Chapter 6
The Adversarial Environment

Who are our adversaries? What do they want? Why should we be concerned now?

We are facing today a multi-pronged, multi-faceted attack on our civilization. This is not a coordinated attack by a single enemy. There are multiple national opponents, who, acting individually, are using a variety of modes of attack over broad scales of time on multiple facets of our national life. There are also many non-nation-state opponents, both external to our country and within it, who are doing the same. There are individuals and small groups of individuals, acting on economic motives, doing the same. Additionally, our social media have created an environment that fosters individual attacks. There are the traditional corporate activities that seek to further their own ends through influence operations. Together, these actors present a vast matrix of competing interests and influence and create an environment of constant conflict.

“The modern internet is not just a network, but an ecosystem of nearly 4 billion souls, each with their own thoughts and aspirations, each capable of imprinting a tiny piece of themselves on the vast digital commons. They are targets not of a single information war but of thousands and potentially millions of them (Singer & Brooking, 2018).”

This conflict involves the individual, the social organizations, the corporate organizations, and the government, using and exacerbating the changing environment. While the technium and the noosphere are the means, media, and immediate and long-term targets, the cognitive domain is the actual domain of conflict.

Much of human history is red n tooth and claw, kill and eat. Frederick the Great said, “Every man has a wild beast within him.” “The question is what releases the beast (Wrangham, 2019).” We humans “have a rare and perplexing combination of moral tendencies. We can be the nastiest of species and also the nicest.” “Peace at home and war abroad” is not rare. “We now recognize that aggression comes in not one but two major forms, each with its own biological underpinnings and its own evolutionary story.” “Reactive (hot, defensive, or impulsive) aggression is a response to a threat.” Proactive aggression (cold, premeditated, offensive) is the aggression of
war (coalitionary proactive aggression) or the deliberate aggression of the socio-path, or, at times, the offended and unrestrained. The proactive individual protagonist typically acts when he can “assess a high likelihood of cost free success.” It is essential that those charged with our security and defense clearly understand that we are low on the scale of one type of aggression (reactive aggression) and high on the other type (proactive aggression) and that “the separate nature of proactive and reactive” aggression helps to explain warfare. Methods of influence, prediction and furtherance of human violence are extant and can be used for dissociative ends (Wrangham, 2019).

**Adversaries**

Adversaries come in many configurations and sizes. All contribute to the environment of conflict in the noosphere and technium.

**Individuals**

Individuals range from the perpetrators of individual defamatory attacks on others to swindlers or the hackers who use their skills to attack the computers of others. The resources of individuals range from having an account on social media to access or control of thousands of computers, with funding ranging from pocket change to millions of dollars.

Malicious individuals or groups may act on their own or may be associated, either informally or formally as proxies, with groups, corporations, or governments. These individuals may penetrate all of the layers of security or may start from a privileged position within a corporation, such as a recent case in which an employee of Amazon’s cloud division is reported to have stolen more than 100 million customers’ data from the Capital One data stored in the Amazon cloud (Mattioli, McMillan, & Herrera, 2019). Another privileged position is created by the creators of applications (apps) that perform useful functions either on smartphones or in web browsers. Some browser apps, called browser extensions, have been found to conduct surveillance. They sell information on “where you surf and what you view into a murky data economy … to be harvested for marketers, data brokers or hackers (Fowler, 2019a).”

**Groups**

Some groups are civic organizations with a benevolent public agenda. There are also both organized groups and loose affiliations of hackers. There are groups who use the Internet almost exclusively and groups who use it to aid their real-world
activism. Clarke and Knake labeled the worst of these groups “advanced persistent threats (APT)” because they are not only highly capable, but also steadfast in their efforts (Clarke & Knake, 2019). Group resources can be expected to be generally larger than individual resources.

**Companies**

Virtually all companies advertise. Some companies engage in industrial espionage. Some companies are captive instruments of their governments and some hold governments captive. Corporate resources can be enormous, with many having millions or billions of dollars in available funds, with commensurate technical resources.

Recently, social media companies have provided a special concern. As described earlier, social media provide vehicles for influence attacks and have been accused of fostering their own agendas in influence operations (McNamee, 2019). However, in an opinion article, Andy Kessler of the Wall Street Journal argued that these risks are exaggerated. He argued that the social media themselves are training people to be more alert to these attacks and more discerning in their acceptance of fake news. He said that, “For all its flaws, social networks and artificial intelligence keep delivering value and utility to users, training people for a world that moves in nanoseconds. Better to teach the next generation how to keep up (Kessler, 2020).” This debate continues.

**Non-State Actors**

Non-state actors are groups that have ambitions in the international arena, some acting independently and some acting as proxies. Some are supposed to be benign, such as United Nations organizations, and some are distinctly malignant, such as Al Qaeda. The resources of most non-state actors are comparable to those of general groups, although some have very large funding bases.

“‘Terrorism is theater,’ declared RAND Corporation analyst Brian Jenkins in a 1974 report that become one of terrorism’s foundational studies. Command enough attention and it didn’t matter how weak or strong you were: you could bend populations to your will and cow the most powerful adversaries into submission (Singer & Brooking, 2018).” “ISIS’s legacy will live on long after the group has lost all its physical territory, because it was one of the first conflict actors to fuse warfare with the foundations of attention in the social media age. It mastered the key elements of narrative, emotion, authenticity, community, and inundation [emphasis in the source] (Singer & Brooking, 2018).” (Authenticity means engendering the belief that the persona of the social media person is really that of the real-life person animating the social media person.)
**Nation-States**

Nation-states have full access to national funding. Their technical and financial resources can be huge. Their goals can range from gaining economic advantages to global dominance. Their methods can range from theft of intellectual property to industrial espionage to war. For some countries, divining intent from methods can be difficult. A translated Chinese document titled *Unrestricted Warfare* made this clear. Their methods for war include, lawfare (using and bending laws to advantage), “hacking into websites, targeting financial institutions, using the media, and conducting terrorism and urban warfare (Qiao & Wang, 1999).”

The U.S. Department of Defense cyber strategy said, “We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation’s economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States’ growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation (Department of Defense, 2018).”

**Digital Adversaries**

Singer and Brooking added an additional type of adversary. “The way the Internet affects its human users makes it hard enough for them to distinguish truth from falsehood. Yet these 4 billion flesh-and-blood netizens have now been joined by a vast number of digital beings, designed to distort and amplify, to confuse and distract. The attention economy may have been built by humans, but it is now ruled by algorithms—some with agendas all their own (Singer & Brooking, 2018).”

**Goals and Intents**

The goals and intents of the adversaries are various and differ within types of adversaries as well as between them. However, some categories of goals and intents are common among adversaries.
**Personal Enmity**

Some people take advantage of social media to conduct personal attacks. They are acting on personal enmity.

Other adversaries seek to create enmity. Singer and Brooking, explaining emotion and purpose of trolls, repeated the words of a well-known troll, ‘Ironghazi,’ who explained, “‘The key to being a good troll is being just stupid enough to be believable, keeping in mind that the ultimate goal is making people mad online (Singer & Brooking, 2018).’”

**Influence**

The desire to gain attention and influence is common among many types of adversaries. Their actions may seek current influence or be positioned for the future.

**Individual and Group Influence**

Malicious individuals and groups may seek to influence their targets to gain current access. Or they may use influence as an indirect means to further their ultimate goals.

**Corporate Influence**

Generally, companies use advertising and similar activities to obtain influence, leading to economic gains. Some companies, such as Google and Facebook, have privileged positions with respect to external data, gathering enormous amounts of personal data from their users. They also are in the information business, selling access to users and their data. Some have been accused of using their positions to exercise political influence on their users (Copeland, 2019b). In 2019, Rep. Tulsi Gabbard, a candidate for the Democrat nominee for President in 2020, accused Google of censoring her by suspending her advertisements (Carlson, 2019).

Singer and Brooking described a company, Breitbart, acting to increase influence, “Bannon embraced social media as a tool to dominate the changing media marketplace, as well as to remake the right-wing. The modern internet wasn’t just a communications medium, he lectured his staff, it was a ‘powerful weapon of war,’ or what he called ‘#War’ (Singer & Brooking, 2018).”
National Influence

Sean McFate cited the Russian Troll Factory, illustrating that the power of cyber-warfare lies in delivering disinformation. “Trolls are anonymous agents provocateur that stalk the internet, throwing seditious hand grenades into chatrooms and on news sites (McFate, 2019).”

Michael Pillsbury described the Chinese use of shi in its hundred-year war to replace America as the global superpower. China has been positioning itself and using influence over others to create a situation that will yield Chinese influence over future events (Pillsbury, 2015).

The U.S. also seeks influence. For example, as Lt Col Patrick McClintock said in a National Defense University capstone report, “The US conducts and supports [Humanitarian Assistance/Disaster Relief] HA/DR operations in the Indo-Pacific to: (1) provide humanitarian relief that alleviates suffering, (2) create a positive image of the US and its military among leaders and inhabitants of the region, (3) build relationships and advance military interoperability with other countries and militaries that support US regional presence, (4) lay the foundation for other forms of security cooperation, and (5) demonstrate the US military’s commitment to allies and partners, to include exposing them to new capabilities (e.g., strategic airlift) (McClintock, 2020).”

Surveillance (the Panopticon)

Clearly, almost ubiquitous surveillance exists now. All of our social media are analyzed for use by the companies who own the social media; devices like Alexa require AI analysis to produce the desired answers and actions; our newest televisions have voice activated controls, which require similar surveillance and analysis; we can expect our security cameras to be merged into systems, perhaps with external surveillance and analysis; and companies are selling refrigerator surveillance systems!

An article on the front page of the Wall Street Journal in November of 2019 was titled, “Google Amasses Personal Medical Records.” The article described how one of the largest health-care systems has teamed with Google to “collect and crunch the detailed personal-health information of millions of people across 21 states.” “The data involved in the initiative encompasses lab results, doctor diagnoses and hospitalization records, among other categories, and amounts to a complete health history, including patient names and dates of birth.” “Neither patients nor doctors have been notified (Copeland, 2019a).” The purpose is to improve health care. However, other benefits are certainly expected by the two parties to accrue to themselves.

Big Brother can be a nation-state or a corporation. However, integrating these various data sources will yield more profitable results than any one stand-alone data feed. The enormous quantity of data spanning all aspects of personal life will pro-
vide excellent input for big data analytics and AI/ML processing, prediction and influence. China is internally deploying that integration now (Lee, 2018).

Today your smartphone tracks your location and reports it to various recipients (depending on the apps you have installed and the connections they make to third parties). If you turn off the tracking feature, your phone still records your locations (with times). When you turn the tracking feature back on, your phone uploads the history of your locations to the recipients so that they have all the information they would have had if you had not ever turned tracking off. If you have any medical apps that record history, these apps may be sending the information to multiple places. If you use a browser on your phone, this information is recorded and sent. Probably there are things you do on your phone today that are not recorded and disseminated. You can assume that one day everything you do on your phone may be disseminated to someone.

If your computer is connected to the Internet, many of your activities are recorded and disseminated. You can assume that one day, unless your computer is never connected to the Internet, everything you do or say (assuming your computer has a microphone and camera) with or around your computer may be recorded and disseminated.

If you have a smart TV, smart appliances, new car, or Internet connected security system, you can assume eventually everything may be recorded and disseminated. Eventually, everything in your house will be “smart.” Already it is difficult to buy a “dumb” TV.

If you purchase groceries or gas with a store-affiliated card, all of your purchases are recorded. That’s how they know to send you those nice coupons that correspond to the things you buy frequently. Credit card companies not only know where you use them and how much you spend, but they also know what these purchases mean—your bill shows the expenses categorized by things such as food, entertainment, and travel.

In the future, you can expect that someone will know everything that you do and draw conclusions about your activities. (Currently, it is possible to live “off the grid;” however, there are places now that don’t accept cash. It will get harder.) Right now, the things about you that someone knows are divided among multiple corporations and the government (unless you live in China, where it is all being collected by the government (Lee, 2018)). No one knows when or if the current division of knowledge about you will be consolidated. That will be the arrival of the Panopticon.

In the United States, there is some push-back against state surveillance. In an article in the Wall Street Journal, Restuccia and Volz described discussions concerning an overhaul of the program that surveils U.S. citizens suspected of posing national-security risks. The Foreign Intelligence Surveillance Act (FISA) was first adopted after Watergate and modified by the post-9/11 Patriot Act. It codifies this type of surveillance. The abuses that took place before and after the Trump inauguration are motivating these concerns (Restuccia & Volz, 2020).
**Economic Gain**

There are individuals and groups who use conventional telephone calls, email, and social media to extort money from others using various swindles. Malicious individuals act for economic gain by using such tools as ransomware for direct economic gain and obtaining control of insufficiently protected computers to support economic motives indirectly.

Information brokers exist, as do companies selling political persuasion services. These entities use data collected through surveillance as the commodity they sell.

Corporations have both external and internal rationales for engaging in information activities. External reasons include acquisition and prevention of the acquisition of economic, scientific, and personal data. The acquisition of external data includes data acquisition from other corporations, governments, selective scientific advances, and customers or potential customers. Internal reasons include acquisition of personal data on employees for business improvement, control of employees, and prevention of internal data theft or other malicious activities. These may all be classified as driven by a desire for economic gain.

**Philosophical and Ideological Motives**

Malicious individuals act for ideological reasons (such as antipathy toward corporations or governments).

**Maliciousness**

There are individuals who act maliciously to display their prowess or create havoc as an enjoyable activity.

**Control of Society**

Nation-states have both external and internal rationales for engaging in information activities, both offensive and defensive. External reasons include acquisition and prevention of the acquisition of military, economic, scientific, and personal data. External reasons can include influence, coercion or control of other countries. Internal reasons include the acquisition of personal data for defensive reasons, such as identification of spies, terrorists and common criminals, and for the control of internal populations and groups.
One reason for intentional conflicts can be stated as “control of society.” The commercial version is controlling actions for profit. The national version is controlling society for power or “for its own good.” In this communications age, control of society begins with control of the narrative. (Histories describe wars for the control of territory sometimes as if one day a king decided to conquer his neighbor and then set out to do so. However, we suspect that the king generally had to prepare the ground to get his followers to engage in the war. Thus, the king had to try to create and control the narrative.)

Singer and Brooking discussed the Chinese view of internal control. “Mao [Zedong] envisioned a political cycle in which the will of the masses would be refracted through the lens of Marxism and then shaped into policy, only to be returned to the people for further refinement.” “To achieve this goal, even stronger programs of control lurk on the horizon. In the restive Muslim-majority region of Xinjiang, residents have been forced to install the Jingwang (web-cleansing) app on their smartphones. The app not only allows their messages to be tracked or blocked, but it also comes with a remote-control feature, allowing authorities direct access to residents’ phones and home networks. To ensure that people were installing these ‘electronic handcuffs,’ the police have set up roving checkpoints in the streets to inspect people’s phones for the app (Singer & Brooking, 2018).”

“The most ambitious realization of the mass line, though, is China’s ‘social credit’ system. Unveiled in 2015, the vision document for the system explains how it will create and ‘upward, charitable, sincere and mutually helpful social atmosphere’—one characterized by unwavering loyalty to the state. To accomplish this goal, all Chinese citizens will receive a numerical score reflecting their ‘trustworthiness … in all facets of life, from business deals to social behavior (Singer & Brooking, 2018).’” Buckley warned that social credit could come to the United States (Buckley, 2019).

Concerning Russia, Singer and Brooking discussed its methodologies for internal control. “Since Putin consolidated power in 1999, dozens of independent journalists have been killed under circumstances as suspicious as those that have befallen his political opponents (Singer & Brooking, 2018).” “The outcome has been an illusion of free speech within a newfangled Potemkin village. ‘The Kremlin’s idea is to own all forms of political discourse, to not let any independent movements develop outside its walls,’ writes Peter Pomerantsev, author of Nothing is True and Everything is Possible. ‘Moscow can feel like an oligarchy in the morning and a democracy in the afternoon, a monarchy for dinner and a totalitarian state by bedtime (Singer & Brooking, 2018).’”

Singer and Brooking continued with Russia’s external efforts. “But importantly, the [Potemkin] village’s border no longer stops at Russia’s frontier.” “The aim of Russia’s new strategy, and its military essence, was best articulated by Valery Gerasimov, the country’s top-ranking general at the time.” Gerasimov delivered a speech saying, “the role of nonmilitary means of achieving political and strategic goals has grown. In many cases, they have exceeded the power of force of weapons in their effectiveness (Singer & Brooking, 2018).”
Hvistendahl, writing in *Science*, discussed the Chinese government’s efforts at societal control (Hvistendahl, 2018). China is using modern digital surveillance techniques to instrument the infrastructure, together with systems analysis and other sophisticated analysis techniques, to effect control of its society. Microsoft is worried about the use of facial-recognition software and is urging governments to regulate its use, especially to prohibit “ongoing surveillance of specific people without a court order (Greene & MacMillan, 2018).” This same article called out China, “where the government uses it [facial-recognition] extensively for surveillance.”

In 2014, Alex Pentland wrote the book *Social Physics* about an attempt to develop a science of how humans behave in society. Part of the book details extremely large data collection experiments using cell-phone type technology to monitor millions of person hours of activities. The point of the book is that such data can be used to design corporate and city environments (Pentland, 2014). During the COVID-19 pandemic, use of cell-phone tracking has been proposed for use in “contact tracing” to help reduce the spread of infection. However, it has been also argued that this could be used to monitor and control the spread of ideas (Servick, 2020).

### War

Intentional conflict up to and including war can be direct or indirect, momentary or a marathon, monothetic or polythetic, overt or covert, and fixed or adaptive. It can involve any of the actor pairs shown in Table 6.1.

David Sanger described the current U.S. thinking, “In almost every classified Pentagon scenario for how a future confrontation with Russia and China, even Iran and North Korea, might play out, the adversary’s first strike against the United States would include a cyber barrage aimed at civilians. It would fry power grids, stop trains, silence cell phones, and overwhelm the Internet. In the worst-case scenarios, food and water would begin to run out; hospitals would turn people away. Separated from their electronics, and thus their connections, Americans would panic, or turn against one another (Sanger, 2018b).”

Christian Brose in his book *The Kill Chain* described a conversation in which a former Pentagon official said about war games, “When we fight China or Russia,

| Table 6.1 Conflict actor pairs |
|--------------------------------|
| Nation versus nation (direct or via proxies), |
| Faction or corporation versus nation, |
| Faction or corporation versus faction or corporation, |
| Individual versus nation, |
| Individual versus faction or corporation, or |
| Some combination of the above. |
blue [our side] gets its ass handed to it. We lose a lot of people. We lose a lot of equipment. We usually fail to achieve our objective of preventing aggression by the adversary (Brose, 2020b)."

These scenarios do not look as incredible now as they once did. As this book is being written, the COVID-19 pandemic is beginning to wane in the U.S.; however, the economic effects of the shutdown, initiated to fight the pandemic, are just beginning to be felt. The repercussions have not yet been assessed, but already can be measured in the trillions of dollars. Because this was a voluntary shutdown, infrastructure is untouched. A cyberattack is capable of destroying generators and large power transformers (LPT) (Clarke & Knake, 2019). According to a Department of Energy report on large power transformers, the average lead time for a single LPT is between five and 16 months and only 15% of them are made in the U.S. The cost for each LPT ranges from $2 to $7.5 million, plus transportation and installation, for another 25–30% (an LPT can weigh 410 tons) (U.S. Department of Energy Infrastructure Security and Energy Restoration Office of Electricity and Energy Reliability, 2012). The situation for generators is similar. A major cyberattack would not destroy just one or two LPTs and generators—it would destroy hundreds and thousands of them. The United States would be without electric power for at least a year.

An article in the MIT Technology Review described a contract to be awarded for cloud computing for the U.S. Department of Defense, worth up to $10 billion. Potential winners of the contract included Amazon, Microsoft, Oracle, and IBM (Weinberger, 2019). (As of March 13, 2020, the contract had been awarded to Microsoft; however, the Department of Defense had asked a judge to let it reconsider the award (Feiner, 2020).] Traditional defense contractors, such as Lockheed Martin, Boeing and Raytheon are known for producing weapons, which Sean McFate (below) believes will be or already are of little importance in the new wars; however, information will be critical. The bidders for this and similar contracts may become the new powers in defense contracting.

New Rules (or No Rules)

Sean McFate believes the old method of warfare, conventional war, is obsolete. In his book, The New Rules of War, he described how war as actually practiced differs from conventional war. For example, he said, “there is no such thing as war or peace—both coexist, always.” By this he meant that actors are working to push the limits to obtain their objectives, using methods that fall short of acts that provoke adversaries into declaring war. He claimed, “technology will not save us,” and “the best weapons do not fire bullets.” Purchasing more sophisticated and expensive weapons will not win wars, but persuasion will (where brute force is not desirable). Shadow wars will be frequent, in which forces wage war but use narrative warfare to obscure the identity of the principal actor and even that a war is taking place (McFate, 2019).
Current wars are using mercenaries (contractors) and this trend will grow. The concept of nation states as the sole actors capable and allowed (by international law) to wage war (the Westphalian Order) has become obsolete. Many of the approximately 194 nations recognized today are nations in name only. Many are narco-states, run by fabulously wealthy drug organizations, or states run by warlords as their personal adjuncts, or essentially lawless areas, denoted by names and boundaries for reference purposes and historical reasons, but not acting as nation-states serving a populace. Corporations and individual billionaires can afford to hire armies and wage wars as they see fit (McFate, 2019).

Kilcullen provided an important image of something he calls competitive control:

“Insurgents make fish traps, as do militias, gangs, warlords, mass social movements, religions (Jesus, for instance, called his apostles to be ‘fishers of men’) and, of course, governments. Like real fish traps, these metaphorical traps are woven of many strands—persuasive, administrative, and coercive. Though each of the strands may be brittle, their combined effect creates a control structure that’s easy and attractive for people to enter, but then locks them into a system of persuasion and coercion: a set of incentives and disincentives from which they find it extremely difficult to break out (Kilcullen, 2013).”

David Sanger opened his book, The Perfect Weapon, saying, “A Year into Donald J. Trump’s presidency, his defense secretary, Jim Mattis, sent the new commander-in-chief a startling recommendation: with nations around the world threatening to use cyberweapons to bring down America’s power grids, cell-phone networks, and water supplies, Trump should declare he was ready to take extraordinary steps to protect the country. If any nation hit America’s critical infrastructure with a devastating strike, even a non-nuclear one, it should be forewarned that the United States might reach for a nuclear weapon in response.” “Trump accepted Mattis’s nuclear recommendation without a moment of debate (Sanger, 2018b).”

“Detecting” War

On a national level, how does a nation determine when malware attacks [or other information attacks] rise to the level of war, even if not officially declared as such by the opposition? In an article in the New York Times, David Sanger said, “State-sponsored Russian hackers appear far more interested this year in demonstrating that they can disrupt the American electric utility grid than the midterm elections, according to United States intelligence officials and technology company executives (Sanger, 2018a).” Two articles in The Wall Street Journal described hacking attacks attributed to the Chinese and potential communications grid problems from Chinese equipment (Lubold & Volz, 2018; Taylor & Germano, 2018). The hacking involved theft of classified information and weapons plans. The potential communications problems involved the use of Chinese-made telecommunications equipment in national networks. Visner described two events as cyber weapons testing: the 2014 North Korean attack on Sony Pictures, in which a hacker group released confidential personnel information and copies of unreleased films and employed malware to erase Sony computer files; and the 2014 unattributed attack on a German
steel mill, in which malware was introduced into the industrial control systems, causing an explosion and significant damage (Visner, 2018). In his book, *The Perfect Weapon*, Sanger said, “After a decade of hearings in Congress, there is still little agreement on whether and when cyberstrikes constitute an act of war (Sanger, 2018b).”

Visner described sovereignty problems in differing views of cyberspace (Table 6.2) (Visner, 2018).

Visner drew some inferences, “If cyberspace is sovereign territory, can a state acquire more of it? Can cyberspace be governed and controlled? How can it be acquired? By force? We know Russia tried to influence US elections. If Russia was successful in influencing US elections by ‘seizing’ cyberspace, was that a military victory? What has Russia gained? What have we lost?”

Visner also discussed the thinking of Dr. Joseph Nye, the former Chairman of the National Intelligence Council, who described the world as a three-level chessboard. At the first level, information technology (IT) is applied through military power, where the US remains the dominant leader (although not unchallenged). Here the barriers to entry are high. At the second level, IT is applied in the world of commerce, which is multi-polar. Middle range powers are able to overcome the barriers to entry here. At the third level, IT is available to groups and individuals, with no one dominant. The barriers here are incredibly low and shrinking. According to Visner, Dr. Nye argued that US policy-makers and decision-makers need to understand the use of the last two levels and the power in them. The reason is that in the past it was believed that the nation with the largest military would prevail in conflict, but that in the information age it could be the state—or non-state actor—with the best story that prevails.

“Today, online battles are no longer just the stuff of science fiction or wonky think tank reports, but an integral part of global conflict. As a result, governments around the world have begun to adapt to it. Russia is the most obvious example—a government whose state media, troll factories, and botnets all conspire to wage (in the words of its own military doctrine) ‘global information warfare.’ Echoing the

| Table 6.2 Sovereignty and cyberspace |
|-------------------------------------|
| For the US and western democracies, cyberspace is a global commons |
| We operate in cyberspace |
| We defend cyberspace—personal information, intellectual property, business, research, infrastructure, our military operations |
| We even fight in cyberspace (Department of Defense, 2015) |
| We don’t “own” cyberspace |
| Think of the Law of the Sea—in this instance, we control cyber assets in our physical space |
| Beyond territorial waters—universal jurisdiction |
| For China, Russia, and possibly others: |
| Cyberspace is territory in which the government has sovereign prerogatives |
| Cybersecurity is about defending the state’s legitimacy and the government’s sovereign prerogatives |
language of ISIS propagandists, Russian military strategists describe how a strong information offensive can have a strategic impact on a par with the release of an atomic bomb.” “[T]he Russian government doesn’t resort to netwar because it wants to. Rather, it sees no other choice. The best defense, after all, is a good offense (Singer & Brooking, 2018).”

China

The noted historian Keegan said, “Oriental warmaking … is something different from and apart from European warfare it is characterized by … evasion, delay and indirectness … wearing down the enemy.” “It includes the ideological and intellectual (Keegan, 1994).”

“Since 2003, the Chinese military has followed an information policy built on the ‘three warfares’: psychological warfare (manipulation of perception and beliefs), legal warfare (manipulation of treaties and international law) [lawfare], and public opinion warfare (manipulation of both Chinese and foreign populations) (Singer & Brooking, 2018).”

Holly South, in a National Defense University capstone report, discussed China’s use of arms sales to gain influence over other countries, not only in South Asia, but also in Africa. For example, she said, “China made its first arms transfer to Djibouti in 2014. A year later, negotiations began for China’s first overseas naval base in the country. China made additional transfers in 2015 and 2016 prior to the base formally opening in 2017 (South, 2020).”

Brose, in The Kill Chain, described a scenario he and his boss, Senator McCain, conceived. In this scenario, some kind of incident with the Chinese precipitated an escalation to war. The Chinese would employ cyberattacks and antisatellite actions early. They would then proceed to defeat our kinetic forces. The argument is that we depend on very expensive platforms (ships, aircraft, etc.) for our military operations. Because they are so expensive, we have relatively few of them. Brose argued that China has achieved technical parity (or nearly so) and that its numbers of less expensive weapons, together with an aggressive pace of operations would overwhelm and defeat our forces in detail (Brose, 2020b). This scenario was just a thought experiment. However, it is a plausible one.

Of special note is the Chinese government’s effort called “military-civil fusion” that aims to harness advances from China’s tech sector for military might. The larger goals are evident in its entanglement with iFlytek efforts toward ubiquitous interpretive surveillance fused with predictive, “prevention and control systems,” voice and facial identification, audio-visual translation technology coupled with sociometrics and biometrics (Hvistendahl, How a Chinese AI Giant Made Chatting—and Surveillance—Easy, 2020). The reach of the Chinese has become more evident in the uncovering of China’s Thousand Talents program, utilizing clandestine financial support for selected American research scientists (Mervis, 2020a).
On a larger scale, China sees the United States as a hegemonic power seeking to “encircle China with a network of offensive alliances.” “Chinese leaders believe the United States has been trying to dominate China for more than 150 years, and China’s plan is to do everything possible to dominate us instead (Pillsbury, 2015).” China’s perception is not wholly incorrect. The U.S. and its allies are working to prevent China’s domination. Captain Aaron Nye of the Royal Australian Navy, in a National Defense University capstone paper, suggested that “Australia should promote itself as a member of a “Middle Power Concert” to balance against rising US-China tensions, and to promote community and regional security building (Nye, 2020).”

Their grand marathon strategy is “relatively stable (Chinese Academy of Military Science, 2018).” It utilizes the wisdom and deception of Sun-Tsu and methods of the ancient warring states where “the only rule is that there are no rules.” It is unrestricted warfare by all possible means (Qiao & Wang, 1999). It is also described in McFate’s book, *The New Rules of Warfare* (McFate, 2019). The battlefields beyond-the-battlefield use “10,000 methods combined that transcend boundaries.” “The winner is the one who combined well (Qiao & Wang, 1999).”

The concept of *shi* is paramount. *Shi* is a principal deceptive stratagem of influencing the present for its effect in the future, often as part of a long-term zero-sum game. Spanning the psychological diplomatic cultural economic and religious domains, the matrix of conflict is combinatorial, adaptive, complex, polythetic, multi-ordinal, and nuanced. It is often trans-domain, using lawfare (the bending of law to achieve desired ends), the media, the military, ecologic warfare, and cyber techniques. The conflict utilizes proxies of many stripes, including mercenaries and temporary alliances. It steals intellectual and strategic secrets, uses narratology, persuasion science, and fake news; it is offensive and defensive, public and private. Evoking local war and conflict at scale, it creates confusion, operates semi-warfare and quasi-warfare, can be preemptive or reactive and approaches from supply and/or demand.

The “gray zone” is a relatively new term for competition below the threshold of armed conflict. (It has obvious overlaps with unconventional conflict.) China uses many techniques, as mentioned above, that lie in the gray zone. Kaleb Redden, in a National Defense University capstone paper, examined these in relation to the U.S. National Defense Strategy (NDS). He said we should “ask which elements of gray zone behavior would undermine DoD’s ability to ensure conventional deterrence and a favorable regional balance of power, either by setting conditions for regional conflict or by allowing China to take measures to make U.S. success less likely if conflict occurs.” He suggested that there are four criteria for actions of particular concern: “Activities that erode the perception of U.S. credibility among regional allies and partners”; “Non-kinetic activities that impede effective U.S. power projection”; “Activities that erode the will of the U.S. populace to intervene in a crisis”; and “Activities that erode America’s long-term technological advantages (Redden, 2020).”

China now not only publishes many more scientific papers than the United States “but its annual growth in publications is ten times that of the United States.” “China
last year likely topped the United States in overall research spending for the first time in history (Mervis, 2020b).” China is also producing more graduates in science, technology, engineering, and mathematics (STEM) than the United States and as of 2016 was building “the equivalent of one university per week.” According to the World Economic Forum, the numbers of STEM graduates for 2016 were 4.7 million for China, 2.6 million for India and 568 thousand for the United States (McCarthy, 2017).

Regarding cognitive competition, China has repeatedly announced its goal of being the dominant AI power by 2030 (Larson, 2018). Toward that end it is spending massively, developing an unrivaled size of big data sets, developing AI for education, sensing, psychometrics and sociometrics and control from kindergarten to university. AI-augmented education has become a national priority (Wang, 2019). China was the first to demonstrate the feasibility of international Quantum communication via satellite connecting China and Australia (Popkin, 2017). China obviously seeks cognitive superiority.

On the other hand, there are those who point out that China has its own problems. LtCol Nathan Packard, in a National Defense University capstone paper, concluded that “The dominant narrative within the U.S. defense establishment misunderstands the trajectory of Chinese power. In reality, critical economic, demographic, and social drivers are trending negatively for the Chinese. In the coming years, China’s economy will not meet the expectations of its population. The [Chinese Communist Party] CCP’s Great Firewall, state censorship, social credit system, and other repressive measures, are an indication of regime weakness, not strength. The current U.S. approach reduces a complex relationship to a matter of black and white. While China is certainly a strategic competitor, threat inflation impedes good strategy making by narrowing the available options and perspectives (Packard, 2020).” If this conclusion is correct, China might be weaker in the future; however, seeing this, it might be more aggressive in the short-term to counteract its internal problems.

Russia

“In early 2014, a policy paper began circulating in the Kremlin, outlining what steps Russia should take if President Victor Yanukovych, the pro-Russian autocrat who controlled Ukraine, was toppled from power. Russia had to be ready, the memorandum’s author urged, to create a new set of political conditions on the ground—to manipulate the ‘centrifugal aspirations’ of ethnic Russians, pushing them to declare independence from Ukraine. In essence, if their guy was ever forced from power, Russia had to be ready to start a war (Singer & Brooking, 2018).” And that is what happened.

The Gerasimov doctrine was openly published in 2013 (Gerasimov, 2013). “The Gerasimov doctrine combines old and new: Stalinist propaganda, magnified by the power of Twitter and Facebook, and backed up by brute force.” It was implemented in the Ukraine, “the country that has become a test-bed for techniques Russia later used against the United States and its allies (Sanger, 2018b).”
The Gerasimov doctrine is grand strategy; however, Russia is also active at the tactical end of the spectrum. Patrick Tucker wrote in Defense One about a new tool for an internet attack. Leaked Russian documents claimed that Russia has developed a botnet toolset that enables hacking of the cognified objects of the internet of things (IoT). Once hacked, these objects are coordinated as a botnet to conduct a distributed denial of service (DDoS) capable of shutting down the internet of a small country for several hours. The claims of these leaked documents have not been independently verified (Tucker, 2020). However, the existence of the Mirai botnet, used by Russia against Estonia in 2007 and cited by Rothrock as being used in a 2016 exploit that largely used internet of things devices (Rothrock, 2018) lends credence to the claims.

The United States

The authors were told that those who cannot comment “on the record” recommend that one should read David Sanger’s book, *The Perfect Weapon* (Hall, 2020). Sanger said that many of the U.S. war plans open with “paralyzing cyberattacks on our adversaries.” In lesser contingencies, such as replying to Russian cyberattacks, the U.S. could “unplug Russia from the world’s financial system; reveal Putin’s links to the oligarchs; make some of his own money—and there was plenty hidden around the world—disappear.” However, the problem would be in dealing with Russia’s responses - escalation.

Sanger said, “The irony is that the United States remains the world’s stealthiest, most skillful cyberpower, as the Iranians discovered when their centrifuges spun out of control and the North Koreans suspected as their missiles fell out of the sky. But the gap is closing (Sanger, 2018b).”

General Paul Nakasone, Commander of the United States Cyber Command (USCYBERCOMMAND), testified before the Senate Committee on Armed Services on February 14, 2019. His statement discussed the environment and mission of his command. Part of his testimony concerned changes in strategic guidance and authorities, “USCYBERCOMMAND has recently improved the scope, speed, and effectiveness of its operations with the help of legal and policy changes. I want to thank Congress for its support of DoD’s cyberspace operations as reflected in provisions of the FY19 National Defense Authorization Act (NDAA) that enhanced our agility to execute missions consistent with law. We also received updated policy guidance that, in conjunction with the NDAA provisions, significantly streamlined the interagency process for approval of cyber operations and thus facilitated recent activities (Nakasone, 2019).”

Patrick Tucker, Technology Editor for *Defense One*, in the Foreword of the November 2019 issue of *Cyber in the Era of Great Power Competition*, said, “The United States has long enjoyed supremacy in every warfare domain: on land, sea, air, and space. But the new domain of cyber is the one where the U.S. lead could erode the fastest. The barriers of entry are cheap and the rules for the use of new tools and weapons are few and difficult to enforce. Moreover, information technology
now touches everything in modern life. So the digital battles of the future will play out in the robotic weapons and vehicles of the future as well as across the phones and internet-connected devices of individuals and businesses around the world. With very little cost, it’s possible to have a huge and disturbing impact on a given nation’s physical and economic security (Tucker, 2019a).”

**Winning**

“The thread that runs through all these strange internet skirmishes is that they take place simultaneously, in the same space. Sometimes, the conflict is between feuding celebrities; other times, nations embroiled in a life-and-death struggle. Sometimes, these battles dominate social media chatter completely; other times, they pass with nary a mention.” “There aren’t two or ten of these conflicts, but many thousands, all unfolding at once and leaving no one and nothing untouched. By merely giving them our attention, we become a part of them. Like cyberwar, these LikeWars are also about hacking. But they’re not targeting computer networks—they’re targeting human minds.” “There’s one more aspect that makes them different from conflicts of the past. Anyone can fight in them, but all the combatants are equally powerless in one key, new way. For while these warriors of LikeWar each fight their own personal and global wars across the internet, they aren’t the ones writing its rules (Singer & Brooking, 2018).”

David Sanger listed some prescriptions, shown in Table 6.3 (Sanger, 2018b).

Packard’s view on China’s power trajectory (in the section on China above), is more sanguine than the views of other experts; however, he did not find the current U.S. approach to China to be effective. Table 6.4 repeats Packard’s conclusions with regard to China. His paper includes more detailed recommendations, all with regard to China; however, all appear to be more broadly applicable.

The importance of cognitive superiority, including information and persuasion, in war is ascending. War itself is changing. At its heart, war is not about breaking things and people; it is about imposing the will of one group on another. The changes in the noosphere and technium are changing the relative utility of the means of war.

| Table 6.3  | Sanger’s prescriptions for cyber security |
|------------|-----------------------------------------|
| We must acknowledge that “our cyber capabilities are no longer unique.” |
| We need a “playbook for responding to attacks, and we need to demonstrate a willingness to use it.” |
| We must “develop our abilities to attribute attacks and make calling out any adversary the standard response to cyber aggression.” |
| We need “to rethink the wisdom of reflexive secrecy around our cyber capabilities.” |
| We need to help the world to “move ahead with setting … norms of behavior even if governments are not yet ready.” |
Why Do We Care—Now More than Ever Before?

Our national history warns us about the need for preparation. We have a limited history to draw from because of the brevity of experience with the digital world, its accelerating rate of change and new scale of time, and the preference for secrecy concerning adverse experiences with the digital world. In the past, we have repeatedly been unprepared when facing wars that threatened our survival and only after significant delays did we adapt to defend and defeat the enemy. The digital “attack” will be at the speed of the electron, enormously faster than the Blitzkrieg of World War II. Our fate may be determined in nanoseconds after a clandestine polythetic prologue. Warfare, how it is waged, by whom it is waged, and its time frame have changed. We are all “newbies” and with the accelerating frontier of knowledge we will continue to be newbies. Further, the barrier to entry and scaling is lower, especially in cyberwar, biological warfare and in cognitive conflict writ large. Increasingly cognitively enabled machines and the drop in the barrier between expert knowledge and end user has changed the paradigm.

Further, in a cognitive conflict, our “near peers” (those we consider worthy of concern) consist of more than just other countries. We know of non-state actors with near-peer capabilities in cyber war and there may be others of which we are ignorant. “We’re all part of the battle.” No matter who the initial protagonists are, once the conflict is open on the Internet, any attention paid to it—by anyone—becomes part of the conflict (Singer & Brooking, 2018). The changes and rate of change in conflict have never been so mixed, so complex, so great. Kinetic superiority is no longer a certain guarantor of security. Now with multiple weapons and layers hidden by method and their “local habitation and name,” we must have cognitive superiority (Table 6.5).

Some Considerations

Some examples of persuasion efforts are relatively benign:

- That used-car salesman who wants to sell you that car.
- That politicians who wants you to vote for them.
- You want to get her to date you.
Persuasion is more and more effective and powerful than ever and the surfaces for its implementation and cycle speed of new opportunities and vulnerabilities are increasing. We live within a matrix of connectivity, with a central axis of accelerating change in the noosphere (sum of knowledge known to man), in the technium (modern system of technology), and in the expanding understanding of man. We even see change in man himself through advanced augmentations. Each of these changes allow new potential opportunities for persuasion and coercion, even control.

Man is a complex adaptive system of and within other complex adaptive systems. The currency of these systems is information, but information has been weaponized. We have information conflict with its attendant ascendancy of the importance of persuasion. Personal data has emerged as a new asset class (Hardjono, Shrier, & Pentland, 2016). According to a Harvard Business Review article, “Persuasion depends mostly on the audience (Chamorro-Premuzic, 2015).” The Panopticon, a vast array of information-gathering methods and metrics, armed with experimentation, fused with Artificial Intelligence (AI) and Machine Learning (AI/ML), human-curated conditional probabilities, and other augmented human analytics, allows would-be persuaders to know the audience. With research, surveillance and analysis, messages can be personalized (micro-targeted using new persuasion profiles) for the optimal density of learning moments (Aristotle’s propitious
moment—kairos). Surveillance and rhetoric are informed by new advances in multiple disciplines such as AI, behavioral and social psychology, social signals, captology, dynamics, and cognitive and information sciences.

Persuasion forces are ubiquitous. Possibilities exist at levels of communication from word choice to metanarrative, all simultaneously and across time, space and scale. Persuasion operates at all levels of power: political, diplomatic, commercial, military, financial, educational, and personal. The low barrier of entry into persuasion battles means there are many players. With these changes come increased connectivity and complexity, resulting in lessened predictability. This necessitates more rapid iterations of persuasion forces and counterforces. Persuasion science has joined the art of persuasion, thereby increasing effectiveness.

**Potentially Malignant**

Some persuasion efforts are potentially malignant. When the civility and argumentative complexity of public discourse declines, then trust in democratic institutions decreases. “The more polarized (and uncivil) political environments get, the less citizens listen to the content the message and the more they follow partisan cues or simply drop out of participating.” The new “science of deliberation” provides some mitigating counterforce (Dryzek, et al., 2019).

Facebook, Twitter, LinkedIn, Google, YouTube, Instagram, Snapchat and WhatsApp are among the dozens of platforms that influence directly, using persuasion science, by their default rules, and by what they crowd out. Defaults influence without visible persuasion or coercion. Social media is engineered to be addictive for massive engagement (Alter, 2018). In the book *Irresistible*, Alter sketched addictive technology’s use of compelling goals that are just beyond reach, irresistible and unpredictable positive feedback, a sense of incremental progress and improvement, tasks that become slowly more difficult, unresolved tensions that demand resolution and strong social ties (Alter, 2018). “Through the technology embedded in almost every major tech platform and every web-based device, algorithms and the artificial intelligence that underlies them make a staggering number of everyday choices for us...[even] how we consume our news...and search (Hosnagar, 2019).”

We have worried that our devices provide surfaces for surveillance and opportunities for experimentation and persuasion. Voice activated devices must listen and process words to activate. The software control for activation is designed elsewhere. Smart TVs can be created with hidden cameras so that not just conversations, but also video images could be captured to read social signals and other data. We didn’t realize that someone has just such a device, asking us to install a spying device in our own homes—and pay for the privilege of being spied upon. Figure 6.1 shows this device.

People with concerns about Facebook’s past privacy actions must have had an impact. (See Roger McNamee’s book, *Zucked* (McNamee, 2019).) The Facebook
This is fine until Facebook decides to change what it is actually doing, with or without telling the customers (perhaps embedding the change in little-viewed legalistic terms of use). Further, like all internet connected objects, if you don’t set good passwords in all the right places, Portal can be hacked.

**Malignant**

Additionally, we are seeing increasing examples of distinctively malignant persuasion efforts (internationally and nationally).
“Social media platforms have been implicated as a key vector for the transmission of fake news (Grinberg, Joseph, Friedland, Swire-Thompson, & Lazer, 2019).” Audio fakeries exist (see Montreal-based company Lyrebird) and visual fakeries are nascent (see Chinese company iFlytek) (Fontaine & Frederick, 2019). Vision is man’s dominant sense and we now live with “deepfakes,” videos altered to make it appear that a person says or does something he or she never said or did. AI-generated fake news makes truth elusive. “A machine designed to create realistic fakes is a perfect weapon for purveyors of fake news (Giles, 2018).”

Psychological Operations (PSYOPS) now operates in our world of ever accelerating changes in the noosphere and the technium (Kelly, 2016). Understanding and inducing intergroup hostility and aggression is a current topic of study (Sapolsky, 2017)! AI and machine learning (ML) are changing man’s cognitive and behavioral decision dynamics. This morphology of increased complexity and adaptive connectivity spans new communities of knowledge requiring more trans-disciplinary expertise and collective lifelong learning. This broader knowledge of those accelerating changes must be coupled with the tacit knowledge of the local complex adaptive systems, e.g. with understanding of the ecologic spheres of influence and conflict and battles for “competitive control (Kilcullen, 2013).”

### Information and Cyber Superiority

Even as AI emerges, the intelligence is not in the machine. Intelligence resides in individuals and teams with tools. “Fundamentally there are two levels of information—the lower level is comprised of what we will define as either instructive or descriptive information and the higher level contains meaning or semantics. Computers work at the lower level. We work from above (Sapolsky, 2017).”

Currently, humans using intelligence augmentation (IA) train AI systems prior to AI augmenting human intelligence—increased IA.

Given the accelerating changes in the noosphere, the technium, and therefore humans, adaptive changes in management, structure and talent will be necessary for information superiority. Some questions to be considered—are we operating to address the facts in Table 6.7?

In the domain of cybersecurity, extremely high classification levels prevail. This presents problems, as a comparison with the information security domain indicates (Table 6.8).

Certain characteristics of cyberweapons are significant (Table 6.9).

The country has to worry about more effective spying and manipulation by foreign actors. However, we also have to worry about more effective surveillance and manipulation by technology corporations, data brokers, attention merchants, and perfidious persuasive political entities.
Table 6.7 Facts about information superiority

- Knowledge is power.
- We must have superior information access at both an individual and a systems level.
- Education excellence must be a national priority.
- We must be superior at using persuasion.
- Malware implants may now make us vulnerable (the prepared battlefield).
- With increasing complexity, there will be more competing ideals and new decisions regarding balancing these ideals, e.g., control versus operational freedom.
- There is need for more agile, flexible and adaptable organizations.
- More creativity, more passionate curiosity, more questioning of defaults, and more originality is necessary.
- More multidisciplinary talent must be recruited, developed, empowered, and rewarded.
- Continuous education for all is required.
- More selective connectivity is necessary.
- Management must structure narratives and the taxonomy of information for external relations, as well as for internal use.

Table 6.8 Classification—too much and too little

| With too little security you end up dying; |
| With too much security you fail because you can’t learn or create or act quickly enough; and |
| There must be sagacity in handling these competing ideals. |

Table 6.9 Cyberweapon characteristics

- They often become ineffective after first use (if we have sharing);
- Their path through the Internet is unknown;
- The time of effect can be uncertain;
- Attribution of author/user can be problematic;
- The scale (and sometimes the nature) of the effect is uncertain;
- The collateral damage can vary from none to extensive and uncontrollable, and can include blowback; and
- Understanding and interpreting escalation dynamics of offensive cyber operations are complex and critical (Lin & Zegart, 2018).

Threat Analysis

Samuelson discussed how wargaming and analysis can complement each other in investigating cybersecurity issues (Samuelson, 2018). (This discussion is also directly applicable to the larger cognition domain.) Wargaming is a process of considering attacks and defenses by pitting two humans or groups against each other.
The process is definitely not exhaustive in considering all possibilities; however, the competition often stimulates people to create novel solutions and imagine new problems. Analysis is also a process of considering attacks and defenses; however, it is structured to either be exhaustive or to sample the entire space of possibilities with a rational plan. Analysis uses predetermined algorithms to compute results. Together, they can discover more than either can separately. Samuelson concluded, “Wargaming may offer considerable potential to identify key issues and policy options in information security. Wargaming is better suited to illuminating decision-making than to assessing technical capabilities and possibilities. Engineering analysis, ideally including penetration testing, is more appropriate as the basis for risk assessments and adjudication (Samuelson, 2018).”

Threat analysis is needed to define the nature and potency of current and possible threats. (Note that while we have emphasized the information threats, such as cyber-attacks, in this book, the threat analysis must also include kinetic threats.) We must have “foresight, for insight, for action (Johansen, 2007).” Questions to be asked are shown in Table 6.10.

Table 6.11 illustrates the concept with broad target categories in the first column and broad threat categories in the first row. The contents of the cells indicate whether the column entry is threatened by the row entry (T = target), contains the actor doing the threatening (A = Actor), or provides support for the threat (S = Support). Human actors include individuals, corporations, non-nation-state actors, and nations. This table is a sketch of a real analysis. For example, it omits information on combinations and second or third order effects.

Defense analysis consists of ongoing, iterative enumeration of the targets and defenses, estimations of the defense quality, and other useful information. Questions to be asked are shown in Table 6.12.

We will assume that the target is the entire U.S. society and its components. That is, the target includes individuals, various groups, and corporations. We must consider collateral damage to social media by bots, reducing trust, engendering legal actions, causing costly monitoring and removal, etc.

Once each iteration of the threat and defense analyses is complete, an analysis of the shortfalls is required to determine what should be done to mitigate the problems. Table 6.13 lists possible areas of concern.

| Table 6.10 | Sample threat analysis questions |
|-------------|----------------------------------|
| What weapons are aimed at which targets? |
| Who is doing what? |
| How are they doing it? |
| How competent are they? |
| What are their motives and plans? |
| What (forces, capabilities, policies, etc.) is contained in the emergent near future? |
The threats to our national security are manifold and growing. The Army Cyber Institute and Arizona State University sponsored a workshop, called Threatcasting Workshop West 2017, in May of 2017. In this workshop the participants forecast threats (threatcasting) “to create 22 futures regarding complex issues: the advancement of AI, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, the future division of work roles between humans and machines, and more (Vanatta, 2017).” The group thought about life in 10 years, taking a whole-of-society approach to envision what might happen and which organizations might take various actions in response to the changed situation. Their conclusions included the statement that “the future environment will be complex,
and the threats and attack vectors will be diverse. Therefore, our solutions must also be diverse and interconnected.”

Figure 6.2 recapitulates our overview of the adversarial environment. It shows multiple types of adversaries and attacks (counting the cognitive drain of our technological “servants” as an attack). For simplicity, the multiple targets are subsumed with a national symbol because all can have national effects. The means are varied, as are the motives. The attacks can be singular or mixed, overt or covert. The attack durations vary from nearly instantaneous to decades. The attacks may not be simultaneous when measured in a time-frame of hours; however, over periods of months to years, they can be characterized as simultaneous.