," *Washington Post*, December 22, 2020; Tabatabai, *Iran's Authoritarian Playbook,* 11, 15–16; National Intelligence Council, "Foreign Threats to the 2020 Federal Elections," (March 10, 2021), 5–7; Miles Parks, "View From the Ground at Washington DC Protests; Misinformation Spreads Online," *NPR*, June 4, 2020; Brian Bennett, "Exclusive: Iran Steps up Efforts to Sow Discord Inside U.S.," *Time*, June 7, 2021; David E. Sanger and Julian E. Barnes, "United States Indicts Iranian Hackers in Voter Intimidation Effort," *New York Times*, November 18, 2021; Phil Muncaster, "US: Iran Was Behind Proud Boys Email Campaign," *Infosecurity Magazine*, October 22, 2020; Lily Hay Newman, "How Iran Tried to Undermine the 2020 US Presidential Election," *Wired*, November 18, 2021.

96 Joseph Menn, "Iran Gained Access to Election Results Website in 2020, Military Reveals," *Washington Post*, April 24, 2023; Christina A. Cassidy and Frank Bajak, "US Cyberwarriors Thwarted 2020 Iran Election Hacking Attempt," *AP*, April 25, 2023; Nakashima, Gardner, Stanley-Becker, and Timberg, "U.S. Government Concludes Iran Was Behind Threatening Emails"; Nakashima, Gardner, and Davis, "FBI Links Iran to Online Hit"; List Tabatabai, *Iran's Authoritarian Playbook,* 11, 15–16; National Intelligence Council, "Foreign Threats"; Parks, "View From the Ground at Washington DC Protests"; Sanger and Barnes, "United States Indicts Iranian Hackers"; Newman, "How Iran Tried to Undermine the 2020 US Presidential Election."

by warning that every organization "has an address, every network can be disrupted." Over two-thirds of the 505 locations shown are police stations or military bases; offices of the Department of Homeland Security, FBI, Secret Service; and government-linked weapons manufacturers.[97]

Iran has reportedly sought to promote domestic dissension also in the United Kingdom. "Free Scotland," an Iranian-affiliated Facebook page promoting Scottish independence, has more than 20,000 followers. "Britishleft.com," one of a number of phony websites, promotes anti-Saudi and anti-Israel messaging. Another site, supposedly in Birmingham, promotes material taken from a state-owned Iranian media network. The cyber information campaign is part of a broader Iranian effort to affect political thinking in the United Kingdom, including through investment in British religious and cultural institutions.[98]

In 2023 the same Iranian hackers who had conducted the information campaign against the 2020 US elections hacked and leaked the names and contact information of more than 200,000 subscribers of Charlie Hebdo, a French satirical magazine. The attack was apparently in response to a series of cartoons critical of Iran's Supreme Leader that the magazine had published at the height of the anti-regime demonstrations in Iran. The hackers used fake Twitter accounts to further amplify the impact of the leaked information.[99]

97 Benjamin Weinthal, "Iran May Be Behind BDS 'Hit List' Targeting Boston Jews – Report," *Jerusalem Post*, March 5, 2023.

98 Charles Hymas, "Iran Targets UK Political System With Fake Websites," *The Telegraph*, June 6, 2021; Paul Stott, *Iranian Influence Networks in the United Kingdom: Audit and Analysis* (Henry Jackson Society, June 2021).

99 Zeba Siddiqui, "Iran Behind Hack of French Magazine Charlie Hebdo, Microsoft Says," *Reuters*, February 3, 2023.

PART 4:
THE IRANIAN CYBER THREAT TO ISRAEL

Israel is Iran's primary adversary in the cyber realm, as it is in all others. Before turning to the Iranian cyber threat to Israel, it is important that we begin by placing them in the broader strategic context of the overall threat that Iran poses to Israel. For decades, the Supreme Leader Khamenei and other Iranian leaders have repeatedly called for Israel's destruction, referring to it, inter alia, as a "cancerous tumor" that must be removed.[100] In 2014 Khamenei even publicly enunciated a nine-point plan for Israel's destruction.[101]

Iranian enmity toward Israel is fundamental. Iranian enmity does not stem from any given policy, or set of policies, that Israel could change and thereby redeem itself in Iranian eyes. Iran's objection is to Israel's existence. As such, it is very different from the enmity that Iran bears toward the United States and Saudi Arabia, its two other primary adversaries, and, along with Israel, the foci of most of its cyber operations. Were the United States to "mend its ways" and make important changes to its policies toward Iran and the region, the Islamic Republic could live with it in a state of relative peace and cooperation, if not great warmth. Iran's theological, strategic, and economic differences with Saudi Arabia are historic and deeply rooted. Of late, however, they have put these differences aside and have begun at least a temporary rapprochement.

For Israel, Iranian rhetoric is anything but idle talk. To the contrary, Iran has devoted considerable efforts and resources to its anti-Israeli efforts ever since the Islamic Republic was founded. Indeed, Iran's carefully calculated

100 Amir Vahdat and Jon Gambrell, "Iran Leader Says Israel a 'Cancerous Tumor' to be Destroyed," *AP*, May 22, 2020; Tamar Pileggi, "Khamenei: Israel a 'Cancerous Tumor' that 'Must be Eradicated,'" *Times of Israel*, June 4, 2018; CNN Staff, "Iran Leader Urges Destruction of 'Cancerous' Israel," *CNN*, December 15, 2000.

101 Stuart Winer and Marissa Newman, "Iran Supreme Leader Touts 9-Point Plan to Destroy Israel," *Times of Israel,* November 10, 2014.

approach to the achievement of its objectives toward Israel, combined with its comparatively advanced society, size, resources, and distance from it, have made Iran the most sophisticated and dangerous adversary that Israel has ever faced. Certainly, no responsible Israeli official can afford to underestimate the threat.

Iran's nuclear program is the primary threat to Israel's national security today and the only potentially existential one that it faces. The likelihood of Iran ever actually using nuclear weapons against Israel is probably quite low, but the potential consequences are intolerable and Israel must, therefore, treat Iran's nuclear program with the greatest gravity. The more plausible threat, however, stems from the greatly enhanced stature and power that a nuclear capability would enable Iran and its proxies to wage an even more aggressive *sub-nuclear* confrontation against Israel. Moreover, the mere presence of nuclear weapons, even if just in the background, could risk escalating otherwise limited regional confrontations into potentially existential ones.

Furthermore, should Iran acquire nuclear weapons, additional states, such as Turkey, Saudi Arabia, Egypt, and possibly even the UAE, may seek to do so as well. A Middle East with multiple nuclear actors is a nightmare scenario with no known remedies. Unlike the nuclear rivalries between the United States and Russia, the United States and China, or India and Pakistan, Iran explicitly seeks its adversary's destruction. Whereas these nuclear powers went to great lengths to prevent or mitigate crises between them, nuclear actors in the Middle East are likely to have only limited channels of communication and crisis management. Furthermore, Iran and Saudi Arabia are theocracies and even if they are likely "rational actors," the rationality of theocracies may be different from that of other states, if only in some small but critical measure. The prospects of nuclear weapons actually being used in the Middle East, especially among multiple nuclear actors, are far greater in this region than elsewhere and are truly frightening.

In contrast to the possibility of posing a nuclear threat, Iran's conventional military capabilities are limited and unlikely to pose a major threat to Israel for some time. Iran does have a significant and growing arsenal of ballistic and cruise missiles, as well as drones, capable of striking Israel; the primary threat it poses, however, is indirect through Hezbollah, its Lebanese proxy. Iran is thought to have armed Hezbollah with a staggering arsenal of up to 150,000 rockets and mortars and over 2000 drones. In a major confrontation, Hezbollah may fire some rockets at Israel each day, for a period of weeks, causing severe damage to its civilian home front.[102]

Moreover, the rockets that Iran is now supplying to Hezbollah are increasingly precise, presenting a possible game changer from Israel's perspective. Precise rockets would provide Hezbollah with the potential to disrupt both defensive and offensive IDF operations, by targeting anti-rocket systems, mobilization centers and air bases; Israel's command-and-control processes, by targeting targets from the premier's office, down through IDF headquarters and military communications nodes; and its economy and society, by targeting critical national infrastructure and population centers. Although Israel's offensive capabilities and rocket defenses will mitigate the threat, they cannot fully neutralize an arsenal of this size. No other Arab adversary has ever had the capacity to cause disruption of this magnitude to Israel's civil and military rears.[103]

Iran is further engaged in a sustained effort to establish a permanent military presence in Syria and to turn it into a transit point for the supply of weapons to Hezbollah in Lebanon. Israel has been relatively successful so far in slowing this effort, but the buildup continues. Syria's long-term future

102 Jerusalem Post Staff, Tovah Lazaroff, "Israel is Updating Attack Plans Against Iran's Nuclear Sites – Gantz," *Jerusalem Post*, March 15, 2021; Anna Ahronheim, "Hezbollah Has Some 2,000 Unmanned Aerial Vehicles – ALMA," *Jerusalem Post*, December 22, 2021; Yonah Jeremy Bob, "IDF Intel Chief: We'll Keep Peace in North Despite Hezbollah Provocations," *Jerusalem Post*, July 11, 2023.

103 Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford: Oxford Press, 2018), 154–160.

is unclear, but it is likely to remain under significant Iranian influence and to constitute at least a partial forward-operating base for Iran in its fight against Israel. The ramifications for Israel are severe and could even lead to a direct clash with Iran, over and above the indirect military confrontation already underway. Iran's presence in Syria also puts pressure on Israel's relations with Russia, the other primary player in Syria, where it has deployed its most advanced anti-aircraft system and maintains air and naval bases. Iran has also deployed missiles in Iraq and Yemen capable of reaching Israel.

In contrast with Israel's Arab adversaries in the past, Iran and Hezbollah do not seek its defeat in the near-term, which they recognize is beyond their capabilities, and have instead adopted a long-term strategy of "attrition until destruction." In so doing, they make use of a variety of weapons and tactics designed to partially neutralize Israel's technological superiority, prevent it from achieving victory, and demoralize its population. To this end, Hezbollah intentionally deploys its rockets among the civilian population, thereby leading to civilian casualties when Israel tries to destroy them, thus creating international pressure on Israel to end the fighting before it has achieved its military objectives. Hezbollah's own offensive efforts are focused overwhelmingly on Israel's civilian population, through massive and protracted rocket attacks.[104]

Iranian Cyberattacks Against Israel

The following section presents a detailed account of the primary cyberattacks that Iran has conducted against Israel. Some of the attacks were parts of broader campaigns against multiple states, others were cross-cutting (i.e., combined elements of CNA, CNE, and CNI attacks, as well as ransomware). The attacks have been categorized in accordance with their primary intent.

CNA (disruptive and destructive) attacks: In 2012 Iranian-affiliated hackers launched an attack against the computer servers of the Israel Police. External

104 Freilich, *Israeli National Security,* chapter 3.

connections to police servers had to be shuttered and each network isolated, until all intrusions could be removed from the servers. Completing this task required a large team, working 24x7 for a full week.[105]

One of the first Iranian attacks against critical national infrastructure in Israel took place in 2014, during the conflict with Hamas that year. Iranian hackers launched a large-scale attack against the civil communications system and attempted to flood Israel's DNS system.[106] A further Iranian attack against critical national infrastructure occurred sometime in 2015 or 2016. The hackers apparently believed that they had succeeded in conducting a massive attack on Israel's electric grid and possibly even a nuclear facility. In reality, the networks attacked had been decoys, known as "honey-pots," designed to deflect the attacks and expose the adversary's intentions and capabilities. Nevertheless, the attackers' willingness to launch such brazen and potentially escalatory attacks was concerning, and as will be seen, this was not the last Iranian cyberattack against nuclear-related targets in Israel.

In 2019–2020 a series of attacks, apparently by the IRGC, again targeted Israel's critical infrastructure; this time, the water supply and waste management system. Israel's cyber defenses successfully blocked the attacks until April 2020, when an attack launched via US-based servers disrupted—or gained control over—the control systems of six water and sewage treatment stations. The attack was detected rapidly and no harm was caused, but had the attackers succeeded, they would have been able to increase the quantity of chlorine and other chemicals injected into the water supply to potentially lethal levels.[107]

105 Shamah, "Official: Iran, Hamas Conduct Cyber-Attacks"; David Shamah, "How Israel Police Computers Were Hacked: The Inside Story," *Times of Israel*, October 28, 2012.

106 Yaakov Lappin, "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says," *Jerusalem Post*, August 17, 2014; Brewster, "Persian Paranoia."

107 Ahiya Raved, "Cyber Attack Targeted Israel's Water Supply, Internal Report Claims," *Ynet*, April 26, 2020; Ynet staff, "Report: Iran Behind Hack of Israeli Water Authority Sites," *Ynet*, May 7, 2020; Amos Harel, "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line," *Haaretz*, May 20, 2020; Yonah Jeremy

Israel was so concerned that a special meeting was convened of the Ministerial Committee on Defense. The head of the Israel National Cyber Directorate defined the attack as a "turning point in the history of modern cyber warfare" and emphasized that it was the first time that Israel's adversaries had used a cyberattack to cause potentially lethal effects.[108]

Just weeks later, the water system was again targeted; this time it consisted of two, more limited, attacks. One attack targeted agricultural water pumps in the Galilee, while the other targeted infrastructure in the center of Israel. Israel's defenses again proved adequate, and neither attack succeeded. The attacks did demonstrate, however, that the counter-strikes that Israel reportedly conducted in reprisal for the earlier ones, had not achieved their intended deterrent effect.[109]

The attacks against the water system were part of an ongoing series of cyber and kinetic blows and counter-blows, which Iran and Israel reportedly exchanged from 2019 to the present. The Iranian attacks came in waves, with Iran launching 19,000 cyberattacks against Israeli firms in July 2020 and another 33,600 in November.[110] In 2020 the Hackers of Saviors, an Iranian-affiliated hacktivist group that promotes the Palestinian cause, timed the attacks to coincide with Iran's annual al-Quds (Jerusalem) Day. Despite warnings issued

Bob, "Israeli Cyber Czar Warns of More Attacks From Iran," *Jerusalem Post*, May 28, 2020; Yonah Jeremy Bob, "The Coming Cyber Winter is Worse Than all Estimates," *Jerusalem Post*, December 10, 2020; Amitai Ziv, "The Iranians Read the Reports about Israel's Cyber Error, and Succeeded to Embarrass it," *The Marker*, May 31, 2020 (Hebrew); TOI Staff, "Israel Behind Cyberattack that Caused 'Total Disarray' at Iran Port – Report," *Times of Israel*, May 19, 2020; Staff, "Iranian Cyberattacks on Israeli Facilities Thwarted for a Year – Report," *Jerusalem Post*, June 7, 2020; Tal Shahaf, "Israel Unprepared for Iranian Attack on Water Supply, Officials Warn," *Ynet*, February 17, 2021; Prime Minister's Office, National Cyber Directorate, "Annual Report" (2021).

108 Bob, "Israeli Cyber Czar."

109 TOI Staff, "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps," *Times of Israel*, July 17, 2020.

110 Meir Orbach and Golan Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack," *Calcalist*, December 13, 2020.

by the INCD, the hackers successfully exploited a vulnerability in the servers of a leading hosting site and defaced thousands of Israeli websites, replacing them with vicious messages, including calls for Israel's destruction. They also sought to lure targets into downloading malware that would have completely erased their computer data. The targeted websites included municipalities, a pharmaceutical company, food chains, and other private firms, NGOs, and a regional water authority.[111]

In 2020 Static Kittens launched what initially appeared to be a ransomware attack but may have actually been the prelude to a large-scale destructive one, while Agrius, yet another Iranian-affiliated hacking group, did launch a cyber espionage campaign that evolved into destructive wiper attacks.[112] In 2021 Siamese Kittens launched a supply chain attack against Israeli computer and telecommunications firms, by posing as colleagues from similar firms so that they could lure their targets into compromising their computers, possibly in preparation for a wiper or ransomware attack.[113]

2022 saw a major upswing in attacks against Israel. Iranian hackers, possibly Charming Kittens, successfully targeted a wide range of Israeli energy firms, including power plants, oil refineries, and natural gas pipelines, as well as the National Infrastructure Protection Center. The hackers were able to steal sensitive data, including intellectual property and financial information, but they failed to disrupt the firms' ongoing operations. Just weeks later, a similar attack, apparently also by Charming Kittens, was launched against El Al airlines and the Bezeq telecommunications firm. The Tel Aviv Stock

111 Ynet reporters, "Host of Israeli Sites Targeted in Massive Cyber-Attack," *Ynet*, May 21, 2020; Ran Bar-Zik, "Thousands of Websites Defaced in Cyberattack Calling for the 'Destruction of Israel,'" *Haaretz,* May 21, 2020; Government of Israel, Prime Minister's Office, National Cyber Directorate, "Annual Report" (2021).

112 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet*, November 10, 2021.

113 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

Exchange was closed for a few hours after a DDoS attack flooded its servers with traffic, making them unavailable to users.[114]

In 2022 APT34 disabled the air traffic control system at Ben Gurion Airport, disrupting airport operations and even closing it for several hours. No damage was caused to the airport's physical infrastructure, but numerous fights had to be canceled and passengers were stranded in terminals. The hackers also released a malicious file that infected the airport's computers, further disrupting operations. A DDoS attack made it impossible for passengers to book flights or check in to them.[115]

In 2022 the Hackers of Saviors disrupted the operations of a logistics firm at the port of Ashdod. The attack may have been a reprisal for an even more severe attack that Israel reportedly conducted against an Iranian port the previous year, in retaliation for the attacks on Israel's national water system.[116]

In 2022 an IRGC-affiliated attack of unprecedented size and scope led the INCD to declare a state of emergency. The DDoS attack temporarily disrupted the websites of a number of government ministries, as well as the Prime Minister's Office. Another attack by MuddyWater disrupted the websites of the Ministry of Defense and the Prime Minister's Office but failed to achieve its primary goal of disrupting Israel's critical infrastructure.[117]

An attack by Charming Kittens against the electric grid in 2022 did damage a number of power plants and substations, and hundreds of thousands of

114 Tomer Ganon, *Jerusalem Post*, March 8, 2022 and April 12, 2022; David Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

115 Judah Ari Gross, *Times of Israel*, May 24, 2022 and May 25, 2022; *Haaretz*, May 11, 2022.

116 Rafael Kahan, *Calcalist*, February 1, 2022; Genia Wilenski, *The Marker*, January 31, 2022; Nevo Trebelsi, *Globes*, January 31, 2022.

117 Amos Harel, *Haaretz*, March 15, 2022; Yaniv Kubovich and Oded Yaon, *Haaretz*, March 14, 2022; Yaniv Halperin, *Anashim Umachshevim*, March 14, 2022; Yaron Avraham and Nir Dvori, *N12*, March 14, 2022; Raphael Kahan, *Calcalist*, March 14, 2022; Stav Namer et al, *Maariv*, March 14, 2022; Daniel Salame, *Ynet*, March 14, 2022; Report by FireEye Mandiant, January 24, 2022.

people were left without power for hours. The water system and other critical infrastructure sites may also have been attacked.[118]

A broad cyber onslaught in early 2023, deliberately timed to coincide with both the annual Palestinian-affiliated #opIsrael campaign and Iran's al-Quds Day, targeted Israel's universities and an array of governmental and commercial targets. The available information is inconclusive, but the attacks may have been conducted by hackers affiliated with Russian intelligence, acting as a front for Iran, as part of the growing cooperation between the two countries following the war in Ukraine. The attacks temporarily disrupted the websites of most of Israel's banks and telecom companies, postal service, electric and water companies, Home Front Command's rocket warning system, the Israel Ports, Securities and Railways authorities, Prime Minister Netanyahu's Facebook page, Ministry of Health and emergency medical responders, a number of newspapers and TV stations, Check Point—Israel's leading cybersecurity firm—and even the public sites of the Mossad and the Shin Bet.[119]

Each year, the IDF faces hundreds of attempts to break through its defenses and penetrate military computer systems and networks, including operational ones.[120] The IDF Home Front Command's early warning system has been attacked on a number of occasions, including during some of the rounds of

118 Judah Ari Gross, *Times of Israel*, March 8, 2022; Ellen Nakashima and Adam Entous, *Washington Post*, March 9, 2022; David E. Sanger and Ronen Bergman, *New York Times*, March 8, 2022.

119 Raphael Kahan, *Haaretz*, April 5 and April 21, 2023; Daniel Salame and Raphael Kahan, *Haaretz*, April 14, 2023; Jerusalem Post Staff, "Israeli Cyber Security Website Briefly Taken Down in Cyberattack," *Jerusalem Post*, April 4, 2023; Jerusalem Post Staff, "United Hazalah Hit By Tens of Thousands of Cyberattacks Past Two Days," *Jerusalem Post*, April 5, 2023; Jerusalem Post Staff, "Israel Independence Day Cyberattack Takes Down Major News Websites," *Jerusalem Post*, April 26, 2023; Ofir Dor, "'Unsophisticated Iranian Cyberattack' Temporally Downs Israeli Bank Sites, Post Office," *Haaretz*, April 14, 2023; TOI Staff, "Website of Israeli Port Hacked; Sudanese Group Said to Claim Responsibility," *Times of Israel*, April 26, 2023.

120 Itam Elmadon, *N12,* January 21, 2021; Yoav Limor, *Israel Hayom*, February 7, 2019.

conflict with Hamas. Had the attackers succeeded, they would have been able to issue false alerts, or prevent the system from being used when actually needed. An attack in 2020 accessed the IDF's civilian supply chain, including gas and food vendors, whose activities and modus operandi can provide important insights into IDF operations.[121]

CNE (espionage) *attacks:* Iran's CNE attacks have focused on Israeli defense officials, defense industries, and even nuclear scientists. Iranian hackers have also repeatedly sought to gain insight into Israel's strategic thinking through espionage attacks against academics with links to the defense establishment. To this end, they have posed as the academics' colleagues and personal acquaintances and have sought to gain their unvarnished assessments, beyond that which appears in published papers. To make the attacks appear more credible, the hackers studied the targets' ongoing email exchanges and even participated in some.[122] In some cases, the attacks against Israeli targets were part of broader campaigns against multiple states around the world, but due to their significant Israeli component, they have been included here.

In the "Thamar Reservoir" attack, which began sometime between 2011–2014, Iranian hackers reportedly used spear phishing and social engineering techniques to lure former Israeli generals, employees of defense consulting firms, and academics into downloading malware attachments disguised in Word and Excel files. The malware contained "keyloggers," or computer code that enabled the hackers to record every keystroke made by the users, take screenshots, and copy files without their knowledge.[123]

In 2012 a spearfishing campaign targeted 800 business executives in the fields of critical infrastructure and financial services, as well as officials

121 Yoav Limor, *Israel Hayom*, February 7, 2020 and June 11, 2020.

122 Ayala Hasson, "Iranian Hackers Posed as General Yadlin and Gained Information from an Israeli Researcher," (Hebrew), *Channel 13*, November 20, 2020.

123 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

and embassy staffs. Targets clicked on email attachments, or links to news articles, thereby downloading malware and giving the hackers access to their computers. Of the targets, 54 were Israeli.[124] Ever since 2013, Copy Kittens has targeted government agencies, defense and IT firms, academic institutions, and municipal authorities in Israel, as well as in the United States, Saudi Arabia, Turkey, Jordan, and Germany. Each of the attacks began with an infected email attachment, usually carefully chosen to match the target's interests.[125]

Between 2013–2017 Iranian hackers successfully penetrated the computer systems of 320 universities, mostly in the United States but also in Israel and elsewhere. Out of over 100,000 academic accounts targeted, approximately 8,000 were successfully breached and vast quantities of data and intellectual property stolen. A further attack—only uncovered in 2018—against 76 universities in the United States, Israel, and other countries once again sought access to unpublished research and intellectual property.[126]

In 2014 Rocket Kittens targeted Israeli academic institutions, defense contractors, and more, along with other targets in the Middle East. In some cases, the hackers impersonated Israeli engineers, including a particularly well-known one, in order to gain credibility with their targets and increase the likelihood that they would download the malware. Facebook and SMS messages, spear phishing emails, and a variety of other techniques were used. The attacks had easily identifiable errors and were generally unsophisticated but were notable for their persistence. In effect, the hackers simply sought to overwhelm the targets with attacks, until someone eventually erred and downloaded the malware.[127]

124 United Against Nuclear Iran (UANI), "The Iranian Cyber Threat," May 2020.

125 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

126 U.S. Department of Justice, "Nine Iranians Charged"; Cuthbertson, "Iranian Hackers Attack UK."

127 ClearSky Research Team, "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks," Clearsky.com, September 1, 2015.

In 2017 Copy Kittens hackers impersonated the Prime Minister's Office and Israeli news sites, targeting Israeli embassies abroad and foreign embassies in Israel. The hackers made use of cyber infrastructure located largely outside of Iran—in the United States, Russia, and the Netherlands—in an attempt to cover their tracks.[128]

In 2017 Oil Rig masqueraded as a well-known Israeli software firm and sent malicious emails, with fake security certificates, to 120 Israeli government agencies, academic institutions, computer firms, and individuals. The phishing attack exploited vulnerabilities in Microsoft Word to access the targets' address lists, which were then used to further spread the attack.[129] In other attacks by Oil Rig, at least five Israeli IT vendors, several financial institutions, and the postal service were targeted; phony websites masqueraded as a registration page for a conference at the "University of Oxford" and as an employment site; and the website of IsraAir, an Israeli airline, was cloned and used to send targets a malicious Excel file.[130]

In 2018 Charming Kittens reportedly targeted Israeli nuclear scientists in the attempt to gain access to sensitive information. The scientists were sent emails, as part of an ongoing phishing scam with links leading to the fake "British News Agency."[131] According to one report, 11 different IRGC hacking groups were involved in the attacks, almost on a daily basis.[132] That same year, an Iranian-affiliated operation exfiltrated large quantities of information about Israeli and other targets in the Middle East, United States, Europe, and

128 Clearsky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *Clearsky.com,* January 25, 2017.

129 Gwen Ackerman and Alisa Odenheimer, "Israeli Official Says First Wave of Cyber Hack Was Thwarted," *Bloomberg*, April 26, 2017; Anshel Pfeffer, "Why Netanyahu Failed to Mention the Iranian Link to the Cyberattack on Israel," *Haaretz*, April 27, 2017.

130 ClearSky Research Team, "Iranian Threat Agent OilRig."

131 TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists," *Times of Israel*, January 30, 2018.

132 NoCamels, February 1, 2018.

Russia, as well as global aerospace and telecommunications firms. The highly targeted campaign had apparently been underway for at least three years but went undetected by using a previously undiscovered Remote Access Trojan designed to evade antivirus tools and other security measures.[133]

2019 marked a dangerous change in Iranian CNE attacks. Using Facebook and messaging apps, an Iranian-led group operating out of Syria, apparently attempted to recruit people in Israel to conduct terrorist attacks. Iran may have also been behind efforts by Hezbollah and Hamas to use the internet as a means of recruiting Israeli Arabs and Palestinians for terrorism and espionage in Israel.[134]

In 2020 Pay2Key, which is apparently affiliated with Fox Kittens, targeted Israel Aircraft Industries (IAI), one of the biggest firms in Israel and a leading defense contractor. The attack may have penetrated the anti-missile systems, drones, and precision guided munitions manufactured by the firm.[135] In 2021 an attack by Fox Kittens, which took two years and spread through the systems of a large number of Israeli firms, accessing information at various levels of secrecy, was exposed.[136] It is unclear if the attack against IAI was part of this operation.

In 2020 Iranian hackers posed as General Amos Yadlin, a former head of Military Intelligence and the head of the Institute for National Security Studies (INSS) at the time. The attack masqueraded as a text message, ostensibly from Yadlin's WhatsApp account, asking an analyst at another institute to

133 Zev Stub, "Newly-Found Iranian Cyber-Espionage May Pose 'Real Threat' to Israel," *Jerusalem Post,* October 7, 2021.

134 Yoav Zitun, "Shin Bet: Iran Tried to Enlist Israelis, Palestinians for Espionage, Terror," *Ynet*, July 24, 2019.

135 Tal Shahaf, *Ynet*, March 13, 2021; Amitai Ziv, "'Iranian Attacker Impersonating Russians': Inside Recent Attacks on Israel," *Haaretz*, May 5, 2021.

136 Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

comment on a still unpublished INSS study, which the attackers had clearly obtained illicitly.[137]

In 2020–2021 Charming Kittens conducted a phishing campaign against 25 senior American and Israeli experts specializing in genetic, neurological, and oncological research; the motives for the attack are unclear.[138] In 2021 Iranian intelligence masqueraded as attractive women on Instagram, in the attempt to lure Israeli businessmen into meetings abroad, ostensibly for business and/or romantic purposes but in reality to harm or kidnap them.[139] Agrius was back with a password-spraying campaign against the Office 360 accounts of Israeli and American manufacturers of satellites, drones, radar, and more. Twenty firms were successfully compromised. An attack on the databases of the postal service and various private firms in 2022 yielded the personal details of hundreds of thousands of people.[140]

Charming Kittens was behind a series of attacks on Israeli companies in 2022—including defense contractors, technology firms, and financial institutions—designed to steal sensitive data, including intellectual property and financial information.[141] In 2022 Refined Kittens (APT33) tried to breach the computer systems of several Israeli government agencies, including the Ministries of Defense and Foreign Affairs and the National Cyber Directorate, in the attempt to gain sensitive information regarding Israel's military capabilities. The hackers used a variety of methods, including phishing emails, malicious websites, and watering hole attacks. Some damage was caused to a small

137 Hasson, "Iranian Hackers Posed as General Yadlin."

138 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack."

139 Yaniv Kubovich, "Iran Used Instagram to Try and Lure Israelis to Meetings Abroad, Shin Bet and Mossad Say," *Haaretz,* April 12, 2021.

140 Demboski and IronNet Threat Research and Intelligence Teams, "Analysis of the Iranian Cyber Attack"; Yuval Mann, *Ynet,* November 10, 2021.

141 David E. Sanger, *New York Times*, January 24, 2022; Dan Lamothe and Felicia Sonmez, *Washington Post*, January 25, 2022.

number of Ministry of Defense servers, and the hackers were able to gain access to some of the targeted systems. Just weeks later, Refined Kittens conducted another attack against the Ministry of Defense, disrupting some websites.[142]

In 2022 Helix Kittens (a.k.a. APT34, OilRig) used spear phishing emails, social engineering, and other techniques to target Israeli financial institutions, including Bank Hapoalim and Bank Leumi. The attack successfully accessed the targeted systems and stole sensitive data, including customer information and financial records, but did not cause major financial losses. In 2022 APT36 successfully attacked the Ministry of Finance, accessing sensitive information regarding Israel's financial system.[143]

In 2023 Charming Kittens penetrated some 32 Israeli firms in the fields of insurance, medicine, communications, information technology, financial services, and more.[144] The attacks' objective is not known, but they were presumably designed to extract sensitive information and possibly also to cause Israel embarrassment.

That same year, IRGC-affiliated hacking groups, including LionTail, waged one of the more sophisticated espionage campaigns against Israel (along with Saudi Arabia and Jordan), exfiltrating large amounts of data. One of the attacks penetrated privately owned Israeli cameras along the sensitive border with Lebanon.[145]

142 Reuters, February 15, 2022; Eli Lake and Naama Stern, *Reuters*, February 25, 2022; Judah Ari Gross, *Times of Israel*, February 24, 2022; FireEye Mandiant Report, February 2022 Cyberattack on Israeli Government Websites.

143 FireEye Mandiant report, February 14, 2022; Microsoft Threat Intelligence Center, January 24, 2022; Judah Ari Gross, *Times of Israel*, April 25 and April 27, 2022.

144 Raphael Kahan, "Iranian Hackers Break Into Networks of More than 30 Companies in Israel," *Ynet*, November 9, 2023, https://www.ynetnews.com/business/article/rjrs5pn02.

145 Ronen Bergman, Aaron Krolik, and Paul Mozur, "In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities," *New York Times*, October 31, 2023.

CNI attacks: Information operations have been a primary component of Iran's overall cyber operations against Israel to date. As with its information operations against the United States and other countries, Iran's CNI operations against Israel have been designed to further stoke domestic divisions, counter Israel's positions on issues of importance, and strengthen Iran's overall deterrent posture.[146] They have also played a part in Iran's overall efforts to isolate Israel and undermine its fundamental legitimacy as a state.

The Tel Aviv Times, a fake Iranian Hebrew-language website, has tens of thousands of monthly views in Israel. In operation since 2013, the site plagiarizes articles from Israeli news media but with critical changes designed to support Iran's agenda.[147] In 2014 Iranian-affiliated hackers temporarily gained control of the IDF blog and Twitter feed and warned that the Dimona nuclear reactor had been struck by rockets and was about to explode. The IDF quickly restored control over the system relatively quickly, but in the interim many citizens feared the worst.[148]

In 2016 an even more dangerous information operation took place. An Iranian-affiliated website falsely quoted Defense Minister Moshe Yaalon as having stated that if Pakistan sent troops to Syria to fight ISIS, Israel "would destroy them with a nuclear attack." The Pakistani Defense Minister responded with a public warning that "Israel forgets (that) Pakistan is a nuclear state, too." The Israeli Defense Ministry, deeply concerned about a possible escalation with a hostile nuclear power, rapidly clarified that the story was a fabrication.[149]

146 Tabatabai, *Iran's Authoritarian Playbook*, 15–19.

147 TOI Staff, *Times of Israel*, September 6 and November 30, 2018; Stubbs and Bing, "Exclusive: Iran-Based Political Influence Operation."

148 Jerusalem Post Staff, *Jerusalem Post,* July 4, 2014; Siboni and Kronenfeld, "Iran and Cyberspace Warfare"; Kayla Ruble, "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak," *Vice*, July 17, 2014; Mohammad J. Herzallah, "Israeli Fights Wire with Wire," *Newsweek*, July 27, 2009; TOI Staff, "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists."

149 TOI Staff, "Cyber Firm Says Three Iran-Run Sites are Targeting Israelis With Fake News," *Times of Israel,* September 6, 2018; TOI Staff, "Iran Duped Pakistan into Israel Nuke Threat

In 2019 at least 350 fake accounts on Facebook, Twitter, and Telegram were traceable to Countdown 2040, an Iranian website that claims Israel will cease to exist by that year. Masquerading as legitimate news websites, the fake ones disseminated fictitious information to as many as half a million people in Israel each month. Countdown 2040 often rephrases genuine news articles in a manner designed to promote divisive discourse in Israel, on such controversial issues as criticism of Prime Minister Netanyahu, wealth inequality, sexual harassment, poverty, and the judicial system. The campaign was originally designed to inflame tensions in Israel over the Israeli–Palestinian conflict, but in a demonstration of considerable operational agility, following the announcement of early elections, the attackers rapidly shifted gears to an attempt to influence the electoral outcome.[150]

In 2019, in a further attempt to sow discord in Israel, the website of Harvard's Belfer Center carried a report ostensibly based on a talk that the former head of the Mossad, Tamir Pardo, had actually given there. The report quoted him as having said that Russian-born Defense Minister Avigdor Lieberman had been dismissed after having been exposed as a Russian mole. In reality, the Center's website had been cloned, Lieberman had been dismissed for entirely different reasons, and the article was a complete fabrication.[151]

Since 2020, if not earlier, Emennet Pasargad, the same Iranian hacktivist group that attacked the American presidential elections that same year, has repeatedly conducted information operations against Israel. Between 2020–2022 it masqueraded as the Hackers of Savior Pro, a Palestinian hacktivist group, and conducted four cyber campaigns against multiple sectors in Israel, mostly around the annual al-Quds Day. It has also posed as cyber criminals

as Tiny Part of Huge Fakery Campaign," *Times of Israel*, November 30, 2018.

150 Roi Rubenstein, "Report: Iranian Bot Army Trying to Influence Israeli Elections," *Ynet*, January 31, 2019; Ron Shamir and Eli Bahar, "Defending Israel Elections from Cyber Attack – What Should Be Done?" *Israel Democracy Institute*, January 2019, 12 (Hebrew).

151 Scott Shane and Ronen Bergman, "New Report Shows How a Pro-Iran Group Spread Fake News Online," *New York Times*, May 14, 2019.

to conduct a lock-and-leak operation against an Israeli call center. To further amplify the impact of its attacks, Emennet Pasargad makes extensive use of its own websites, Telegram, and fake personas on social media, as well as online hacking and illicit trading forums. In so doing, it seeks to undermine confidence in the targets' networks, cause them reputational damage and financial loss, demonstrate the weakness of Israel's cyber defenses, and promote anti-Israeli messaging.[152]

In 2020 Iranian hackers sought to exacerbate tensions between the Netanyahu government and the public over the government's handling of the COVID-19 crisis. The hackers created official-looking Facebook and Instagram accounts, which were followed by 1,100 and 9,500 Israelis respectively; however, little effort was devoted to making the accounts look authentic.[153]

When the coronavirus crisis diminished, Iranian hackers turned their attention in 2020–2021 to an information campaign designed to further aggravate the political crisis underway in Israel at the time. The identities of American Jewish philanthropists were hacked to collect information about the opposition to Prime Minister Netanyahu. This information was then used on phony Facebook, Twitter, Instagram, and Telegram accounts to disseminate inflammatory and even violent messages designed to taint the opposition. After Netanyahu was forced out of office, a Telegram account urged that he be imprisoned, with a photoshopped image of him behind bars. The similarity between the techniques used by both these hackers and Russian hackers during the attack on the American elections suggests possible collaboration.[154]

152 Anna Ribeiro, "FBI Reveals Iranian Cyber Group Emennet Pasargad Executing Hack-and-Leak Operations Using False-Flag Personas," *Industrial Cyber*, October 21, 2022; Dennis Fisher, "FBI Warns of Attacks From Iranian Threat Group Emennet Pasargad," *Decipher*, October 21, 2022.

153 Facebook, *Threat Report The State of Influence Operations 2017–2020*, May 2021.

154 Sheera Frenkel, "Iranian Disinformation Effort Went Small to Stay Under Big Tech's Radar," *New York Times*, June 30, 2021; Omer Benjakob, "Iranian Accounts, Russian Tactics and Q: Israel Has Become a Disinformation Battlefield," *Haaretz*, April 21, 2021.

Other hackers posed as members of Israel's opposition movement, setting up a false website and seeking to disrupt WhatsApp groups. Facebook removed three accounts of allegedly opposition activists who had posted inflammatory content, including comparisons between Israel's right and Hitler. Another attack on Facebook had 1,800 followers, mostly Israeli citizens who had been made followers by the hackers themselves. In 2021 an Instagram account used bots to tag tens of thousands of Israeli citizens with opposition messages. In 2021 10 Facebook and Twitter accounts, active in more than 90 mostly right-wing groups, posted content critical of the Bennet-Lapid government then in office and called for anti-government demonstrations. In some cases, the hackers sought to make direct contact with political activists close to the prime minister; in others they masqueraded as real political activists.[155]

Iranian hackers sought to interfere in the 2022 elections in Israel. Prior to the elections, some 40 fake Twitter accounts called for a split among the right-wing parties, presumably to weaken them. During the campaign, thousands of Tweets, by profiles ostensibly belonging to left-wing Israelis, called for an electoral boycott. The profiles also posted hate messages against the right wing and Haredim (ultra-Orthodox). Similar messaging took place on election day itself, in an attempt to try and suppress voter turnout.[156] In this case, the hackers' objective may have been to weaken the center-left, leading to a right-wing victory that would harm Israel's international standing and weaken its strategic posture, as, indeed, occurred. The attempts to affect the elections do not appear to have succeeded.[157]

In 2022 another Iranian information campaign again sought to stoke internal divisions in Israel. Hackers on Facebook, Telegram, and other social

155 Frenkel, "Iranian Disinformation Effort"; FakeReporter, "Rolling in the Deep: An Iranian Cross-Platform Influence Operation Summary."

156 Omer Benjakob, "Israel Election: Twitter Purges Foreign Influence Op to Suppress Voting," *Haaretz*, November 1, 2022; FakeReporter, "Rolling in the Deep."

157 Amos Harel, *Haaretz*, June 11, 2023.

media platforms posed as an ultra-Orthodox nationalist group, seeking to encourage anti-government protests by the far right; promote anti-police sentiment among the ultra-Orthodox community; and spread the belief that the inclusion of an Islamist party in the governing coalition meant that Israel was being taken over by Muslims. The attackers went to considerable lengths to make the phony website look genuine, creating a page for a fictitious bakery in an ultra-Orthodox town, using the identity of a real ultra-orthodox man who had died a few years earlier, and more.[158]

In 2022 the Iranian hacker group Moses Staff posted personal pictures and tax documents on the internet, taken from the cell phone belonging to the head of the Mossad's wife, along with some of his medical records. The attack was presumably designed to cause him embarrassment, as he was the senior official charged with Israel's efforts to contain Iran, and to further magnify the attack's public impact. The same hacker group also posted bloody pictures of a terrorist attack in Jerusalem, which it had hacked from unencrypted security cameras, to amplify the attack's impact.[159]

Between June 2022 and May 2023, 24 Iranian-affiliated influence operations took place, compared to just 7 in 2021, mostly by Emennet Pasargad. The operations focused primarily on Israel, as well as Iran's Gulf adversaries and the US. Most of the operations were designed to bolster Palestinian resistance, sow fear among Israelis, and counter normalization of Arab-Israeli ties.[160] The Hunters and No Voice groups used social media, including WhatsApp, Facebook,

158 Tom Bateman, "Iran Accused of Sowing Israel Discontent With Fake Jewish Facebook Group," *BBC*, February 3, 2022.

159 Haim Golditch, *Ynet*, December 24, 2022; Yaniv Kubovich, "Iranian Hackers Post Footage of Jerusalem Bombing, Taken by Large Security Agency," *Haaretz*, November 24, 2022; Michael Horovitz, "Report: Iran Hacked Israeli Cameras a Year Ago; Defense Officials Knew, Didn't Act," *Times of Israel*, December 19, 2022; Itamar Eichner and Yuval Mann, *Ynet*, April 4, 2022.

160 Clint Watts, "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide," *Microsoft.com,* May 2, 2023.

Twitter, Instagram and Telegram, to try to exacerbate the domestic political divide in Israel over the controversial "judicial overhaul" underway at the time. One attack called on the opponents of the proposed reforms to attack both police officers and demonstrators. It also disseminated photographs of police violence, along with the police officers' names, addresses and more, as part of a shaming campaign. In another attack, the hackers used WhatsApp groups of Likud activists to stoke confrontations and encourage violence against anti-judicial reform protesters. Other attacks, to the contrary, sought to promote opposition to pro-government demonstrators.[161]

Combined attacks: Most of the destructive CNA attacks that Iran had conducted up to that time were directed at countries other than Israel, with few exceptions, primarily the failed attack against Israel's water system in 2020. The attacks against Israel were primarily intended for purposes of disruption or espionage, with some information operations. Mid-2020, however, marked a turning point, as most of the attacks shifted to mixed ones, combining disruption, espionage, information operations, and ransomware.

Since mid-2022, in particular, Iran has leveraged cyber information operations to amplify its offensive cyber capabilities and to try to undermine Israel's sense of security. Fundamentally, it has sought to use information operations to foster political and strategic change in accordance with regime objectives.[162] Attacks masquerading as ransomware were employed primarily for purposes of information operations.

In 2020 Sapiens, an Israeli software firm, was forced to pay $250,000 following a Bitcoin ransomware attack, in which Iranian-affiliated hackers threatened to

161 David Siman-Tov, "Attempted Foreign Influence as a Challenge to Israel's National Resilience: Using the Judicial Overhaul Protests to Deepen Internal Rifts," *INSS Insight* No. 1741, June 26, 2023; Bar Peleg, Josh Breiner, and Omer Benjakob, "Iran, Russia or Both, A Foreign Influence Operation to Incite Violence in Israel is Reemerging," *Haaretz,* July 3, 2023.

162 Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations For Greater Effect," May 2, 2023; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

shut down its entire system. Tower Semiconductors paid a ransom of several million dollars, rather than lose a single day of manufacturing time. The attack may have been part of a broader campaign against prominent Israeli firms by Static Kittens that was designed to look like ransomware, but which was actually similar to the highly destructive Shamoon attack against Saudi Aramco. The attack damaged Tower Semiconductor's operating systems, the "holy grail" of cyberattacks, not just its information systems.[163]

That same year, Black Shadow (a possible alias for Agrius, or APT36) conducted a ransomware attack against Shirbit, an insurance firm that caters largely to government employees, including those from sensitive defense agencies, such as the Shin Bet. In this case, the hackers intentionally presented unrealistic deadlines for payment of the ransom and then posted the stolen data on the internet when Shirbit refused to do so. The data posted included the names of those insured; the agencies they worked for; confidential hospital records; contents of WhatsApp conversations; home and email addresses; ID, phone, license plate, and credit-card numbers, and more.[164]

Hacker group Pay2Key used the remote connection systems of employees at seven Israeli firms to conduct a sophisticated ransomware attack. Four of the firms paid the ransom.[165] Pay2Key then targeted Amital, which provides specialized software to 70 percent of the logistics firms in Israel. After penetrating

163 Meir Orbach, *Calcalist*, June 14, 2020 and September 7, 2020; Omer Benjakob, "'Operation Quicksand': Iran-Linked Hackers Target Israel in 'New Cyberwar Phase,'" *Haaretz*, October 19, 2020; Amitai Ziv, "Cash-Strapped Over Coronavirus, Crime Organizations Unload Cyberattacks," *Haaretz*, September 21, 2020.

164 Bernard Brode, "The Shirbit Data Hack Was an Attack on National Security. Now What?" *Times of Israel*, December 18, 2020. According to one source, the attack against was conducted by Hezbollah. See Tal Shahaf, *Ynet*, October 29, 2021.

165 Omer Benjakob, "'It's Not About Money': Destructive Cyberattack Proves Israel Lacks One Key Thing," *Haaretz,* December 9, 2020; Hagay HaCohen, "Check Point Unveils New Iranian Cybercrime, Ransoming Companies' Data," *Jerusalem Post*, November 12, 2020; Meir Orbach, "Israeli Cybersecurity Giant Tracks Ranson Payments From New Cyber Attack to Iranian Nationals," *The Algemeiner*, November 12, 2020.

Amital's computer system, Pay2Key spread to the systems of at least 40 of its clients and infected them with ransomware, thereby placing a significant part of Israel's entire air and maritime cargo traffic at risk. Some of the firms targeted were providers of logistics services to the defense establishment, with potentially sensitive information on weapons imports and exports. At least three were providers of the highly complex logistics services required to distribute the coronavirus vaccine.[166]

In still another attack, Pay2Key stole proprietary information about new semiconductors then under development by Havana Labs, an Israeli subsidiary of Intel, which was critical to Intel's future business plans.[167] Once Pay2Key's CNE attack against Israel Aircraft Industries was exposed in 2021, it switched to a hack and leak attack, releasing the details of approximately 1,000 users. By this point, Pay2Key had attacked over 80 Israeli firms, many for the purpose of ransomware-based information operations. Twitter and Telegram were used to dump stolen information, as was a specially designed website, while a myriad of threats against Israel were posted on social media.[168]

In 2021 Black Shadow launched a ransomware attack against KLS Capital, a car leasing firm. As with the attack against Shirbit, one of the primary motives may have been to demonstrate the weakness of Israel's defenses and to cause it reputational damage. The hackers succeeded in erasing much of the firm's servers and then dumped personal data on the internet on a scale

166 Tal Shahaf, *Ynet*, December 13, 2020 and December 15, 2020; Raphael Kahan, *Calcalist*, December 13, 2020; Orbach and Hazani, "Israel's Supply Chain Targeted in Massive Cyberattack."

167 Tal Shahaf, *Ynet*, December 13, 2020, December 15, 2020, and December 17, 2020; Raphael Kahan, Calcalist, December 13, 2020; Amitai Ziv, "Iran Suspected After Massive Cyberattack on Israeli Firms Revealed," *Haaretz*, December 13, 2020; Amitai Ziv, *Haaretz*, December 31, 2020; Tal Schneider, *Ynet*, December 20, 2020.

168 Tal Schneider, *Ynet*, December 20, 2020; Yonah Jeremy Bob, "Suspected Iranian Cyberattack Targets Israel Aerospace Industries," *Jerusalem Post*, December 20, 2020; Omer Benjakob, "Iranian Hackers Hit Top Israeli Defense Contractor, Data Leaked as Cyberattack Continues," *Haaretz*, December 20, 2020; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

that dwarfed the Shirbit attack, even while the ransom negotiations were still under way. Black Shadow then hacked the website of Israel's leading LGBTQ organization. After initially demanding a ransom, the hackers posted the names of the organization's entire membership, along with explicit pictures, sexual orientations, chats, and health history, including exposure to HIV. Another attack leaked the personal data of 1.5 million patients of a private health network.[169] Networm, likely just a new name for Pay2Key, conducted ransomware attacks against Veritas, another Israeli logistics firm, as well as the Israeli franchise of the H&M clothing chain. Once again, the primary motivation appears to have been to cause embarrassment and reputational damage, as well as to deter Israel.[170]

In 2021, in a significant security breach, Moses Staff succeeded in hacking and dumping the personal details of an entire IDF combat brigade on the internet, including each of the soldiers' names, addresses, phone numbers, training, role, mental health and socioeconomic status. Footage posted on Telegram showed the surroundings of Israel's top secret defense contractor, Rafael.[171]

In 2022 Black Shadow sent spear phishing emails to employees at some of Israel's largest medical centers, demanding a ransom of $10 million in Bitcoin and threatening to release patients' medical records, financial data, and other sensitive information, if its demands were not met. The emails were disguised as legitimate ones from trusted sources but contained malicious attachments.

169 Adir Yanko, Tal Shahaf, and Hadar Gil-Ad, *Ynet*, November 1, 2021; Farnaz Fassihi and Ronen Bergman, "Israel and Iran Broaden Cyberwar to Attack Civilian Targets," *New York Times*, November 27, 2021.

170 Tal Shahaf, *Ynet*, March 13, 2021; Ziv, "Iranian Attacker Impersonating Russians."

171 Tal Shahaf and Nina Fuchs, *Ynet*, October 26, 2021; Tal Shahaf, *Ynet,* October 26, 2021; Michael Horovitz, *Times of Israel*, December 19, 2022.

The hackers also tried to exploit vulnerabilities in the hospitals' computer systems to disrupt their operations, including medical supply systems.[172]

In 2023 Static Kittens launched what initially seemed to be a ransomware attack against the Technion, Israel's equivalent of MIT, encrypting servers and disrupting critical systems. The malware was specifically tailored to the Technion's systems, likely only possible after having first mapped out its entire network. The Technion was forced to disconnect its computers from the internet, limit computer use by faculty and students, and postpone some examinations. The harsh anti-Israel and pro-Palestinian rhetoric the hackers used on Telegram suggests that their primary motivation may have been political, not financial.[173]

Hezbollahs Cyberattacks Against Israel

In the early 1980s Iran established Hezbollah as a proxy organization in Lebanon, with the dual objective of strengthening the Shiite community there and of creating a forward base of operations against Israel. Ever since, Iran has provided Hezbollah with a mammoth rocket arsenal, advanced anti-aircraft, drone and electronic warfare capabilities, and more.[174]

The IRGC, according to one source, has provided Hezbollah with massive technical, material and financial support for its cyber capabilities. Another source believes that Iran has turned Hezbollah into the most sophisticated and influential terrorist organization in the cyber realm today, as a means of gaining deniability, deflecting attention from itself, and strengthening

172 Judah Ari Gross, *Times of Israel*, April 25, 2022 and April 27, 2022; Tomer Ganon, *Jerusalem Post*, April 12 and April 26, 2022.

173 TOI Staff, "Israel Publicly Blames Iran for Cyberattack on Major University Last Month," *Times of Israel*, March 7, 2023; Roei Hahn and Yuval Mann, "Leading Israeli Research Institute Falls Prey to Cyberattack," *Ynet*, December 2, 2023; Israel National Cyber Directorate, "Iranian Government Sponsored Threat Actor Muddy Water Conducts Cyber Attack Against Israel," March 9, 2023.

174 Yonah Jeremy Bob, "Iran Hackers Closer to Penetrating Israel US Drones Cyberdefense CEO," *Jerusalem Post*, November 21, 2022.

Iran's hold on Lebanon.[175] Despite these assessments, the publicly available information on Hezbollah's cyber capabilities is limited and thus difficult to make an informed judgment. Whether this paucity of information reflects the limits of Hezbollah's cyber capabilities, or the efficacy of its operational secrecy, is unknown. It is reasonable to presume that the latter is at least partly the case.

CNA attacks: A sophisticated multi-year Hezbollah attack against the IDF was uncovered in 2015. The attack sought to circumvent the IDF computers' built-in protections, by targeting the firms that supply it with software.[176]

CNE attacks: In 2010, in what may have served as a model for a number of later attacks by Hamas, Hezbollah hackers created a phony Facebook profile of an attractive young woman, who sent "friendship" requests to IDF soldiers. Approximately 200 responded, along with information about the names of other personnel and, in some cases, detailed descriptions of bases and even codes. It took almost a year before the attack was discovered.[177]

In 2012 the Hezbollah Cyber Army launched Volatile Cedar, an espionage campaign that used custom-built malware to target military suppliers, telecommunications firms, media outlets, and universities in Israel, the United States, United Kingdom, a number of Middle Eastern states, and more. In 2015 Hezbollah hackers participated in the above-mentioned "Thamar Reservoir" attack, which employed social engineering techniques against a variety of Israeli targets, including retired generals and defense consulting firms.[178]

175 Pahlavi, "Digital Hezbollah"; Benjamin R. Young, "How Iran Built Hezbollah into a Top Cyber Power," *National Interest*, April 11, 2022.

176 Oded Yaron, "Has Hezbollah's Cyber Spy Ring Been Exposed?" *Haaretz*, April 8, 2015.

177 Rid, *Cyber War Will Not Take Place*, 103.

178 Jeff Moskowitz, "Cyberattack Tied to Hezbollah Ups The Ante for Israel's Digital Defenses," *Christian Science Monitor*, June 1, 2015; Pahlavi, "Digital Hezbollah"; Lucas Ropek, "Hezbollah-Linked Cyber Unit Has Been Hacking Into Internet Companies for Years," *Gizmodo*, January 29, 2021; TOI Staff, "Iran Spying on Israel, Saudi Arabia with Major Cyberattacks," *Times of Israel*, June 14, 2015.

In 2016 Hezbollah hacked closed-circuit security camera systems in government buildings in Haifa and Tel Aviv, including the IDF's General Staff Headquarters and the Ministry of Defense, and released the images on social media platforms. Although not a particularly sensitive breach, it provided Hezbollah with a propaganda coup and did enable it to monitor those entering the buildings.[179]

A more serious campaign that same year employed social media to recruit Israeli Arabs and West Bank Palestinians for intelligence and terrorist purposes. One of those reportedly involved was the son of Hezbollah leader, Hassan Nasrallah. In one attack, an online recruit was enlisted to kidnap Israelis and transfer the hostages to Lebanon; in another, to conduct a suicide bombing. The attacks, which were thwarted by Israel, typically began with contact on Facebook and then switched to encrypted communications platforms.[180]

In 2021 Hezbollah's Cedars of Lebanon used vulnerabilities in Oracle and Atlassian servers to attack approximately 250 telecommunications, web hosting, and infrastructure firms in Israel, the United States, United Kingdom, Egypt, Jordan, Saudi Arabia, the UAE, Palestinian Authority, and elsewhere. Once the attacks penetrated the targeted systems, most proceeded manually, but some provided the attackers with remote control. The code used was similar to that employed by various Iranian hacker groups, indicating close cooperation. The Cedars of Lebanon were first discovered in 2015 but were able to continue operating under the radar by taking measures designed to avoid leaving a unique footprint.[181]

179 Ryan De Souza, "Israeli Security Camera Systems Targeted by Pro-Hezbollah Hackers," *Hackread*, February 21, 2016; Sagi Cohen, *Ynet*, June 15, 2015.

180 Michael Shkolnik and Alexander Corbeil, "Hezbollah's 'Virtual Entrepreneurs': How Hezbollah is Using the Internet to Incite Violence in Israel," *CTC Sentinel* 12, no. 9 October 2019.

181 Amichai Stein, *Kan Hadashot*, January 28, 2021; Tal Shahaf, *Ynet*, January 28, 2021; Raphael Kahan, *Calcalist*, January 28, 2021; Yossi Hatoni, "Hezbollah Cyberattacked Hundreds of Companies, Also in Israel," *People and Computers*, January 28, 2021(Hebrew).

In 2022 a joint Iranian and Hezbollah cyberattack reportedly targeted UNIFIL, the UN peacekeeping force stationed in Lebanon. The attack was designed to steal materials regarding UNIFIL's activities and deployment.[182]

CNI attacks: The Hezbollah Cyber Army reportedly conducts training camps in Lebanon, designed to create "electronic armies" around the region. Thousands of Iranian-affiliated social media activists from Iraq, Saudi Arabia, Bahrain, Syria, and elsewhere have undergone intensive training on propaganda and disinformation campaigns, including digital manipulation of photographs, management of fake social media accounts, video production, and means of circumventing the censorship techniques employed by social media firms.[183]

As with Iran, information operations have long been a critical part of Hezbollah's multi-decade strategy of asymmetric warfare. To this end, Hezbollah has used social media such as Facebook, Twitter, YouTube, Telegram, WhatsApp, and Signal to reach a Muslim and international audience on a previously unprecedented scale and to brand itself as the leader of the anti-Israel "Resistance Front." It has further used these media to amplify information campaigns designed to adversely affect Israel's international standing and to promote international pressure on it to cease military operations before it is able to achieve its objectives.[184] Hezbollah's leader, Hassan Nasrallah, reportedly believes that cyber information campaigns are even more effective for Hezbollah's purposes than military operations.

182 Amos Harel, Yaniv Kubovich, and Reuters, "Israel Accuses Iran, Hezbollah of Hacking UN Force in Lebanon," *Haaretz,* June 29, 2022; Emanuel Fabian, "Gantz Says Iran and Hezbollah Tried to Hack UN Peace Force, Steal Deployment Data," *Times of Israel*, June 29, 2022.

183 Wil Crisp and Suadad al-Salhy, "Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East," *The Telegraph*, August 2, 2020; Pahlavi, "Digital Hezbollah."

184 Anshel Pfeffer, "Israel Suffered Massive Cyber Attack During Gaza Offensive," *Haaretz*, June 15, 2009, Oded Yaron, "Palestinians Behind Cyber Attacks on Israeli Army and Government Targets," *Haaretz*, February 16, 2015; Paul J. Springer, *Encyclopedia of Cyberwarfare* (ABC-Clio, 2017), 220–221.

Hezbollah has long blended asymmetric warfare and information campaigns. Its TV station, al-Manar, has a Twitter feed followed by half a million people. It also runs more than 20 websites in seven languages (Arabic, Azeri, English, French, Hebrew, Persian, and Spanish), as well as the above-noted social media network. Social media platforms are also used as a means of recruiting fighters and hackers from around the Arab and international worlds.[185] Hezbollah has reportedly joined Iranian information campaigns designed to sow discord in Western countries. It is also suspected of conducting information operations targeting populations of Lebanese descent in several West African countries.[186]

Palestinian Islamic Jihad (PIJ)'s Cyberattacks Against Israel

An Iranian proxy based in Gaza, PIJ successfully hacked the (unencrypted) communications of IDF drones operating over Gaza for two full years, between 2012–2014. The attack enabled it to monitor the intelligence gathered by the drones in real-time and facilitated both its efforts and those of Hamas in hiding their rockets. Live feeds from Israeli road cameras were also hacked in order to ascertain where rockets had fallen and to monitor the movement of IDF forces, thereby improving PIJ's rocket targeting. Another attack tracked aircraft landings and departures at Ben Gurion Airport, to better target rocket attacks during times of conflict and to disrupt Israel's civil aviation. In contrast, PIJ's attempts to intercept phone conversations on Israeli telecommunications were reportedly unsuccessful. PIJ cyber operatives have been trained in Gaza by Iran and, in some cases, in Iran itself.[187] Beyond this, little is known about PIJ's cyber activities.

185 Ron Ben-Yishai, *Ynet*, July 24, 2021; Pahlavi, "Digital Hezbollah."
186 Pahlavi, "Digital Hezbollah."
187 Gili Cohen, *Haaretz*, March 23, 2016; Yonah Jeremy Bob, *Jerusalem Post*, March 23, 2016.

The War in Gaza 2023

Fifteen hacking groups affiliated with Iran, Hezbollah, and Hamas were active in the first weeks of the war with Hamas that began in October 2023, all of which cooperated with each other to some degree. The Iranian hackers do not appear to have had preplanned cyber attacks aligned with Hamas's surprise attack; rather, it appears they operated largely reactively, exploiting opportunities as they arose. The war began primarily with CNE attacks and rapidly pivoted to CNA and CNI operations.[188] As of the end of the third month of the war, these attacks do not appear to have had a significant impact.

CNA: Vast numbers of relatively simple DDoS attacks were launched, designed to disrupt Israeli websites, especially those belonging to media and software firms, as well as banks, financial institutions, and government sites. During the first six days of the war, DDoS attacks reached one million attempted logons per second, before decreasing to under 100,000 in the following two weeks (an average website is able to process up to 10,000 at a time). Short-lived attempts were also made to disrupt Israel's rocket alert systems.[189]

At the onset of the war, the website of the *Jerusalem Post* was knocked off line for 2–3 days, presumably as part of an effort to prevent Israel from presenting its side of the conflict abroad.[190] Of somewhat greater consequence, the Iranian-affiliated hacking group Agrius, with the involvement of Hezbollah's Lebanese Cedar, sought to disrupt operations at the Ziv Hospital. The attack was

188 Israel National Cyber Directorate, "The Cyber Dimension of the 'Iron Swords' War: Insights and Means of Coping," December 24, 2023, https://www.gov.il/he/departments/news/published24122 (Hebrew); "Reactive and Opportunistic: Iran's Role in the Israel–Hamas War," *Microsoft.com*, November 9, 2023, https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023.

189 Raphael Kahan, "Hamas Hackers Are Trying to Scare Israelis with Fake SMS Messages and News Sites," *Ynet*, October 25, 2023, https://www.ynetnews.com/business/article/hjoy4f8mp.

190 Kahan, "Hamas Hackers."

thwarted before it succeeded in disrupting hospital operations, but sensitive patient information was stolen.[191] A separate phishing attack, impersonating emails from a cybersecurity firm, urged recipients to make urgent security updates to their software. To make the emails appear genuine, they included real information about the equipment used by the target organization. Once downloaded, the attached malware collected information from the targeted system and then used wiper software to erase the organization's entire information system. The attack was preceded by a careful study of the appropriate technical people to approach in each organization, in order to maximize the damage.[192]

CNI: In order to undermine Israel's standing and cast blame on the United States for Israel's alleged war crimes, Iran promoted highly charged, slanted, and at times even false information on social media, reaching a vast global audience in support of Hamas. Iranian accounts on Facebook and Twitter glorified Hamas atrocities against Israeli civilians and encouraged further attacks against them.[193]

Prewar incitement and disinformation campaigns targeting opponents of the "judicial overhaul" continued unabated during the early weeks of the war. Accounts on Facebook, Twitter, Instagram, Telegram, and WhatsApp were also used to stoke and exacerbate societal tensions surrounding sensitive

191 Israel National Cyber Directorate, "Iran and Hezbollah Stand Behind the Cyberattack against the Ziv Hospital during the Iron Swords War," December 18, 2023, https://www.gov.il/he/departments/news/ziv181223 (Hebrew).

192 Israel National Cyber Directorate, "A New Fishing Attack from Iran Tries to Erase Information in Organizations," December 26, 2023, https://www.gov.il/he/departments/news/iranf5_2612 (Hebrew).

193 Steven Lee Myers and Sheera Frenkel, "In a Worldwide War of Words, Russia, China and Iran Back Hamas," *New York Times*, November 3, 2023, https://www.nytimes.com/2023/11/03/technology/israel-hamas-information-war.html.

topics, such as the status of Israeli Arabs and radical positions identified with the extreme Israeli right.[194]

CNE: Tens of fake Iranian accounts on social media, especially Telegram, sought to provide Hamas with useful intelligence. In some cases, the fake profiles ostensibly pursued romantic relationships with IDF soldiers, as a means of tempting them into providing information about their units and operations. Thousands of IDF soldiers were targeted.[195]

194 Raphaela Goichman, "The Iranian Cyber attacks – More Sophisticated and Destructive," *The Marker*, November 6, 2023, https://www.themarker.com/captain-internet/2023-11-06/ty-article/.premium/0000018b-a44b-dc41-af9f-ef6bdcca0000 (Hebrew).

195 Raphael Kahan, *Ynet*, November 9, 2023.

PART 5:
CONCLUSIONS AND RECOMMENDATIONS

Iran's cyber capabilities have advanced considerably since the anti-regime demonstrations in 2009 and the Stuxnet attack in 2010 first sparked its interest in the cyber realm. In the past decade, Iran has become one of the more active states in cyberwarfare, probably at, or near, the top of the second tier of global actors. The number of attacks that Iran has launched and their sophistication have grown, and it has demonstrated the potential to destroy, disrupt, distort, sabotage, or undermine critical national infrastructure, commercial interests, military capabilities, domestic politics, societal resilience, and international diplomacy. Iran's capabilities will likely continue to improve, as a result of its own indigenous capabilities and due to Russian and Chinese assistance.

A reasonable working assumption is that Iran has provided Hezbollah with advanced cyber capabilities, much as it has done in other realms, but the publicly available evidence is insufficient to fully substantiate this conclusion. Most likely, this reflects the limitations of the information, rather than Hezbollah's capabilities. Far less information is available regarding PIJ; in this case, the paucity of information may more accurately reflect reality.

Without detracting from the depth of Iranian enmity toward the United States, Saudi Arabia, and—above all—Israel, it is important to recognize that much of its activity in the cyber realm, as in others, has been reactive and defensive. To illustrate, the rapid buildup of Iran's cyber capabilities was largely a response to the Stuxnet attack, as were the subsequent Abadil attacks against American financial institutions and the attack on Saudi Aramco. Iran prepared and conducted cyberattacks both prior to and following the signing of the 2015 nuclear deal; responded by cyber means to the American killing of Qassem Suleimani, the head of the IRGC's al-Quds arm; and has reportedly engaged in an ongoing exchange of cyber blows with Israel in recent years, including the attacks on Israel's water system and Ben Gurion Airport.

Asymmetric warfare has long comprised a critical component of Iran's national security strategy, designed to offset the advantages of its more powerful adversaries. In contrast with Israel's Arab adversaries in the past, Iran does not seek its defeat in the near-term, which it knows to be beyond its capabilities. Instead, Iran has adopted a long-term strategy of attrition designed to sap Israel's military strength, erode its international standing, and undermine its national morale and societal resilience, thereby leading to Israel's ultimate collapse. Over the years, cyber has come to constitute an increasingly important component of this strategy of attrition, Iran's overall national security strategy, and a set of policy instruments. Cyber is also particularly suited to Iran's strategic culture, which emphasizes ambiguity, deniability, and the use of proxies.

Iran's cyber operations have reached a global scale. It has attacked targets in Israel, the United States, and Saudi Arabia, as well as other countries around the world. An incomplete list includes France, Britain, Germany, Denmark, Albania, Canada, Australia, New Zealand, India, Japan, Bahrain, Jordan, Iraq, Turkey, and even Iran's two foremost allies—Russia and China. The types of targets it has attacked are similarly broad and include parliaments, government ministries—including defense and foreign affairs, defense contractors, military targets and diplomatic delegations; critical infrastructure firms—including power, water, and communications, air traffic control, oil and gas refineries, and pipelines; financial institutions, health organizations, airlines, high-tech and manufacturing firms; media organizations; academic institutions, think tanks, NGOs, and more.

The scale of Iran's activities, notwithstanding, it views cyber as a complementary capability, not a stand-alone one. As such, cyber is designed to buttress Iran's diplomatic, economic, and military capabilities and to strengthen its deterrence. Cyber is further viewed as a means of augmenting and amplifying Iran's more traditional asymmetric capabilities, such as terrorism, the use of proxies, and information operations. Cyber is a particularly important

instrument of asymmetric warfare for Iran because its leading adversaries, including the United States and Israel, are far more cyber dependent than it is and, therefore, potentially more vulnerable to attack.

Much like other states, including the United States and United Kingdom, Iran has adopted a full spectrum and flexible military doctrine. In other words, it reserves the right to take both offensive and defensive action, by whatever means it deems appropriate: kinetic, cyber, or increasingly through a combination of CNA, CNE, and CNI attacks.

Iran's praxis clearly demonstrates that it has *not* adopted a policy of "no first use" in the cyber realm. Conversely, there is no indication that Iran has integrated its cyber and nuclear strategies, such as whether it views systemic cyberattacks as an escalatory rung below the nuclear level and whether both are part of one overall national security strategy.

The following summarizes the study's primary findings regarding Iranian attacks in the categories of CNA, CNE, and CNI attacks, as well as combined ones, at times in conjunction with the use of ransomware.

CNA attacks: The Abadil and Shamoon attacks, and the attacks against Albania, among others, highlighted Iran's capability to cause significant economic disruption. Iranian attacks against critical national infrastructure in Israel, the United States, and Europe have yet to cause severely destructive effects, but the potential has been demonstrated. As noted, US intelligence believes that Iran is now capable of causing damage, with the attacks against Israel's water supply and air traffic control systems having demonstrated the potential for lethal harm.

Most of the CNA attacks that Iran has conducted to date have not been sophisticated, and the defenses that advanced cyber actors have put in place have usually proven sufficient to prevent significant damage. Indeed, most of the attacks have been against lightly defended public and private sector targets, thereby lending at least some credence to the contention that most Israeli and Western targets of importance are defended at a level beyond

all but the most sophisticated attacks. Conversely, unsophisticated Iranian defacements and disruptions of websites, both commercial and governmental, have succeeded in causing considerable inconvenience, along with some psychological effects on the public or on the consumer confidence.

Iran's ability to conduct effective and sustained military cyber operations, as opposed to attacks on civil and commercial targets that are not well defended, cannot be fully assessed on the basis of the public record. For obvious reasons, target states and Iran itself are loath to divulge their military cyber capabilities, or details of military cyberattacks conducted against them. Iran has also yet to manifest cyber capabilities at a systemic national level. It may, however, be withholding its most advanced capabilities for the "appropriate" circumstances. What is clear is that the cyber realm does provide Iran and its allies with an important tool kit with which to conduct deniable, under the radar operations.

CNE attacks: The very nature of espionage makes it difficult to fully assess the effectiveness of the Iranian CNE attacks to date. At a minimum, they have been numerous and have yielded some classified information of significance. CNE attacks have been conducted for a variety of purposes. Some have sought to collect intelligence regarding defense industries, weapons development programs, overall military capabilities, Israel's nuclear policy, and American, Western, and Israeli political and strategic thinking generally. Other CNE attacks have been conducted in preparation for future CNA and CNI attacks, including against defense firms, or to gain insights into the scientific and technological capabilities of Israel and other states. CNE operations for purposes of terrorist recruitment and perpetration of terrorist attacks already constitute an extent threat.

The intelligence windfall that Iran and others stood to gain from the attacks on the Shirbit and KLS Capital firms were arguably the Israeli equivalent of the damage that the infamous Russian SolarWinds attack caused the United States (and of which Israel, too, was a secondary victim). In the cases of the

attacks on Shirbit and KLS Capital firms, the intelligence debacle was further amplified by the subsequent Iranian information campaign, designed to cause Israel reputational damage by dumping the information on the internet.

Iran has made particularly effective use of CNE attacks for purposes of political surveillance and suppression, reportedly targeting dissidents both in Iran and abroad. Control of Iran's cyber realm, through the establishment of the NIW and a variety of other cyber means, has been used to suppress repeated rounds of demonstrations against the regime and help ensure its long-term stability.

CNI attacks: Iran has made extensive and rapidly growing use of information operations. Some operations have sought to create and exacerbate domestic divisions and discord, affect electoral processes, and undermine the social resilience of the target states, as evinced by Iran's repeated attacks against American and Israeli elections. Other attacks have been used to try to disrupt relations between foreign states and to instigate potentially severe crises, even at the nuclear level, in the case of Israel and Pakistan. Still others have caused financial and reputational damage to private firms around the world. Still, none of these attacks have approached the comprehensiveness and sophistication of those conducted by Russia against the US elections in 2016, and, in practice, their actual effectiveness has been limited. Iranian cyber information operations are also not known to have disrupted important political and governmental processes, nor did they cause significant social discord. Nevertheless, the number of such attacks is increasing and concern is growing.

Cyber information operations have provided Iran and its proxies with a variety of effective platforms for reaching a vast number of people around the world, directly, instantly, and at minimal cost, as part of the ongoing efforts to promote support for the Iranian regime. In so doing, cyber operations also have provided Iran them with important new means of creating international pressure on Israel to halt, or curtail, military operations before it can achieve

its objectives. As such, they have had an adverse impact on its ability to effectively wage war and on its international standing.

Combined attacks: The growing use of combined CNA, CNE, and CNI attacks, often together with ransomware, has produced comparatively effective results for Iran. The dumping on the internet of essentially all the personal information of Israel's LGBTQ community, or of an entire IDF combat brigade, are cases in point. The use of ransomware attacks primarily for purposes of information operations, as opposed to financial gain, is unique to Iran's confrontation with Israel.[196]

Iran's cyber praxis, to date, sheds light on three critical quandaries of interest both to cyber practitioners and theorists. First, it has demonstrated not just the importance that Iran attaches to the cyber realm, as a means of achieving its political and military objectives, but of doing so with little risk of escalation. In the aforementioned exchange of cyber and kinetic blows between Iran and Israel, the danger of escalation apparently was not a significant deterrent to future attacks and escalation.

In retrospect, Iran had good reason not to fear escalation. The United States is only known to have responded to cyberattacks by using kinetic means on two occasions, neither of which involved Iran. Israel is reported to have responded to cyberattacks by kinetic means only twice, in both cases against Hamas, and to have only used cyber means in response to cyberattacks on isolated occasions.[197] Israel reportedly did respond to an Iranian attack on its water system by escalating to an even more severe attack on an Iranian port, to which Iran then responded with additional, but clearly circumscribed, attacks on Israel's water system and other targets. Neither side, however,

196 Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations For Greater Effect," May 2, 2023; Dolev and Siman-Tov, "Iranian Cyber Influence Operations."

197 Borghard and Lonergan, "Cyber Operations"; Catalin Cimpanu, "Israel Bombed Two Hamas Cyber Targets," *The Record,* May 19, 2021; BBC Staff, *BBC*, June 9, 2021; Tal Shahaf, *Ynet*, May 21, 2021.

escalated further. The combined attacks that Iran has launched against Israel in recent years have certainly been disruptive and costly but not nearly as escalatory as attacks on critical infrastructure or military targets.

Second, if the contention that most Western and Israeli targets of importance are defended at a level that is beyond Iran's capabilities is indeed true, this would lend support to the position of those who contend in the professional literature that cyber is increasingly becoming defense, rather than offense, dominant. As noted, some even believe that Iran's ability to cause significant harm to sophisticated cyber actors is actually decreasing.

Third, whereas some cyber experts maintain that the cyber realm strengthens weaker actors by providing them with additional asymmetric means with which to counter the greater power of their adversaries, others argue that the sophisticated technological capabilities required to effectively use the cyber realm actually strengthen the advanced states even more. Experience with Iran appears to lend greater weight to the latter school of thought. Iran has certainly made important use of its cyber capabilities, but Israel, the United States, and other Western countries appear to have applied cyber to far greater socioeconomic, diplomatic, and military avail. Moreover, these countries make effective use of some of the same asymmetric military advantages that cyber proffers to Iran, while also wielding more powerful kinetic capabilities. They thus enjoy the advantages of both worlds. The bottom line may be a net overall gain in state power for already advanced actors.

Fourth, if an assessment of the Iranian cyber threat is based on the number of successful attacks of importance that have taken place to date and the actual consequences they have caused, then the threat has been significant albeit limited. If, however, the assessment is based on a realistic assessment of the potential for future disruption and damage, a growing threat cannot be discounted. Israel thus has no choice but to continue investing in its cyber ecosystem, civil cyber defense, and defensive and offensive military capabilities.

Israel's public and private sector cyber strategy was one of the first of its kind, based on cabinet decisions adopted between 2011–2015. Much has changed in the interim, however, and a significant review is warranted. Areas requiring renewed consideration include, but are not limited to, the regulatory system, ecosystem, systemic resilience, international cooperation, and inter-agency coordination. The new strategy must include clear objectives and a multi-year work plan with well-defined benchmarks.

The IDF has formulated an operational cyber doctrine but does not have an overall military cyber strategy. Furthermore, it is now eight years since the IDF decided to establish a unified cyber command and then suspended the decision, pending further review.[198] In order to maximize Israel's cyber capabilities, the IDF must formulate a comprehensive military cyber strategy, and it must be effectively integrated together with the other elements of Israel's national power into one overall national security strategy. Cyber capabilities are not—and should not be viewed—as a stand-alone category. How to reconstitute the force structure is the subject of considerable controversy; one way or the other, this issue must be resolved.

There is no statutory forum below the cabinet that is actively responsible for determining and coordinating military and intelligence cyber priorities, integrating the civil and military cyber strategies, and assigning organizational responsibility for implementing them. An informal arrangement does exist,[199] but this, too, does not maximize Israel's potential and must be rectified.

Stand-alone defeat of an adversary, in the traditional sense of preventing it from continuing to wage a conflict or undermining its psychological will to do so, is not usually achievable in the cyber realm. Instead, Israel should seek "cyber superiority"; that is, the ability to impose a level of disruption or

198 Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power* (Oxford: Oxford University Press, 2023), 250, 256, 257, 309.

199 Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 259.

damage on an adversary that it cannot tolerate, or to reduce the severity of attacks against Israel to a level at which it can continue to function without significant disruption. Stand-alone cyber superiority will also not usually prove feasible, but it may be possible to achieve cumulative mixed-domain superiority;[200] in other words, the gradual, additive application of the full range of capabilities available to Israel (cyber, kinetic, diplomatic, and economic). Cyber intelligence superiority is particularly important in Israel's uniquely harsh threat environment, both for purposes of early warning and for its overall intelligence capabilities.

Maintaining cyber superiority means cultivating a national pool of highly talented cyber professionals, in the civil, commercial, academic, and military realms. Israel, however, faces a considerable shortage of professionals.[201] Cyber education in schools and universities and adult training programs must be expanded. The IDF and intelligence agencies must continue exploring new ways of recruiting, training, and retaining personnel. The lure of the private sector, in Israel and abroad, remains a considerable challenge.

Israel must formulate a national strategy to counter malicious cyber information operations, designed to exacerbate social tensions, affect public discourse, and influence, or disrupt, electoral processes. The United States, United Kingdom, and France, among other democracies, have begun addressing this threat, and Israel can learn from their experience.

The Iranian nuclear program remains the greatest military threat to Israel's national security. The "Begin Doctrine," the preventive component of Israel's counter-proliferation strategy, has been implemented twice to date, against Iraq's nuclear program in 1981 and Syria's in 2007. It has not, however, been implemented against the Iranian nuclear program, at least in the classic sense of an air strike. Some believe that the numerous kinetic and cyberattacks that Israel has reportedly conducted to sabotage, delay, and derail the Iranian

200 Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 79–80.
201 Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 198.

program may be a new means of implementing the doctrine. The Stuxnet virus is the most famous of these efforts and may have been an early harbinger of this changing reality.[202] Be that as it may, Israel must ensure that it has the kinetic and cyber capabilities to prevent Iran from ever gaining an operational nuclear capability.

Finally, the United States is Israel's primary partner in the cyber realm, as in all others, and the two countries engage in extensive civil and military cooperation. Unlike most areas of bilateral military cooperation, Israel's cyber capabilities are primarily homegrown, and it has much to offer the United States and not just to gain. It is important that Israel should further expand cyber cooperation to the extent possible, but that it does so in a manner that minimizes the risks to its freedom of independent action. A formal and permanent structure of cyber dialogue should be institutionalized between the relevant government agencies and formalized in new and expanded Memoranda of Understanding.[203]

202 Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 318.
203 Freilich, Cohen, and Siboni, *Israel and the Cyber Threat,* 221, 330.

BIBLIOGRAPHY

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data*. Santa Monica: Rand Corporation, 2014.

Ackerman, Gwen and Alisa Odenheimer. "Israeli Official Says First Wave of Cyber Hack Was Thwarted." *Bloomberg*, April 26, 2017, https://www.bloomberg.com/news/articles/2017-04-26/israeli-official-says-first-wave-of-cyber-hack-was-thwarted#xj4y7vzkg.

Ahronheim, Anna. "Hezbollah Has Some 2,000 Unmanned Aerial Vehicles – ALMA." *Jerusalem Post*, December 22, 2021, https://www.jpost.com/middle-east/article-689470.

Akbar, Ali. "Iran's Regional Influence in Light of its Security Concerns." *Middle East Policy* 28, no. 3–4 (2021): 186–202.

Alimardani, Mahsa. "Iran Declares 'Unveiling' of its National Intranet." *Advox*, September 2, 2016, https://advox.globalvoices.org/2016/09/02/iran-declares-unveiling-of-its-national-intranet/.

Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace, 2018.

AP. "Microsoft Says Iranian Hackers Targeted Conference Attendees." October 28, 2020, https://apnews.com/article/germany-hacking-iran-email-saudi-arabia-807fe633c5388341f19a050414f65669.

Arghire, Ionut. "Iran-Run ISP 'Cloudzy' Caught Supporting Nation-State APTs, Cybercrime Hacking Groups." *SecurityWeek*, August 1, 2023, https://www.securityweek.com/iran-run-isp-cloudzy-caught-supporting-nation-state-apts-cybercrime-hacking-groups/.

Barnes, Julian. "Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says." *New York Times*, December 21, 2018, https://www.nytimes.com/2018/12/21/us/politics/russia-midterm-election-influence-coates.html.

Barnes, Julian E. and David E. Sanger. "Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn." *New York Times*, October 21, 2020, https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html.

Barzashka, Ivanka. "Are Cyber-Weapons Effective?" *RUSI Journal* 158, no. 2 (2013): 48–56.

Bar-Zik, Ran. "Thousands of Websites Defaced in Cyberattack Calling for the 'Destruction of Israel.'" *Haaretz,* May 21, 2020, https://www.haaretz.com/israel-news/2020-05-21/ty-article/.premium/thousands-of-websites-defaced-in-cyberattack-calling-for-the-destruction-of-israel/0000017f-e104-df7c-a5ff-e37e01bb0000.

Bateman, Tom. "Iran Accused of Sowing Israel Discontent With Fake Jewish Facebook Group." *BBC*, February 3, 2022, https://www.bbc.com/news/world-middle-east-60229146.

Bebber, R. "Information War and Rethinking Phase 0." *Journal of Information Warfare* 15, no. 2 (2016): 39–52.

Behroozi, Setareh. "We are in Iran for Cooperation, not to Sign Memorandums: Russian Official." *Tehran Times*, June 24, 2019, https://www.tehrantimes.com/news/437369/We-are-in-Iran-for-cooperation-not-to-sign-memorandums-Russian.

Benjakob, Omer. "Iranian Accounts, Russian Tactics and Q: Israel Has Become a Disinformation Battlefield." *Haaretz*, April 21, 2021, https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/iranian-accounts-russian-tactics-and-q-israel-has-become-a-disinfo-battlefield/0000017f-e827-df2c-a1ff-fe77db160000.

___. "Iranian Hackers Hit Top Israeli Defense Contractor, Data Leaked as Cyberattack Continues." *Haaretz*, December 20, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-20/ty-article/.premium/iranian-hackers-hit-israel-aerospace-industries-leak-data-as-cyberattack-continues/0000017f-df09-d856-a37f-ffc918470000.

___. "Israel Election: Twitter Purges Foreign Influence Op to Suppress Voting." *Haaretz*, November 1, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-11-01/ty-article/.premium/israel-election-twitter-purges-foreign-influence-op-to-suppress-voting/00000184-337c-d0c7-affe-7b7efb650000.

___. "'It's Not About Money': Destructive Cyberattack Proves Israel Lacks One Key Thing." *Haaretz,* December 9, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-09/ty-article/.highlight/its-not-about-money-destructive-cyberattack-proves-israel-lacks-one-key-thing/0000017f-e184-d568-ad7f-f3efed670000.

___. "'Operation Quicksand': Iran-Linked Hackers Target Israel in 'New Cyberwar Phase.'" *Haaretz*, October 19, 2020, https://www.haaretz.com/israel-news/tech-news/2020-10-19/ty-article/iran-hackers-israel-new-phase-cyberwar-operation-quicksand/0000017f-e1a0-df7c-a5ff-e3fa7d400000.

Bennett, Brian. "Exclusive: Iran Steps up Efforts to Sow Discord Inside U.S." *Time*, June 7, 2021, https://time.com/6071615/iran-disinformation-united-states/.

Bergman Ronen and Farnaz Fassihi. "Iranian Hackers Found Way Into Encrypted Apps, Researchers Say." *New York Times*, September 18, 2020, https://www.nytimes.com/2020/09/18/world/middleeast/iran-hacking-encryption.html.

Bernard, Tara Siegel, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Bing, Chris. "Chinese-authored Spyware Found on More than 700 Million Android Phones." *Cyber Scoop*, November 15, 2016, https://cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/.

Bob, Yonah Jeremy. "The Coming Cyber Winter is Worse Than all Estimates." *Jerusalem Post*, December 10, 2020, https://www.jpost.com/israel-news/the-coming-cyber-winter-is-worse-than-all-estimates-651696.

___. "IDF Intel Chief: We'll Keep Peace in North Despite Hezbollah Provocations." Jerusalem Post, July 11, 2023, https://www.jpost.com/israel-news/article-750010.

___. "Iran Hackers Closer to Penetrating Israel US Drones Cyberdefense CEO." *Jerusalem Post*, November 21, 2022, https://www.jpost.com/middle-east/iran-news/article-722964.

___. "Israeli Cyber Czar Warns of More Attacks From Iran." *Jerusalem Post*, May 28, 2020, https://www.jpost.com/israel-news/israeli-cyber-czar-warns-of-more-attacks-from-iran-629577.

___. "Secret Iran Hacking Plans Against West Revealed – Report." *Jerusalem Post*, July 27, 2021, https://www.jpost.com/international/secret-iran-hacking-plans-against-west-revealed-report-674992.

___. "Suspected Iranian Cyberattack Targets Israel Aerospace Industries." *Jerusalem Post*, December 20, 2020, https://www.jpost.com/breaking-news/suspected-iranian-cyberattack-targets-israel-aerospace-industries-652731.

Borghard, Erica D and Shawn W. Lonergan. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* (2019): 122–145.

Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia, 2018.

Braue, David. "Iranian Hackers Targeting Australian Infrastructure." *ACS*, September 26, 2022, https://ia.acs.org.au/article/2022/iranian-hackers-targeting-australian-infrastructure.html.

Brewster, Tom. "Persian Paranoia: America's Fear of Iranian Cyber Power." *The Guardian*, August 29, 2014, https://www.theguardian.com/technology/2014/aug/29/iran-cyber-power-america-networks.

Brode, Bernard. "The Shirbit Data Hack Was an Attack on National Security. Now What? *Times of Israel*, December 18, 2020, https://blogs.timesofisrael.com/deconstructing-the-shirbit-data-breach-now-what/.

Brunner, Jordan A. "The (Cyber) New Normal: Dissecting President Obama's Cyber National." *Jurimetrics Journal* 57, no. 3 (2017): 397–431.

Buchanan, Ben. *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford, 2017.

Burke, Garance and Jonathan Fahey. "AP Investigation: US Power Grid Vulnerable to Foreign Hacks." *Associated Press,* December 21, 2015, https://apnews.com/general-news-c8d531ec05e0403a90e9d3ec0b8f83c2.

Cahmutoğlu, Ersin. *Iran's Cyber Power*. Ankara: iRAM: Center for Iranian Studies, April 2021.

Cassidy, Christina A. and Frank Bajak. "US Cyberwarriors thwarted 2020 Iran Election Hacking Attempt." *Associated Press,* April 25, 2023, https://apnews.com/article/election-security-iran-2020-voting-cybersecurity-c2faa52ffa3009f53232e4d89053980c.

Cilluffo, F. J. and Clark, J. R. "Building a Conceptual Framework for Cyber's Effect on National Security," *Journal of Information Warfare* 15, no. 2 (2016): 1–16.

Cimpanu, Catalin. "Israel Bombed Two Hamas Cyber Targets." *The Record,* May 19, 2021, https://therecord.media/israel-bombed-two-hamas-cyber-targets.

___. "New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company." *ZDNet*, January 8, 2020, https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/.

Citrinowicz, Danny and Ari Ben-Ami. "The Iranian Information Revolution: How Iran Utilizes Social Media and Internet Platforms to Incite, Recruit and Create Negative Influence Campaigns." *European Eye on Radicalization*, Report 30, July 2022.

Citrinowicz, Danny and Jason Brodsky. "Iran's Cyberspace Evolution." *The Dispatch*, April 12, 2022.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It*. HarperCollins, 2010.

Clearsky Research Team. "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford." Clearsky.com, January 25, 2017, https://www.clearskysec.com/2017/01/.

___. "Rocket Kitten 2 – Follow-Up on Iran Originated Cyber-Attacks." Clearsky.com, September 1, 2015, https://www.clearskysec.com/rocket-kitten-2/.

CNN Staff. "Iran Leader Urges Destruction of 'Cancerous' Israel." *CNN*, December 15, 2000, http://edition.cnn.com/2000/WORLD/meast/12/15/mideast.iran.reut/.

Cohen, Daniel and Danielle Levin. "Operation Protective Edge: The Cyber Defense." In *The Lessons of Operation Protective Edge*, edited by Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2014), 59–63.

Cohen, Matthew S., Charles (Chuck) D. Freilich, and Gabi Siboni. "Israel and Cyberspace: Unique Threat and Response." *International Studies Perspectives* 17, no. 3 (2016): 307–321.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. "Four Big 'Ds' and a Little 'r': A New Model for Cyber Defense." *Cyber, Intelligence, and Security* 1, no. 1 (2017): 21–36.

Congressional Research Service. "Iranian Offensive Cyber Attack Capabilities." (January 13, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11406.

Connolly, Kate. "Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel." *The Guardian*, May 13, 2020, https://www.theguardian.com/world/2020/may/13/russian-hacking-attack-on-bundestag-damaged-trust-says-merkel.

Conti, Gregory and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion 2017.

Corera, Gordon. "Iran 'Hides Spyware in Wallpaper, Restaurant and Games Apps.'" *BBC News*, February 8, 2021. https://www.bbc.com/news/technology-55977537.

Cornish, Paul, ed. *Oxford Handbook of Cyber Security*. Oxford University Press, 2021.

Crisp, Wil and Suadad al-Salhy. "Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East." *The Telegraph*, August 2, 2020, https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/.

Cuthbertson, Anthony. "Iranian Hackers Attack UK Universities to Steal Research Secrets." *The Independent*, August 24, 2018, https://www.independent.co.uk/tech/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html.

Cyber Threat Brief. *Flash Critic*. November 29, 2015.

Davidi, Avi. "Iranian-Russian Cooperation on Hack Attacks May Challenge Israeli Cyber Supremacy." *Times of Israel*, April 18, 2023, https://www.timesofisrael.com/iranian-russian-cooperation-on-hack-attacks-may-challenge-israeli-cyber-supremacy/.

De Souza, Ryan. "Israeli Security Camera Systems Targeted by Pro-Hezbollah Hackers." *Hackread*, February 21, 2016, https://www.hackread.com/israeli-security-camera-systems-targeted-by-hezbollah-hackers/.

Demboski, Morgan and IronNet Threat Research and Intelligence Teams. "Analysis of the Iranian Cyber Attack Landscape." *IronNet*, September 15, 2021, https://www.ironnet.com/blog/iranian-cyber-attack-updates.

Demchak, Chris C. *Wars of Disruption and Resilience*. University of Georgia Press, 2011.

Denning, Dorothy. "Explainer: How Iran's Military Outsources its Cyberwarfare Forces." *Navy Times*, January 23, 2020, https://www.navytimes.com/news/your-navy/2020/01/23/explainer-how-irans-military-outsources-its-cyberwarfare-forces/.

Dickstein, Corey. "Military Warns of Iranian Hackers Targeting American Troops With Fake Job Website." *Stars and Stripes*, October 4, 2019, https://www.stripes.com/theaters/middle_east/military-warns-of-iranian-hackers-targeting-american-troops-with-fake-jobs-website-1.601787.

Doffman, Zak. "U.S. Military Warns Outlook Users to Update Immediately Over Hack Linked to Iran." *Forbes,* July 3, 2019, https://www.forbes.com/sites/zakdoffman/2019/07/03/u-s-cyber-command-warns-millions-of-outlook-users-of-malicious-hack-linked-to-iran/?sh=b29bce326fd4.

Dolev, Boaz and David Siman-Tov. "Iranian Cyber Influence Operations Against Israel Disguised as Ransomware Attacks." INSS Special Publication, January 27, 2022.

Dor, Ofir. "'Unsophisticated Iranian Cyberattack' Temporally Downs Israeli Bank Sites, Post Office." *Haaretz*, April 14, 2023, https://www.haaretz.com/israel-news/2023-04-14/ty-article/.premium/unsophisticated-iranian-cyberattack-temporally-downs-israeli-bank-sites-post-office/00000187-7fd6-dc6c-a5ff-7fd77fad0000.

Douris, Constance. "Cyber Assault on Electric Grid Could Make U.S. Feel Like Post-Hurricane Puerto Rico." *Forbes,* February 6, 2018, https://www.forbes.com/sites/constancedouris/2018/02/06/cyber-assault-on-electric-grid-could-make-u-s-feel-like-post-hurricane-puerto-rico/.

Economist. "The Big Data Breach Suffered by Equifax Has Alarming Implications." September 16, 2017, https://www.economist.com/finance-and-economics/2017/09/16/the-big-data-breach-suffered-by-equifax-has-alarming-implications.

___. "The WannaCry Attack Reveals the Risks of a Computerised World." May 20, 2017, https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-the-risks-of-a-computerised-world.

Esfandiari, Golnaz. "Iran to Work With China to Create National Internet System." *Radio Free Europe*, *Radio Liberty*, September 4, 2020, https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html.

Even, Shmuel and David Siman-Tov. *Cyber Warfare: Concepts and Strategic Trends.* Memorandum No. 117. Tel Aviv: INSS, 2012.

Fabian, Emanuel. "Gantz Says Iran and Hezbollah Tried to Hack UN Peace Force, Steal Deployment Data." *Times of Israel*, June 29, 2022, https://www.timesofisrael.com/gantz-says-iran-and-hezbollah-attempted-to-hack-unifil-steal-deployment-infomation/.

Facebook. *Threat Report The State of Influence Operations 2017–2020.* May 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf.

FakeReporter, "Rolling in the Deep: An Iranian Cross-Platform Influence Operation Summary." Rolling_in_the_Deep_Summary.pdf (fakereporter.net).

Fassihi, Farnaz and Ronen Bergman. "Israel and Iran Broaden Cyberwar to Attack Civilian Targets." *New York Times*, November 27, 2021, https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html.

Fassihi, Farnaz and Steven Lee Myers. "China, With $400 Billion Iran Deal, Could Deepen Influence in Mideast." *New York Times*, March 27, 2021, https://www.nytimes.com/2021/03/27/world/middleeast/china-iran-deal.html.

___. "Defying U.S., China and Iran Near Trade and Military Partnership." *New York Times*, July 11, 2020, https://www.nytimes.com/2020/07/11/world/asia/china-iran-trade-military-deal.html.

Faucon, Benoit. "Iran Restricts Internet Access as Women's Rights Protests Spread." *Wall Street Journal*, September 22, 2022, https://www.wsj.com/articles/iran-restricts-internet-access-as-womens-rights-protests-spread-11663874073.

Faucon, Benoit and Liza Lin. "U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup." *Wall Street Journal*, February 4, 2023, https://www.wsj.com/articles/u-s-weighs-sanctions-for-chinese-companies-over-iran-surveillance-buildup-11675503914.

FBI Boston. "FBI Releases Cybersecurity Advisory on previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies." September 17, 2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-releases-cybersecurity-advisory-on-previously-undisclosed-iranian-malware-used-to-monitor-dissidents-and-travel-and-telecommunications-companies.

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2018): 381–393.

Fisher, Dennis. "FBI Warns of Attacks From Iranian Threat Group Emennet Pasargad." *Decipher*, October 21, 2022, https://duo.com/decipher/fbi-warns-of-attacks-from-iranian-threat-group-emennet-pasargad.

Freilich, Charles D. *Israeli National Security: A New Strategy for an Era of Change*. Oxford: Oxford Press, 2018.

Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power*. Oxford: Oxford Press, 2023.

Frenkel, Sheera. "Iranian Disinformation Effort Went Small to Stay Under Big Tech's Radar." *New York Times*, June 30, 2021, https://www.nytimes.com/2021/06/30/technology/disinformation-message-apps.html.

Fung, Brian. "Uber Reaches $148 Million Settlement over its 2016 Data Breach, which Affected 57 Million Globally." *Washington Post*, September 26, 2018, https://www.washingtonpost.com/technology/2018/09/26/uber-reaches-million-settlement-over-its-data-breach-which-affected-million-globally/.

Government of Israel, Ministry of Intelligence, National Intelligence Directorate. "Foreign Interference and Influence on Social Media in Israel." (Hebrew), May 7, 2023.

Greenberg, Andy. "Iranian Hackers Have Been 'Password-Spraying' the US Grid." *Wired*, January 9, 2020, https://www.wired.com/story/iran-apt33-us-electric-grid/.

Greene, Jay, Tony Romm, and Ellen Nakashima. "Iranians Tried to Hack U.S. Presidential Campaign in Effort that Targeted Hundreds, Microsoft Says." *Washington Post*, October 4, 2019, https://www.washingtonpost.com/technology/2019/10/04/iran-tried-hack-us-presidential-candidates-journalists-effort-that-targeted-hundreds-microsoft-finds/.

HaCohen, Hagay. "Check Point Unveils New Iranian Cybercrime, Ransoming Companies' Data." *Jerusalem Post*, November 12, 2020, https://www.jpost.com/israel-news/check-point-unveils-new-iranian-cybercrime-ransoming-companies-data-648928.

Hahn, Roei and Yuval Mann. "Leading Israeli Research Institute Falls Prey to Cyberattack." *Ynet*, December 2, 2023, https://www.ynetnews.com/business/article/syjobiuti.

Halpern, Sue. "Should the U.S. Expect an Iranian Cyberattack?" *New Yorker*, January 6, 2020, https://www.newyorker.com/tech/annals-of-technology/should-the-us-expect-an-iranian-cyberattack.

Hardie, John and Annie Fixler. "Russia-Iran Cooperation Poses Challenges for US Cyber Strategy, Global Norms." *C4ISR*, February 8, 2021, https://www.c4isrnet.com/thought-leadership/2021/02/08/russia-iran-cooperation-poses-challenges-for-us-cyber-strategy-global-norms/.

Harel, Amos. "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line." *Haaretz*, May 20, 2020, https://www.haaretz.com/middle-east-news/iran/2020-05-20/ty-article/.premium/cyberattack-on-iran-marks-a-clear-red-line/0000017f-f4f9-d5bd-a17f-f6fb54c40000.

Harel, Amos, Yaniv Kubovich, and Reuters. "Israel Accuses Iran, Hezbollah of Hacking UN Force in Lebanon." *Haaretz,* June 29, 2022, https://haaretz.com/israel-news/2022-06-29/ty-article/.premium/israel-accuses-iran-hezbollah-of-hacking-un-force-in-lebanon/00000181-ae8d-dacc-a9f7-eedf37450000.

Harris, Shane. *@War: The Rise of the Military-Internet Complex*. Eamon Dolan/Mariner, 2014.

Hasson, Ayala. "Iranian Hackers Posed as General Yadlin and Gained Information from an Israeli Researcher." (Hebrew), *Channel 13*, November 20, 2020, https://13news.co.il/item/news/politics/security/iran-hackers-1162861/.

Hatoni, Yossi. "Hezbollah Cyberattacked Hundreds of Companies, Also in Israel." *People and Computers* (Hebrew), January 28, 2021, https://www.pc.co.il/news/331154/.

Herr, Trey. "PrEP: A Framework for Malware & Cyber Weapons." *Cyber Security Policy and Research Institute*. George Washington University, March 12, 2014.

Herzallah, Mohammad J. "Israeli Fights Wire with Wire." *Newsweek*, July 27, 2009.

Hope, Bradley, Warren P. Strobel, and Dustin Volz. "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran." *Wall Street Journal*, August 7, 2019, https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488.

Horovitz, Michael. "Report: Iran Hacked Israeli Cameras a Year Ago; Defense Officials Knew, Didn't Act." *Times of Israel*, December 19, 2022, https://www.timesofisrael.com/report-iran-hacked-israeli-cameras-a-year-ago-defense-officials-knew-didnt-act/

Howarth, Josh. "80+ Amazing IoT Statistics (2023-2030)." Explodingtopics.com, March 16, 2023, https://explodingtopics.com/blog/iot-stats.

Hsu, Jeremy. "U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks." *IEEE Spectrum*, March 26, 2014, https://spectrum.ieee.org/us-suspicions-of-chinas-huawei-based-partly-on-nsas-own-spy-tricks.

Hymas, Charles. "Iran Targets UK Political System With Fake Websites." *The Telegraph*, June 6, 2021, https://www.telegraph.co.uk/politics/2021/06/06/iran-targets-uk-political-system-fake-websites/.

Industrial Cyber. "New Dragos Report Reveals Iranian Hackers Targeting U.S Power Grid amid Tensions Between Two Nations." January 13, 2020, https://industrialcyber.co/industrial-cyber-attacks/new-dragos-report-reveals-iranian-hackers-targeting-u-s-power-grid-amid-tensions-between-two-nations/.

International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." Research Papers, June 28, 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

Isaac, Mike and Sheera Frenkel. "Facebook Security Breach Exposes Accounts of 50 Million Users." *New York Times*, September 28, 2018, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

Israel National Cyber Directorate. "Iranian Government Sponsored Threat Actor Muddy Water Conducts Cyber Attack Against Israel." March 9, 2023, https://www.gov.il/en/departments/news/_muddywater.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option.* Rowman and Littlefield, 2017.

Jerusalem Post Staff. "Israel Independence Day Cyberattack Takes Down Major News Websites." *Jerusalem Post*, April 26, 2023.

___. "Israeli Cyber Security Website Briefly Taken Down in Cyberattack." *Jerusalem Post*, April 4, 2023.

___. "United Hazalah Hit By Tens of Thousands of Cyberattacks Past Two Days." *Jerusalem Post*, April 5, 2023.

Jerusalem Post Staff and Tovah Lazaroff. "Israel is Updating Attack Plans Against Iran's Nuclear Sites – Gantz." *Jerusalem Post*, March 15, 2021, https://www.jpost.com/israel-news/gantz-reveals-classified-hezbollah-target-map-during-fox-news-interview-661029.

Joffre, Tzvi. "Iran-Backed Hackers Targeting Activists, Journalists, Politicians – HRW." *Jerusalem Post*, December 5, 2022, https://www.jpost.com/middle-east/iran-news/article-724088.

Derek Johnson, "Iranian Hacking Group Impersonating Nuclear Experts to Gain Intel from Western Think Tanks." *SC Media*, July 6, 2023, https://www.scmagazine.com/news/an-iranian-hacking-group-is-impersonating-nuclear-experts-to-gain-intel-from-western-think-tanks.

Jones, Sam. "Cyber Warfare: Iran Opens a New Front." *Financial Times*, April 26, 2016, https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3.

Kanno-Youngs, Zolan and David Sanger. "U.S. Accuses China of Hacking Microsoft." *New York Times*, July 19, 2021, https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html.

Kausch, Kristina and Lior Tabansky. "Cybered Conflict in the Middle East." *Mediterranean Dialogue Series* No. 15, Konrad Adenauer Stiftung, 2018.

Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security* 38, no. 2 (2013): 7–40.

Kenney, Michael. "Cyber-Terrorism in a Post-Stuxnet World." *Orbis* 59, no. 1 (2015): 111–128.

King Faisal Center for Research and Islamic Studies. *Iran's Cyberattacks Capabilities*, Special Report, January 2020.

Kube, Courtney, Carol E. Lee, Dan De Luce, and Ken Dilanian. "Iran Has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials." *NBC News*, July 20, 2018, https://nbcnews.to/2uFfKi0.

Kubovich, Yaniv. "Iran Used Instagram to Try and Lure Israelis to Meetings Abroad, Shin Bet and Mossad Say." *Haaretz*, April 12, 2021, https://www.haaretz.com/israel-news/2021-04-12/ty-article/.highlight/iranian-intelligence-used-instagram-to-try-and-lure-israelis-abroad-shin-bet-says/0000017f-ef6c-d497-a1ff-efec462c0000.

___. "Iranian Hackers Post Footage of Jerusalem Bombing, Taken by Large Security Agency." *Haaretz*, November 24, 2022, https://www.haaretz.com/israel-news/2022-11-24/ty-article/.premium/iranian-hackers-breach-major-israeli-security-agency/00000184-a988-dd96-ad8c-eba817250000.

Kuperwasser, Yossi and David Siman-Tov, eds., *The Cognitive Campaign: Strategic and Intelligence Perspectives*. Memorandum No. 197. Tel Aviv: INSS, 2019.

Lappin, Yaakov. "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says." *Jerusalem Post*, August 17, 2014, https://www.jpost.com/arab-

israeli-conflict/iran-attempted-large-scale-cyber-attack-on-israel-senior-security-source-says-371339.

Lee, Michael. "Chinese Facial Recognition Technology Helping Iran to Identify Women Breaking Strict Dress Code: Report." *Fox News,* January 12, 2023, https://www.foxnews.com/world/chinese-facial-recognition-technology-helping-iran-identify-women-breaking-strict-dress-code-report.

Lee, Vivian. "Despite Iran's Efforts to Block Internet, Technology Has Helped Fuel Outrage." *New York Times*, September 29, 2022, https://www.nytimes.com/2022/09/29/world/middleeast/iran-internet-censorship.html.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation, 2009.

___. "Second Acts in Cyberspace." In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart. Brookings, 2019.

Lieber, Dov, Benoit Faucon, and Michael Amon. "Russia Supplies Iran With Cyber Weapons as Military Cooperation Grows." *Wall Street Journal*, March 27, 2023, https://www.wsj.com/articles/russia-supplies-iran-with-cyber-weapons-as-military-cooperation-grows-b14b94cd.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force. *Journal of National Security Law and Policy* 4, no. 63 (2010):63–86.

Lin, Herbert and Amy Zegart. *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Brookings, 2019.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, no. 3 (2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

Long, Austin. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart. Brookings, 2019.

Loudermilk, Micah. "Iran Crisis Moves Into Cyberspace." Policy Watch 3151, *Washington Institute for Near East Policy* (July 9, 2019), https://www.washingtoninstitute.org/policy-analysis/iran-crisis-moves-cyberspace.

Matania, Eviatar and Eldad Tal-Shir. "Continuous Terrain Remodelling: Gaining the Upper Hand in Cyber Defence." *Journal of Cyber Policy* 5, no. 2 (2020): 285–301. https://doi.org/10.1080/23738871.2020.1778761.

Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan. "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy." *Georgetown Journal of International Affairs* 27, no. 3 (2016): 77–84.

McMillan, Robert. "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years." *Wall Street Journal*, March 6, 2019, https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

Menn, Joseph. "Iran Gained Access to Election Results Website in 2020, Military Reveals." *Washington Post*, April 24, 2023.

Microsoft Threat Intelligence. "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect." May 2, 2023.

Miller, Maggie. "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack." *Politico*, October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

Morello, Carol and Missy Ryan. "U.S. Says Iranian Forces May Have Killed More Than 1,000 Protestors." *Washington Post*, December 5, 2019, https://www.washingtonpost.com/world/national-security/trump-administration-alleges-iran-has-killed-more-than-1000-protesters/2019/12/05/e9c11a76-1775-11ea-bf81-ebe89f477d1e_story.html.

Moskowitz, Jeff. "Cyberattack Tied to Hezbollah Ups The Ante for Israel's Digital Defenses." *Christian Science Monitor*, June 1, 2015, https://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

Muncaster, Phil. "US: Iran Was Behind Proud Boys Email Campaign." *Infosecurity Magazine*, October 22, 2020, https://www.infosecurity-magazine.com/news/us-iran-was-behind-proud-boys/.

Nakashima, Ellen. "Iranian Hackers Are Targeting U.S. Officials Through Social Networks, Report Says." *Washington Post*, May 29, 2014, https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html.

Nakashima, Ellen, Josh Dawsey, and Matt Viser. "China, Iran Targeting Presidential Campaigns With Hacking Attempts, Google Announces." *Washington Post*,

June 4, 2020, https://www.washingtonpost.com/national-security/china-iran-targeting-presidential-campaigns-with-hacking-attempts-google-announces/2020/06/04/45a64e78-a692-11ea-b619-3f9133bbb482_story.html.

Nakashima, Ellen, Amy Gardner, and Aaron Davis. "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims." *Washington Post*, December 22, 2020, https://www.washingtonpost.com/national-security/iran-election-fraud-violence/2020/12/22/4a28e9ba-44a8-11eb-a277-49a6d1f9dff1_story.html.

Nakashima, Ellen, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg. "U.S. Government Concludes Iran Was Behind Threatening Emails Sent to Democrats." *Washington Post*, October 22, 2020, https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

Nakashima, Ellen and Spencer Hsu. "Microsoft Says it Has Found Iranian Hackers Targeting U.S. Agencies, Companies and Middle East Advocates." *Washington Post*, March 27, 2019, https://www.washingtonpost.com/local/legal-issues/microsoft-says-it-has-found-iranian-hackers-targeting-us-agencies-companies-and-middle-east-advocates/2019/03/27/8056c51e-50a0-11e9-8d28-f5149e5a2fda_story.html.

National Intelligence Council. "Foreign Threats to the 2020 Federal Elections." March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

Newman, Lily Hay. "How Iran Tried to Undermine the 2020 US Presidential Election." *Wired*, November 18, 2021, https://www.wired.com/story/iran-2020-election-interference/.

___. "How the Iranian Government Shut Off the Internet." *Wired*, November 17, 2019, https://www.wired.com/story/iran-internet-shutoff/.

Nye, Joseph S. *The Future of Power: Its Changing Nature and Use in the Twenty-first Century*. New York: Hachette Book Group, 2011.

O'Flaherty, Kate. "DoJ Unveils Iran Disinformation Campaign—Seizes 92 Domains Violating U.S. Sanctions." *Forbes*, October 9, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/10/09/doj-unveils-iran-disinformation-campaign-seizes-92-domains-violating-us-sanctions/.

Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." (2021).

___. "Annual Threat Assessment of the U.S. Intelligence Community." (2022), https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Orbach, Meir. "Israeli Cybersecurity Giant Tracks Ranson Payments From New Cyber Attack to Iranian Nationals." *The Algemeiner*, November 12, 2020, https://www.algemeiner.com/2020/11/12/israeli-cybersecurity-giant-tracks-ransom-payments-from-new-cyber-attack-to-iranian-nationals/.

Orbach, Meir and Golan Hazani. "Israel's Supply Chain Targeted in Massive Cyberattack." *Calcalist*, December 13, 2020.

Page, Carly. "Iran-Backed Hackers Breached a US Federal Agency that Failed to Patch Year-Old Bug." *Yahoo News*, November 17, 2022.

Pahlavi, Pierre. "Digital Hezbollah and Political Warfare in Cyberspace." *National Interest*, October 31, 2022, https://nationalinterest.org/feature/digital-hezbollah-and-political-warfare-cyberspace-205558.

Parks, Miles. "View From the Ground at Washington DC Protests; Misinformation Spreads Online." *NPR*, June 4, 2020.

Perkovich, George and Ariel (Eli) Levite, eds. *Understanding Cyber Conflict: 14 Analogies.* Washington DC: Georgetown University Press, 2017.

Perlroth, Nicole. "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack." *New York Times*, October 3, 2017, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

___. "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies." *New York Times*, February 18, 2019, https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

___. "Cyberespionage Attacks Tied to Hackers in Iran." *New York Times*, May 29, 2014, https://archive.nytimes.com/bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/.

Pfeffer, Anshel. "Israel Suffered Massive Cyber Attack During Gaza Offensive." *Haaretz*, June 15, 2009, https://www.haaretz.com/2009-06-15/ty-article/israel-

suffered-massive-cyber-attack-during-gaza-offensive/0000017f-f6ac-ddde-abff-feedb26c0000.

___. "Why Netanyahu Failed to Mention the Iranian Link to the Cyberattack on Israel." *Haaretz*, April 27, 2017, https://www.haaretz.com/israel-news/2017-04-27/ty-article/why-netanyahu-failed-to-link-iran-to-cyberattack-on-israel/0000017f-e858-dea7-adff-f9fb5c720000.

Pileggi, Tamar. "Khamenei: Israel a "Cancerous Tumor' that 'Must be Eradicated." *Times of Israel*, June 4, 2018, https://www.timesofisrael.com/khamenei-israel-a-cancerous-tumor-that-must-be-eradicated/.

Pinko, Eyal. "Iranians Developing the Cyber Capabilities of Hezbollah." *Israel Defense*, March 30, 2021, https://www.israeldefense.co.il/en/node/49094.

Pomerleau, Mark. "US Cyber Forces Wrap Up Deployment to Albania in Response to Iranian Cyberattacks." *DefenseScoop*, March 23, 2023, https://defensescoop.com/2023/03/23/cyber-forces-wrap-up-deployment-to-albania-in-response-to-iranian-cyberattacks/.

Prokupecz, Shimon, Tal Kopan, and Sonia Moghe. "Former Official: Iranians Hacked into New York Dam." *CNN*, December 22, 2015, https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html.

Raved, Ahiya. "Cyber Attack Targeted Israel's Water Supply, Internal Report Claims." *Ynet*, April 26, 2020, https://www.ynetnews.com/article/HJX1mWmF8.

Reuters. "Aramco Says Cyberattack Was Aimed at Production." *New York Times*, December 9, 2012, https://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html.

Ribeiro, Anna. "FBI Reveals Iranian Cyber Group Emennet Pasargad Executing Hack-and-Leak Operations Using False-Flag Personas." *Industrial Cyber*, October 21, 2022, https://industrialcyber.co/critical-infrastructure/fbi-reveals-iranian-cyber-group-emennet-pasargad-executing-h.

Rid, Thomas. *Cyber War Will Not Take Place.* London: C. Hurst and Co, 2013.

Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *The Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

Ropek, Lucas. "Hezbollah-Linked Cyber Unit Has Been Hacking Into Internet Companies for Years." *Gizmodo*, January 29, 2021, https://gizmodo.com/latest?startTime=1611974820316.

Rosenberger, Laura. "Making Cyberspace Safe for Democracy." *Foreign Affairs* (May/June 2020), https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Rubenstein, Roi. "Report: Iranian Bot Army Trying to Influence Israeli Elections." *Ynet*, January 31, 2019, https://www.ynetnews.com/articles/0,7340,L-5455991,00.html.

Ruble, Kayla. "Syrian Hackers Hijack IDF Twitter Sparking Fears of Nuclear Leak." *Vice*, July 17, 2014.

Sanger, David E. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Crown, 2018.

Sanger, David E. and Julian E. Barnes. "United States Indicts Iranian Hackers in Voter Intimidation Effort." *New York Times*, November 18, 2021, https://www.nytimes.com/2021/11/18/us/politics/iranian-hackers-voter-intimidation-indicted.html.

Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." *New York Times*, January 2, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Satter, Raphael. "AP Exclusive: Iran Hackers Hunt Nuclear Workers, US Targets." *Associated Press*, December 13, 2018, https://apnews.com/article/0d4dcaab0e134cf6a1c6ce6be3b7b6a8.

Schneier, Bruce. "8 Ways to Stay Ahead of Influence Operations." *Foreign Policy* (August 12, 2019), https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

Schroeder, Stan. "CIA, FBI, NSA: We Don't Recommend Huawei or ZTE Phones." *Mashable*, February 14, 2018, https://mashable.com/article/nsa-fbi-cia-huawei.

Schweitzer, Yoram, Gabi Siboni, and Einav Yogev. "Cyberspace and Terrorist Organizations." *Military and Strategic Affairs* 5, no. 3 (2013): 17–26.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Ages*. New York: Public Affairs, 2017.

Shahaf, Tal. "Israel Unprepared for Iranian Attack on Water Supply, Officials Warn." *Ynet*, February 17, 2021, https://www.ynetnews.com/article/rJW2Cjcb00.

Shakil, Sana. "Cyber Attacks by Iran Hackers on Rise." *New Indian Express*, March 6, 2022, https://www.newindianexpress.com/thesundaystandard/2022/mar/06/cyber-attacks-by-iran-hackers-on-rise-2426859.html.

Shamah, David. "How Israel Police Computers Were Hacked: The Inside Story." *Times of Israel*, October 28, 2012, https://www.timesofisrael.com/how-israel-police-computers-were-hacked-the-inside-story/.

___. "Official: Iran, Hamas Conduct Cyber-Attacks Against Israel." *Times of Israel*, August 13, 2015, https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

Shamir, Ron and Eli Bahar. "Defending Israel Elections from Cyber Attack – What Should Be Done?" Policy Study (Israel Democracy Institute) 136 (January 2019) (Hebrew).

Shane, Scott and Ronen Bergman. "New Report Shows How a Pro-Iran Group Spread Fake News Online." *New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html.

Shkolnik, Michael and Alexander Corbeil. "Hezbollah's 'Virtual Entrepreneurs': How Hezbollah is Using the Internet to Incite Violence in Israel." *CTC Sentinel* 12, no. 9 October 2019, https://ctc.westpoint.edu/hezbollahs-virtual-entrepreneurs-hezbollah-using-internet-incite-violence-israel/.

Siboni, Gabi, Léa Abramski, and Gal Sapir. "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy." *Cyber, Intelligence and Security* 4, no. 1 (2020): 21–40.

Siboni, Gabi and Sami Kronenfeld. "Iran and Cyberspace Warfare." In *Cyberspace and National Security – Selected Articles*, edited by Gabi Siboni, 81–103. Tel Aviv: INSS, 2013.

Siddiqui, Zeba. "Iran Behind Hack of French Magazine Charlie Hebdo, Microsoft Says." *Reuters*, February 3, 2023, https://www.reuters.com/business/media-telecom/iran-behind-hack-french-magazine-charlie-hebdo-microsoft-says-2023-02-03/.

Silber, Jonathan. "Cyber Vandalism – Not Warfare." *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

Siman-Tov, David and Shmuel Even. "A New Level in the Cyber War between Israel and Iran." *INSS Insight* no. 1328, June 3, 2020.

Siman-Tov, David and Ohad Zaidenberg. "Influence Operations: A Combination of Technological Attacks and Content Manipulation." *INSS Special Publication*, March 11, 2021 (Hebrew), https://www.inss.org.il/he/publication/cyber-attack-and-manipulations/.

Sinoruka, Fjori. "FBI: Iranian Hackers Accessed Albanian Systems Over Year Ago." *Balkan Insight*, September 22, 2022, https://balkaninsight.com/2022/09/22/fbi-iranian-hackers-accessed-albanian-systems-over-year-ago/.

Solomon, Shoshana. "Israeli Entrepreneur Calls for NATO-Style Cybersecurity." *Times of Israel*, January 31, 2018.

Spadoni, Giacomo. "IRGC Cyber-Warfare Capabilities." Herzliya: International Institute for Counterterrorism (ITC), 2019, https://ict.org.il/UserFiles/IRGC%20Cyber-Warfare%20Capabilities.pdf.

Springer, Paul J. *Encyclopedia of Cyberwarfare*. ABC- Clio, 2017.

Staff. "Iranian Cyberattacks on Israeli Facilities Thwarted for a Year – Report." *Jerusalem Post*, June 7, 2020, https://www.jpost.com/breaking-news/iranian-cyber-attacks-on-israeli-water-facilities-thwarted-for-a-year-report-630592.

Starks, Tim. "An Iranian Hacking Group Went on the Offensive Against US Targets, Microsoft Says." *Washington Post*, April 18, 2023.

___. "Russia, China and Iran Trying to Hack Presidential Race, Microsoft Says." *Politico*, September 10, 2020, https://www.politico.com/news/2020/09/10/russia-china-iran-cyberhack-2020-election-411853.

Statista. "Estimated Cost of Cybercrime Worldwide 2017-2028." https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/.

___. "Forecast Number of Mobile Devices Worldwide from 2020 to 2025 (in Billions)." https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/.

___. "Share of households with a Computer at Home Worldwide from 2005 to 2019." https://www.statista.com/statistics/748551/worldwide-households-with-computer/.

Stickings, Tim. "Berlin Security Service Blames Iran for Cyber Attack on German Companies." *The National News*, May 12, 2021, https://www.thenationalnews.com/world/europe/berlin-security-service-blames-iran-for-cyber-attack-on-german-companies-1.1221570.

Stott, Paul. *Iranian Influence Networks in the United Kingdom: Audit and Analysis*. Henry Jackson Society, June 2021, https://henryjacksonsociety.org/wp-content/uploads/2021/06/HJS-Iranian-Influence-Networks-in-the-UK-Report-HR-web-1.pdf.

Straub, Jeremy. "Hackers Could Kill More People than a Nuclear Weapon." LiveScience.com, August 27, 2019, https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html.

Stub, Zev. "Newly-Found Iranian Cyber-Espionage May Pose 'Real Threat' to Israel." *Jerusalem Post,* October 7, 2021, https://www.jpost.com/jpost-tech/newly-found-iranian-cyber-espionage-may-pose-real-threat-to-israel-681196.

Stubbs, Jack and Christopher Bing. "Exclusive: Iran-Based Political Influence Operation – Bigger, Persistent, Global." *Reuters*, August 28, 2018, https://www.reuters.com/article/us-usa-iran-facebook-exclusive-idINKCN1LD2R9.

Stubbs, Jack and Katie Paul. "Facebook Says it Dismantles Disinformation Network Tied to Iran's State Media." *Reuters,* May 5, 2020, https://www.reuters.com/article/us-iran-facebook-idUSKBN22H2DK.

Sulmeyer, Michael. *Cyberspace: A Growing Domain for Iranian Disruption*. Washington DC: Center for Strategic and International Studies, 2017.

Tabatabai, Ariane M. *Iran's Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran's Influence Operations*. Washington DC: Alliance for Securing Democracy, 2020. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/09/Irans_Authoritarian_Playbook.pdf.

Timberg, Craig, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima. "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation." *Washington Post*, August 21, 2018, https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/.

Timberg, Craig and Tony Romm. "It's not just the Russians Anymore as Iranians and Other Turn Up Disinformation Efforts Ahead of 2020 Vote." *Washington Post*, July

25, 2019, https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/.

___. "New Report on Russian Disinformation, Prepared for the Senate, Shows Operation's Scale and Sweep." *Washington Post*, December 17, 2018, https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/.

TOI Staff. "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps." *Times of Israel*, July 17, 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.

___. "Cyber Firm Says Three Iran-Run Sites are Targeting Israelis With Fake News." *Times of Israel,* September 6, 2018, https://www.timesofisrael.com/cyber-firm-says-iran-run-sites-target-israelis-with-fake-news/.

___. "Iran Duped Pakistan into Israel Nuke Threat as Tiny Part of Huge Fakery Campaign." *Times of Israel*, November 30, 2018, https://www.timesofisrael.com/iran-duped-pakistan-into-israel-nuke-threat-as-tiny-part-of-huge-fakery-campaign/.

___. "Iran Hackers Reportedly Tried to Phish Israeli Nuclear Scientists." *Times of Israel*, January 30, 2018, https://www.timesofisrael.com/iran-hackers-reportedly-tried-to-phish-israeli-nuclear-scientists/.

___. "Iran Spying on Israel, Saudi Arabia with Major Cyberattacks." *Times of Israel*, June 14, 2015, https://www.timesofisrael.com/iran-spied-on-israel-saudi-arabia-with-major-cyberattack/.

___. "Israel Behind Cyberattack that Caused 'Total Disarray' at Iran Port – Report." *Times of Israel*, May 19, 2020, https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/.

___. "Israel Publicly Blames Iran for Cyberattack on Major University Last Month." *Times of Israel*, March 7, 2023, https://www.timesofisrael.com/israel-publicly-blames-iran-for-cyberattack-on-major-university-last-month/.

___. "Website of Israeli Port Hacked; Sudanese Group Said to Claim Responsibility," *Times of Israel*, April 26, 2023, https://www.timesofisrael.com/websites-of-israeli-port-hacked-sudanese-group-said-to-claim-responsibility/.

Tokyay, Menkse. "Iran-Linked Hacker Group Targets Turkey's Cyber Network." *Arab News*, February 17, 2022, https://www.arabnews.com/node/2027016/middle-east.

Trobisch, Jan. *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm*, School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, KS, 2014.

U.S. Cyberspace Solarium Commission. *Report*, March 2020, https://www.solarium.gov/report.

U.S. Department of Homeland Security. "CISA Statement on Iranian Cybersecurity Threats." CISA.gov, January 3, 2020, https://www.us-cert.gov/ncas/current-activity/2019/06/24/CISA-Statement-Iranian-Cybersecurity-Threats.

___. "Cybersecurity Strategy." 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

U.S. Department of Justice. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guards Corps." Press Release, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

United Against Nuclear Iran (UANI). "The Iranian Cyber Threat." *UANI* (May 2020).

___. "The Iranian Cyber Threat." (September 2022), 5–8, https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat_9.7.22_JC_JMB_CMJ.pdf.

United States Institute for Peace. "Albania Cuts Ties With Iran Over Cyberattack." September 12, 2022, https://iranprimer.usip.org/blog/2022/sep/09/albania-cuts-ties-iran-over-cyberattack.

United States, Subcommittee on Emergency Preparedness, Response and Communications and the Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies. "Cyber Incident Response." 2014.

Vahdat, Amir and Jon Gambrell. "Iran Leader Says Israel a 'Cancerous Tumor' to be Destroyed." *Associated Press*, May 22, 2020, https://apnews.com/article/a033042303545d9ef783a95222d51b83.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion.* New York: Oxford University Press, 2018.

Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities.* New York: Oxford University Press, 2015.

Volz, Dustin. "FBI Chief Blames Iran for Cyberattack on Boston Children's Hospital." *Wall Street Journal*, June 1, 2022, https://www.wsj.com/articles/fbi-chief-blames-iran-for-cyberattack-on-boston-childrens-hospital-11654096382.

Volz, Dustin and Jim Finkle. "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam." *Reuters*, March 24, 2016, https://www.reuters.com/article/ctech-us-usa-iran-cyber-idCAKCN0WQ1JF.

Wakabayashi, Daisuke and Scott Shane. "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election." *New York Times*, September 27, 2017, https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html.

Watts, Clint. "Rinse and Repeat: Iran Accelerates its Cyber Influence Operations Worldwide." Microsoft.com, May 2, 2023, https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/.

Wechsler, Omree. "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East." *Council on Foreign Relations*, March 15, 2021, https://www.cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east.

Weiner, Rachel. "Iranian Men Accused of Hacking U.S. Aerospace Companies." *Washington Post*, September 17, 2020, https://www.washingtonpost.com/local/legal-issues/iranian-men-accused-of-hacking-us-aerospace-companies/2020/09/17/1a55f442-f8e7-11ea-89e3-4b9efa36dc64_story.html.

Weinthal, Benjamin. "Iran May Be Behind BDS 'Hit List' Targeting Boston Jews – Report." *Jerusalem Post*, March 5, 2023, https://www.jpost.com/diaspora/antisemitism/article-733382.

Winer, Stuart and Marissa Newman. "Iran Supreme Leader Touts 9-Point Plan to Destroy Israel." *Times of Israel,* November 10, 2014, https://www.timesofisrael.com/iran-supreme-leader-touts-9-point-plan-to-destroy-israel/.

Yaron, Oded. "Has Hezbollah's Cyber Spy Ring Been Exposed?" *Haaretz*, April 8, 2015, https://www.haaretz.com/2015-04-08/ty-article/.premium/has-hezbollahs-cyber-spy-ring-been-exposed/0000017f-e0c1-df7c-a5ff-e2fb9bec0000.

___. "Palestinians Behind Cyber Attacks on Israeli Army and Government Targets." *Haaretz*, February 16, 2015, https://www.haaretz.com/2015-02-16/ty-article/.

premium/palestinians-behind-cyber-attacks-on-israeli-targets/0000017f-dbff-d856-a37f-ffff6f160000.

Ynet reporters. "Host of Israeli Sites Targeted in Massive Cyber-Attack." *Ynet,* May 21, 2020, https://www.ynetnews.com/article/SkXO1amsU.

Ynet staff. "Report: Iran Behind Hack of Israeli Water Authority Sites." *Ynet*, May 7, 2020, https://www.ynetnews.com/article/By2gZO1198.

Young, Benjamin R. "How Iran Built Hezbollah into a Top Cyber Power." *National Interest*, April 11, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-iran-built-hezbollah-top-cyber.

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

Zimmt, Raz. "The Israeli Threat—The View From Iran." *Bein HaKtavim*, Dado Center for Interdisciplinary Military Research, forthcoming, Fall 2023.

Zitun, Yoav. "Shin Bet: Iran Tried to Enlist Israelis, Palestinians for Espionage, Terror." *Ynet*, July 24, 2019, https://www.ynetnews.com/articles/0,7340,L-5556631,00.html.

Ziv, Amitai. "Cash-Strapped Over Coronavirus, Crime Organizations Unload Cyberattacks." *Haaretz*, September 21, 2020, https://www.haaretz.com/israel-news/tech-news/2020-09-21/ty-article/.premium/cash-strapped-over-coronavirus-crime-cartels-unload-cyberattacks/0000017f-e3ac-d9aa-afff-fbfc13ab0000.

___. "Iran Suspected After Massive Cyberattack on Israeli Firms Revealed." *Haaretz*, December 13, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-13/ty-article/.premium/iran-suspected-after-massive-cyberattack-on-israeli-firms/0000017f-dbe1-df9c-a17f-fff95fab0000.

___. "'Iranian Attacker Impersonating Russians': Inside Recent Attacks on Israel." *Haaretz*, May 5, 2021, https://www.haaretz.com/israel-news/tech-news/2021-05-05/ty-article/iranians-impersonating-russians-inside-cyberattacks-on-israel/0000017f-e1e1-d7b2-a77f-e3e7baaf0000.

___. "The Iranians Read the Reports about Israel's Cyber Error, and Succeeded to Embarrass." *The Marker*, May 31, 2020 (Hebrew), https://www-themarker-com.ezproxy.bgu.ac.il/technation/2020-05-31/ty-article/.premium/0000017f-dbed-d856-a37f-ffedd3c00000.

Iran was one of the first states to formulate a national cyber strategy, including development of the necessary state institutions and technological capabilities. Today, Iran is one of the more active states in the cyber realm, near the top of the second tier of global actors. Iran's cyber attacks have demonstrated the potential to disrupt, sabotage and even destroy civil and commercial targets, critical national infrastructure and military capabilities, and its cyber espionage and information operations have been particularly extensive. Israel and the United States are Iran's primary targets.

This study presents a comprehensive and up-to-date analysis of Iran's cyber strategy, institutions and praxis. Its five parts present: a brief background on the cyber threat and what makes it different from other realms of conflict; Iran's cyber strategy and the institutions and capabilities it has developed; the primary cyber attacks Iran has conducted against the US and actors in the Middle East and around the world; the Iranian cyber threat to Israel; and an assessment of the actual impact of Iran's attacks to date, along with conclusions and policy recommendations.

Dr. Chuck Freilich, a senior researcher at INSS, served for over 20 years in Israel's national security establishment, as a senior analyst and as a deputy national security adviser. He was a long-time senior fellow at Harvard's Belfer Center and has taught political science at Harvard, Columbia, NYU and Tel Aviv Universities. Freilich specializes in Israel's national security strategy and policymaking processes, US Middle East policy and US-Israeli relations. He is the senior editor of the *Israel Journal for Foreign Affairs*.

Freilich is the author of *Zion's Dilemmas: How Israel Makes National Security Policy* (Cornell Press 2012); *Israeli National Security: A New Strategy for an Era of Change* (Oxford Press 2018); and I*srael and the Cyber Threat: How the Startup Nation Became a Global Cyber Power* (Oxford Press 2023). He has published numerous academic articles and over 220 op-eds, appears frequently in the Israeli and international media and speaks before a wide range of audiences.

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