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.