Chapter 2
The Technium: Tools and Targets of the Conflicts

Why might others have inordinate influence over you? In this chapter, we look at one of the subordinate questions: How do they exercise that power? What are the tools and targets in this influence conflict? How do the tools work and what are the target vulnerabilities?

The technium is multiordinal

The technium is technology as a whole system. “Technology is humanity’s accelerant (Kelly 2016).” Our technium is different from the technium of that during World War II and different from that of the Middle Ages and still more different from that of ancient Greece and Rome. However, our technium evolved from those of the past. The current technium supports our lives. The technium ranges from hardware tools and targets to specific computer applications to methods of personal contact to the framing of the structure and taxonomy of corporate information technologies and beyond. As Lucas Kello said, “The revolutionary potential of technology resides not in the invention itself but in its political and social effects (Kello 2017).” Multiordinal coordination may be the most difficult and the most important part of the desiderata for surviving and prospering in a changing world.

The technium contains both technology for offense and defense and the objects of society that are targets of attack. Tools consist of tangible tools, such as hardware, intangible but explicit tools, such as software, and intangible and variable cognitive artifacts from the noosphere.

In this chapter, we describe the targets of information conflict in the technium, the tools used in that conflict, and the trends of change to the technium.
The Targets in the Technium

The technium provides the medium for most of our cognitive artifacts. When our technology is attacked, our lives are affected. In some situations, the effects are immediate and personal. In other situations, the effects start in the larger society and affect us by damaging our society. In Mobile Persuasion, Fogg said, “I believe mobile phones will soon become the most important platform for changing human behavior (Fogg & Eckles 2014).”

Basic Technium Components

The technium includes the hardware and software of our lives, serving the components shown in Table 2.1.

The technium also includes the software that controls many of these services. The technium intersects with the noosphere in the area of tactics, techniques and procedures for operating the services and creating new parts of the technium.

Cognified Objects (Toward the Internet of Things)

Cognified objects are the nodes in the extant and growing internet of things. Some of the current objects in the technium differ from the corresponding objects in the technium of the past. When is a refrigerator not just a refrigerator? The answer is, “when it knows what its contents are and is connected to the Internet.” This refrigerator has become a cognified object. We have become familiar with computers being vulnerable to attacks; however, they are now not the only objects that are vulnerable.

Table 2.1 Patrons of the technium

| Transportation services, such as automobiles, trains, and planes; |
| Communications services, such as phones, radios, televisions, and computers; |
| Energy services, such as power plants, transmission lines, and refineries; |
| Healthcare services, such as doctors’ offices, hospitals, and clinics; |
| Educational services, such as schools, universities, and libraries; |
| Utility services, such as water, sewage, and power; |
| Governmental services, such as local, state, and national governments; |
| Military Services, such as air, ground, naval, and space services, including their cyber commands; |
| Personal devices, such as tools, books, and computers; and |
| The infrastructure that supports each of these. |
Direct attacks can come through the computer, directed against that computer. However, with the advent of multiply connected and cognified devices, the vulnerabilities increase. Figure 2.1 illustrates some of the vulnerable surfaces in the home office. In addition to the attack points in the computer, there are attack points in the Wi-Fi router and the local area network (LAN). Wireless phones and wireless intercoms also have attack points.

Do you have a smart TV with a voice activated remote? It is listening to you. Do you know that it is not watching you? Digital cameras are small. The bedroom shown in Fig. 2.2 also has vulnerable surfaces. A smart TV and a voice-activated remote control provide attack points. A smart phone in the bedroom also provides attack points.

Who actually designs and builds the hardware and software of these TVs? We can imagine that the Pentagon war room has a large number of big monitors for displaying information. Who built them? What capabilities are hidden in them for monitoring the watchers and capturing the information presented on the monitors? Can any of this be tunneled out of “secure” facilities? What is your level of cyber-resilience when your systems are penetrated?

The kitchen of the future (or the current kitchen for early adopters) will also have vulnerable surfaces. Figure 2.3 shows a kitchen with an Amazon Echo Alexa device and an Internet connected refrigerator. There are lots of objects that contain or can obtain valuable information. Is your refrigerator watching you? When it orders food that is getting low, who does it tell? The figure also indicates the presence of a wireless home security system, which also has attack points.
Fig. 2.2  The cognified bedroom

Fig. 2.3  The cognified kitchen
There is also your smart phone—it is always with you and it “knows” where you are and sends that information to various places. Depending on the apps you have on the phone, it passes an amazing amount of information to the apps’ home servers and also to third parties—whose identity is generally undisclosed. Some of this information is sent in real-time and some is uploaded at night. Geoffrey Fowler’s iPhone had 5400 hidden app trackers and sent “out 1.5 gigabytes of data over the span of a month. That’s half of an entire basic wireless service plan from AT&T (Fowler 2019b).”

The individual is responsible for defending against attacks at all of these points of vulnerability. Currently, each has its own password and encryption system; however, when they are linked, the linkage can bypass the individual device security systems, a situation that may not be obvious to the individual. Even a fairly sophisticated individual may be unaware of a problem or unable to figure out how to rectify it.

These familiar cognified objects are part of the civilian world. However, cognified weapons have also been proposed. Naturally, there are worries about autonomy and control of such weapons. There are also worries about the availability of bandwidth on the battlefield for operations (Tucker 2019b). Of course, there is also the worry about the weapons being hacked.

*Communication (Apropos the Technium)*

Communication spans social signals (Matsumoto, Frank, & Hwang 2013), spoken language, written language, mathematical, musical and choreographic notation, and bits and bytes of the digital world, as well as all sorts of other signs and symbols. Stories, speeches, ceremonies, and symbols continue as central to communication, even as new presentations, such as video, are becoming more and more common. Video has become central in communications and with extended reality (xR) brings immersion and mixing of new communications technologies. Each hierarchical, structural level of language carries information from word choice and turn of phrase to narratives, metanarratives, and memes; language shapes thought; but stories are primal.

Physical networks are part of the technium. The telegraph was an early physical network (the “Victorian Internet” (Rothrock 2018)). It was a manual network, with telegraph operators sending messages to other telegraph operators. The telephone allowed private individuals to talk to others, originally via a manual switchboard, now through automated switching systems. Radios originally were strictly broadcast systems, providing one-way communications. (Two-way communication was accomplished by two broadcasts on the same frequency with each party taking turns broadcasting.) Later, radio networks were established to provide the same broadcasts from multiple locations. Television evolved similarly; however, it has recently added cable and satellite transmission media. Most recently, limited two-way communication was established to permit the selection of content by users (“on-demand”)
content). The Internet has evolved into an enormous communication system, mediated by complicated software and hardware, which serves up email, messaging, image transmission, voice-over-internet, video, and a wide variety of social media.

Figure 2.4 illustrates Claude Shannon’s simple communication model (Shannon 1948a, 1948b). The mathematical formulation is germane here. Some concepts are of interest. First, information is defined by novelty: if the contents are known to the receiver before the transmission, no “information” was transmitted. That leads to a definition based on the number of possible states of a system. For example, a coin toss has two possible results or states. Thus, information about a single coin toss is represented by a single bit of information. Passing N bits of information requires \(2^N\) states. (For those familiar with binary representation of decimal numbers, a byte consists of 8 bits [each represented by a ‘0’ or a ‘1’] and can have \(2^8\) or 256 states or values.) The information we acquire may be flawed by noise in the transmission. If we add intentional distortion to the noise factor, the information fidelity problem only gets worse.

Although Shannon was describing the nature of electrical transmission of information, his theory is applicable to all communications, including speech. Figure 2.5 modifies Fig. 2.4 by adding the feedback from the receiver to the sender to illustrate two-way communication (Shannon & Weaver 1963).

Fig. 2.4  Shannon’s information flow

Fig. 2.5  Shannon’s communication loop
Shannon, after writing the formula for binary information transfer, cautioned that technical accuracy and semantic precision do not equate to effectiveness.

Figure 2.6 illustrates the difference between accuracy and precision. The target on the left has five bullet holes, with average strike point shown by the green six-pointed star. The target on the right also has five bullet holes, with average strike point shown by the star. The target on the left displays greater accuracy (but lower precision)—on average the bullets are hitting very close to the aim point (but are dispersed). The target on the right displays greater precision (but lower accuracy)—on average the bullets are hitting in the same spot (but further from the aim point). In shooting at paper targets, having both greater accuracy and greater precision will yield greater effectiveness. Shannon’s point is that in transferring information, there is another factor at work. If you have great accuracy and precision, but the target is made of metal, the bullet may not penetrate. Similarly, in communications, having a great communications system does not guarantee the recipient will act on it as desired or even understand it.

All signals are context dependent. Signal-to-noise ratio is a part of context. With a Niagara Falls of incoming information, it is hard to distinguish the salient or even the relevant from the noise (indigestion from apocalypse).

The Internet has changed the way information is transferred and often even created. It has also brought manifold changes in languages. Internet communication “is making our language change faster, in more interesting ways, than ever before (McCulloch 2019).” The Internet is the backbone of the digital matrix bringing the network diffusion dynamics to the fore. Multiple genres from text, email, blogs, to podcasts, with new abbreviations, emojis and keysmashes that convey markers of social membership. The “always on,” mobile, ubiquitous nature of this phenomenon exponentially increases communication volume, copying, accessing, sharing, filtering, remixing, and questioning. AI/ML will likely change this even more.

The dynamics of network communications are addressed in in the Network Science section in Chap. 5.
Rothrock quoted a French philosopher as saying that the existence of ships implies shipwrecks and the existence of planes implies plane crashes. He quoted the consultant Joshua Ramos as extending this to networks: the existence of networks implies network crashes (Rothrock 2018).

Attack surfaces, the span of different points where an attacker can try to enter, change or extract data, are generally considered when discussing a single computer program or system. The concept applies to your organization and your networked matrix (e.g., suppliers and customers) and easily generalizes to the technium as a whole because these cognified objects are generally connected to the Internet and, thus, connected to each other (the internet of things (IoT)) and to the whole supply chain. Attack surfaces are increasing in number and form as the technium involves the Internet. Each of the objects in Table 2.2 has its attack surfaces and each is part of the attack surface of the larger system we use in everyday life.

The internet of things forcefully exports the point of attack from a local problem to a global surface of attack, as the IoT embodies an exponential surge in the general increase in digital connectivity.

**Table 2.2** Cognified objects and surfaces of attack

| Object                  | Vulnerable items (data and controls)                      |
|-------------------------|------------------------------------------------------------|
| Computer                | Documents, pictures, passwords, connections               |
| Router                  | Device connections                                        |
| Printer                 | Stored images                                             |
| Cell phone              | Connections, passwords, data                              |
| Cloud storage           | Documents, pictures, passwords, data                       |
| Social media system     | Connections, pictures, information                        |
| Security system         | Real-time visuals, system controls, entry                  |
| Cognified appliances     | Inventory, real-time visuals, controls                     |
| Cognified infrastructure| Programmable industrial controls                          |
| Database                | Information                                               |
| Computer networks       | Access to cognified objects                               |
| Internet of Things (IoT)| Control of objects, connections to networks               |
| General infrastructure  | Operations, when connected to cognified objects           |

**Vulnerabilities in the Technium (Surfaces of Attack)**

Before computers, the noosphere consisted of the contents of people’s brains and their written records. The most permanent parts were in books and the most evanescent written records were in newspapers. Today there are still brains, books and newspapers, but the technium has grown and there are also computer stores of
knowledge, both localized on your own computer and indeterminate, in the “cloud,” stored on someone else’s computers elsewhere.

**Malware and Defenses**

*Malware* is computer software that interferes with the correct processing of information or corrupts that information. Malware is used to attack the part of the technium that is based on or connected to computers (computers themselves and machinery that uses computers, such as automobiles, the electrical grid, and centrifuge controllers). Clarke and Knake said, “66 percent of malware was delivered in email attachments (Clarke & Knake 2019).” The direct action of malware is on the technium; however, it also can act as an indirect attack on the noosphere, corrupting knowledge and inserting fake news. An article in the Journal of Cybersecurity provided a taxonomy of these “cyber-harms” (Agrafiotis, Nurse, Goldsmith, Creese, & Upton 2018).

An opinion article in The Wall Street Journal described a new type of malware—hardware malware. The article described the possibility of creating a Trojan horse in the hardware logic of a computer chip. Each chip that is manufactured and employed in a device would then come preloaded with the Trojan horse that looks legitimate, but is not. Its actual purpose may be to allow external control or exfiltrate information or simply to turn off the chip, that purpose to be activated at will by its designer. The point of the article is that most chips used in the U.S. are designed in the U.S., but manufactured in foreign countries. One such country could modify the design to include the Trojan horse and the complexity of the chip design would hide the modification (Scher & Levin 2020).

*Malware*

In cataloging malware, it is important to realize that the brains (cognition) behind the creation and use of the malware is more significant than the malware itself. With the exception of the unintended kind, such as the Morris worm, malware is used by humans to create ill effects. (The Morris worm was created to demonstrate vulnerabilities, but ended up infecting 10% of the computers connected to the internet in the late 1980s, causing massive denial of service by accident (Rothrock 2018).) The most sophisticated and dedicated malware users are called advanced persistent threats (APTs) (Clarke & Knake 2019).

Malware (software) is relatively cheap and easy to produce, purchase, scale, and deploy and can produce effects at almost any scale. Some of the earliest malware examples were simple “worms” that propagated through the early computer networks, produced by eager novices. Because of these and later examples, protection software and principles were created, requiring modern malware to be more sophisticated. Still, malware must be much smaller than some of the million-line programs
in use today, so in relative terms, “cheap” and “easy” remain accurate descriptors. The “ease of entry” in obtaining malware is profound; there are even websites from which pre-built malware can be obtained for prices ranging from $1 to $3500 (Paganinin 2018). Naturally, there is a commercial market for anti-malware systems; however, as a result malware is evolving extremely rapidly. Currently, the advantage goes to the attacker in malware. However, Rothrock said that advances in digital resistance are eroding this advantage (Rothrock 2018).

Our ontology includes a section on malware, derived in part from a Carnegie Mellon University ontology (Costa et al. 2016). **Malware Tool**: “A malicious piece of software,” implanted in a computer for immediate or delayed activation. Figure 2.7 illustrates some types of malware.

The definitions of some of the types of malware are shown in Table 2.3.
Bots are “software agents used to generate simple messages and ‘conversations’ on social media.” They range in sophistication from the very crude to extremely credible replications of humans. In 2014 a bot passed the Turing test for the first time. After a five-minute “conversation,” a third of the judges believed there was a human on the other end of the conversation. This was one of the original goals of AI (Woolley & Howard 2019).

Typically, bots are hosted on a computer, whether legitimately (as with most service bots) or by infesting target computers. However, Rothrock discussed a 2016 exploit that largely used internet of things devices, rather than computers to host bots. This botnet was created by the Mirai botnet tool and consisted of around 100,000 nodes (Rothrock 2018).

Social bots or chat bots are built to respond like humans with pauses and other human cues. Some are clearly labeled as chat bots on web sites and provide a help function, releasing human help personnel to handle more difficult queries. Other social bots have more nefarious functions. For example, a set of bots can boost the apparent popularity of a product by posting positive statements from numerous “users” of the product. Sophisticated bots can maintain simultaneous presence on several social media sites, producing cross-feeds of supporting “opinions.” Sophisticated bots respond to posts from other social media users (real or bot), supporting or contradicting these posts. Because they are software, bot usage is easily scaled to a very large presence (Woolley & Howard 2019).

Dubois and McKelvey investigated the use of bots in Canada. They identified several types. Political bots are social bots with an agenda of political manipulation. Dampener bots can suppress or dampen contrary political opinions by crowding out or reducing the accessibility to the public of the contrary opinions. Amplifier bots work to amplify supported political opinions by adding additional posts and

---

### Table 2.3 Definitions of selected malware types

| Class          | Definition                                                                 |
|----------------|-----------------------------------------------------------------------------|
| **Virus**      | “A program that is capable of replicating itself and has malicious purposes.” | The tools in orange with the “is-a” arrows going in both directions are different names for the same tool. |
| **Backdoor Software** | “A computer program designed to allow an unauthorized path into the network or a system.” |
| **Logic Bomb** | “A malicious program that is coded to execute when a certain set of requirements are met.” |
| **Password Cracker** | “A program that is used to identify an unknown or forgotten password to a computer or network resource.” |
| **Port Scanner** | “A software program which scans a network for systems with open ports.” |
| **Key Logger** | “A type of surveillance software that has the capability to record every keystroke made to a log file, usually encrypted.” |
| **Spam**       | “Unsolicited e-mail. May send harmful links, malware or deceptive content. Goal may be to obtain sensitive information.” |
| **Trojan Horse** | Malware that looks legitimate, but is not. |
reposting the supporting opinions (of real users or other bots). Transparency bots attempt to draw attention to the actions of public officials by posting those actions (generally of one given type of action per bot). Servant bots consist of bots such as the chat bots that serve help functions; however, to the extent that they collect personal information about the user chatting with them, their overall use may be problematical (Dubois & McKelvey 2019).

Singer and Brooking discussed the activities of bots. “For example, the day after Angee Dixson was outed [as a bot] in an analysis by the nonprofit organization ProPublica, a new account was spun to life named ‘Lizynia Zikur.’ She immediately decried ProPublica as an ‘alt-left #HateGroup and #FakeNews Site.’ Zikur was clearly another fake—but one with plenty of friends. The bot’s message was almost instantly retweeted 24,000 times, exceeding the reach of ProPublica’s original analysis. In terms of virality, the fake voices far surpassed the reports of their fakeness (Singer & Brooking 2018).”

“As businesses whose fortunes rise or fall depending on the size of their user base, social media firms are reluctant to delete accounts—even fake ones. On Twitter, for instance, roughly 15 percent of its user base is thought to be fake. For a company under pressure to demonstrate user growth with each quarterly report, this is a valuable boost (Singer & Brooking 2018).”

“Moreover, it’s not always easy to determine whether an account is a bot or not. As the case of Angee Dixson shows, multiple factors, such as time of activity, links, network connections, and even speech patterns must be evaluated. Researchers then take all of these clues and marry them up to connect the dots (Singer & Brooking 2018).”

Memes

The science fiction author, David Gerrold wrote about the importance and power of memes. “Humans live and breed for their beliefs: often they sacrifice everything for the thoughts they carry. History is a chronicle of human beings dying for their convictions, as if the continuance of the idea is more important than the continuance of the person (Gerrold 2003).”

“The memetic warfare envisioned by Singer and Brooking in their book, LikeWar, recognizes the power of virality—the need to produce and propel viral content through the online system. But it also recognizes that the content that goes viral—the meme—can be quite easily hijacked. And whoever does that best determines what reality looks like (Singer & Brooking 2018).”

Wells and Horowitz described meme factories and some of the problems they cause in a Wall Street Journal article. They described how 421 Media records videos of stunts and searches for other posts that it can re-post for Instagram followers. The problem, as described, is that the volume of such posts by 421 Media and other meme factories endanger the “stylish and intimate aesthetic” of Instagram (Wells & Horowitz 2019).
Malicious Actions

Figure 2.8 illustrates some of the many malicious actions that can be performed to attack cognified systems. These include various forms of phishing, which rely on convincing a human operator to do something he or she shouldn’t (like install malware) and various types of denial of service attacks that prevent the legitimate operation of the computer.

For example, suppose that Ralph (the leader), John, Sue, and Joe have invaded a system and copied a document, as shown in Fig. 2.9. Further, these individuals are linked to an instantiation (groupZeta) of the social faction class. This ontological view supports analysis at a higher level of aggregation than supported by the individual names.

Suppose it is determined that the theft was accomplished through the use of a phishing attack that allowed planting a backdoor into the system, followed by copying the document. These actions are shown in Fig. 2.10. These actions are linked to an aggregated action called stealDocumentA.

Two object instances are involved in this cyberattack, the document to be stolen and the malware tool used in the theft. These objects are shown in Fig. 2.11.

This example illustrates a purposeful attack with a unique goal, theft of the contents of a particular document. The cybersecurity firm Crowdstrike reported on the

![Diagram](image_url)
2015 hacking of the Democratic National Committee computers. Russian hackers infiltrated the computers (through unspecified means) and prepared documents for exfiltration. Comparative digital footprints of these documents matched those of documents that were released, indicating that they were successfully stolen (The United States House of Representatives 2017).

However, many attacks have a general goal, with success measured in high probabilities of success, not any individual success. “The lesson for BuzzFeed, and for all aspiring social media warriors, was to make many small bets, knowing that some of them would pay off big.” “Recall that ISIS could generate over a thousand official
propaganda releases each month. In each case, this continuous cascade allowed these savvy marketers to learn what worked for the next round (Singer & Brooking 2018).”

**Computational Propaganda**

Woolley and Howard defined the technical component of *computational propaganda* “as the assemblage of social media platforms, autonomous agents, algorithms, and big data tasked with the manipulation of public opinion.” The social component is the propaganda, “communications that deliberately subvert symbols, appealing to our baser emotions and prejudices and bypassing rational thought, to achieve the specific goals of its promoters.” As they explained it, “computational propaganda typically involves one or more of the following ingredients: bots that automate content delivery; fake social media accounts that require some (limited) human curation; and junk news (Woolley & Howard 2019).”
Time Duration of Successful Attacks

A denial of service attack takes milliseconds for the first set of packets to bombard a system. The technical success of the attack is apparent almost immediately. For the attack to be pragmatically successful, it must last long enough to disrupt the services of the target. Depending on the resources of the attacker and its goal, the duration can extend from hours to days.

Other types of attacks take time to develop. For example, it might take months of phishing to induce a person to click on a link or open an attachment that lets the attacker into a system. After that, it can take minutes to days for the attacker to explore the system and find the desired data. More malware may be required to actually exfiltrate the data out of the system into the hands of the attacker. Very large amounts of data may take days or weeks to exfiltrate (partially to avoid notice caused by abnormal data flows.) Ray Rothrock estimated that the Target data theft of 2013 that involved data records of 70 million customers took about two weeks, most in the exfiltration phase (Rothrock 2018). CrowdStrike defined “breakout time” as the time between the initial compromise and successful lateral movement in the victim environment. Breakout time represents the best window for stopping the attack. In 2018, the average breakout times for four major (attacker) nations and a crime group ranged from under 19 min to more than 9 h (Crowdstrike 2019).

Rothrock said, “an entire category of breach is categorized as an ‘Advanced Persistent Threat’ (APT), a network attack in which the intruder not only gains access to the network but remains active in it for a long period of time.” (Note that here APT refers an action type, shown at the bottom of Fig. 2.8, whereas earlier it referred to a type of actor.) Rothrock referred to the “most spectacular documented APT,” which is believed to be a Chinese attack. That attack maintained access to various networks for an average of 356 days, with the longest duration for one network being 1764 days (Rothrock 2018).

Defensive Tools and Actions

Protection tools and actions are relatively inexpensive; however, they must be used to be effective. Protection Tool: “A piece of software that serves as protection against malware.” Figure 2.12 illustrates some protection tools.

Table 2.4 defines some protection tools.

Figure 2.13 illustrates some of the actions that can be performed to prevent and mitigate malicious attacks on cognified systems and provide other protective services. Some are standard preventive security actions, such as replicating data, installing patches, and updating software regularly. Some are protection against particular types of attacks, such as authenticating sessions, limiting query types and blocking redundant queries. Reciprocal information sharing, including sharing attack profiles and attack code, can cause institutional problems, but is necessary (Falco et al. 2019). The final protection action is holistic in nature, aimed at creating and maintaining a resilient system. Modeling the network refers to more than just a
map of connections among the components, but includes methods for checking on the effects of modifying the system (Rothrock 2018). The mitigation actions support resilience. They include digital and organizational resilience, sharing of strategies and decoupling. Decoupling refers to the segmentation of data into access classes to prevent unauthorized access.

**Trust Technologies**

While trust is a human belief, there are technologies to support its application. You trust that when you put your money in a bank you will be able to retrieve it as needed. There was a time when this trust was sorely tested; banks failed; and people lost their money. In the U.S., the Federal Deposit Insurance Corporation (FDIC)
was created to restore trust in banks. The blockchain technology allows “secure” transactions outside of the traditional banking businesses (Henderson 2019). These are economic technologies. In a time when identity theft is common, we have a problem of trust—trust that our identities won’t be stolen and trust that the identity proffered by someone else is valid.

A group from MIT has done extensive thinking about the subject, made presentations to various groups including the White House Commission on Cybersecurity, and published a book entitled, Trust::Data: A New Framework for Identity and Data Sharing (Hardjono, Shrier, & Pentland 2016). They began with the point that the systems that we use in daily life were not created with same fears about trust that we now have. Our banking systems started with personal visits to the bank: there was no need to validate electronic identities because they didn’t exist. We were asked to supply our social security number when making a purchase at many places—and didn’t worry about doing that. We often had it printed on our checks along with

Fig. 2.13 Protection and mitigation actions
name and address! The authors remarked on the pervasive sensing that now exists: smart phones collect and share location data and people share incredible amounts (and scarcely credible [to the authors, at least] types) of data on the Internet. The authors called for reinventing societal systems to remedy the current situation—to ensure trust. Further, they described, in a fair amount of detail, proposals to do that.

Influence, Persuasion, Manipulation, Coercion, Control

Influence, persuasion, manipulation, coercion, and control are intrinsic to man, citizen of the noosphere and the technium, utterly intertwined. Malware is aimed at the objects in the technium. Thus, it acts indirectly on humans. However, there are tools in the technium that act directly on humans. This section introduces these tools. Table 2.5 lists fundamentals of persuasion. As always, consider context, timing, meta-structure, access to information, simplicity, ease of used, and repetition. The Persuasion section in the chapter on humans (Chap. 4) will define each item and discuss why and how they work.

There is and always has been a battle of ideas at the highest level of politics, policy and statecraft using speeches, stories, ceremonies, and symbols. Lies have been part of human culture since records have been kept. They are assaults on the noosphere (the total information available to humanity). However, our current (seeming) insistence on euphemisms, such as counterknowledge, half-truths, extreme views, alt truth, conspiracy theories, and fake news, in place of the word “lies” and the deterioration of our education with respect to critical thinking has lowered the bar for lies to be weaponized (Levitin 2016). The ammunition consists of stories, words, memes, numbers, pictures and statistics. Salient topics include deepfakes (artificial intelligence (AI)-augmented false news, pictures, sound and video clips putting words into the mouths of others), associative decoding (inserting false memories (Ramirez et al. 2013)), meaning platforms, serenics, knowledge of the spread dynamics of information versus spread of behavior or spread of violence, in traditional and digital systems (Centola 2018b). Weaponized lies purposefully undermine our ability to make good decisions (Levitin 2016).

Influence, as it operates in the continuum of persuasion, coercion and control, can take many forms. Default rules can eliminate choices from search engines to traditionally offered choice lists. There is power in perfidy. Trust is central and offers a target of influence. Merchants of doubt are often used. With the fragile and stringent markers of social membership and humans’ powerful bias toward membership, affiliative and dissociative forces can be marshalled. Mis-directions such as bait-and-switch are seen frequently. Influencing the decision time frame can work. Denial, obfuscation, reframing, redefining, relabeling, and repositioning are methods of influence. Quantitative propaganda has manifold forms. Changes in signal-to-noise ratios are powerful: haystacks of misinformation can hide a needle of truth or confuse indigestion with apocalypse. Fake news can use bot armies and hide innumerable human biases, fears and needs.
Table 2.5  Persuasion fundamentals

| Central Forms | Aristotle | Cicero | Claidini | Sharot | Fogg | Thaler & Sundstein | Pink | Berger | Martin & Marks | Centola/ Jackson | Digital Attention Merchants |
|---------------|-----------|--------|----------|--------|------|--------------------|------|--------|--------------|-----------------|---------------------------|
| Personal Contact | Ethos | Knowledge | Liking | Priors | Motivation | Incentives | Carrots | Reduce Reactance | Messenger Bias | Network Structure | Garnering attention |
| Stories | Logos | Understand-Reciprociting the Cause | Emotion | Ability | Understanding Mapping | Sticks | Ease Endowment | Hard Messenger | Network Dynamics | Addictive technology |
| Speeches | Pathos | Arranging the Argument | Authority | Incentives | Prompts/Triggers | Structure Complex Choices | Autonomy | Shrink Distance | Soft Messenger | Diffusion: Information Behavior | Persuasion profiles |
| Ceremonies | Kairos | Emotions | Social Proof | Agency | Captology | Defaults | Mastery | Alleviate Uncertainty | Human & Digital Fulcrum of Connectivity | Always On |
| Symbols | Eloquent Delivery | Consistency | Curiosity | MIP | Give feedback | Meaning | Corroborating Evidence | Micro-targeting | Swarms | |
| Social Signals | Practice | Scarcity | State | Expect error | Unity | Others | Virality | Global scale | |

Technology’s New Ecology, Mix and Match: Adaptive, Combinatorial, AI/ML Augmented, Synchronic or Diachronic, nascent xR

Assessment of Credibility, Character and Ability underlies Trust (trust technologies are nascent)

**Diachronic** (occurring over time or for future effect, as opposed to synchronic or contemporaneous effect)
- Shi: A central ancient Chinese stratagem of warfare, a deception involving influencing the present as part of a larger or grand strategy to influence the future at a propitious moment, often for a long-term, zero-sum game.
- Apple of Discord: Sowing a small disagreement to create growth to a major conflict, e.g., election interference for trust, polarization & outcomes.
- Sleeper software: Implanted malware to be activated at a later time.
- Parable of the seed in the Bible: The seed is sown in various environments with different effects at a later time.
With research, surveillance and analysis, messages can be personalized (micro-targeted) for the optimal density of learning moments. Surveillance and rhetoric are informed by new advances in multiple disciplines. Gargan personalized these concepts, discussing using new forums of cognition (social media) and new features of arrangement (attention catching, non-boring introductions and follow-through) (Gargan 2017).

**Computerized Persuasion**

Maurits Kaptein calculated the effect of the Internet on sales. The simple formula he used was that the effect should be proportional to the reach (the number of people touched) times the impact (effectiveness of the message). The reach has increased dramatically over time: consider pre-printing press reach, post-printing press reach, radio and television reach, and Internet reach (almost the whole world). The Facebook social network has 2.9 billion users (Forbes 2020). Certainly, different salesmen have different levels of competency and thus impact; however, they should average out at some level. Projecting the increased reach multiplied by impact should yield enormous increases in sales. Sales have increased; however, dividing actual sales by reach shows that impact has declined as reach has increased. The Internet has not been delivering the expected dividends! Kaptein concluded that, on average, the Internet “touches” were less effective than live salesmen. Kaptein’s research showed that to have greater impact, the Internet influence efforts would need to employ the persuasion techniques described by such as Cialdini (listed in (Cialdini 2009)) and take advantage of the research of Fogg (below) (Kaptein 2015).

**Captology** is the study of computers as persuasive technologies (Fogg, Home, n.d.). This includes the design, research, ethics and analysis of interactive computing products (computers, mobile phones, websites, wireless technologies, mobile applications, video games, etc.) created for the purpose of changing people’s attitudes or behaviors. In his book, *Persuasive Technology*, Fogg discussed the elements of captology (Fogg 2003). Clearly, the potential target of persuasion (person) is not interacting with a human being in a face-to-face encounter. However, the target is not interacting with a “computer” (think machine with blinking lights and spinning magnetic tapes), but with a computer interface—typically a computer monitor, a cell phone screen, or a speaking “personality,” such as Alexa or Siri. The large amount of human interaction that occurs through these same devices reduces the perceptible difference between face-to-face persuasive encounters and computer persuasive encounters.

Fogg pointed out several advantages that computers have over human persuaders. Computers are persistent; they allow anonymity; they can access large stores of data; they can vary their presentations; they can expand the numbers of simultaneous targets; and they can be everywhere. These advantages are actually just the beginning. Humans can also vary their persuasive presentations. However, this variation is based on the skill of the particular human at reading the situation and making modifications. Computer adaptations can be based on scientific research, using
those large data stores, to choose the variation that is most likely to succeed based on the situation.

Fogg’s Stanford Persuasive Tech Lab website contains discussions on human behavior and techniques for changing it using technology (Fogg, Home, n.d.). This includes both individual persuasion and changing attitudes and behaviors on a mass scale—Mass Interpersonal Persuasion (MIP). He also included some warnings about computer persuasion. The first warning relates to source trust: just because a website exists, does not mean its contents are true. The topic of “website credibility” has developed a large body of knowledge. Even videos can be faked or contain faked parts. The second warning concerns “seduction via video games.” In all video games, the cause and effect relations that underlie the action may or may not reflect real-world cause and effect. However, as part of our human learning process we internalize our notions of cause and effect by observation, not through school courses. Where simulations lead to errors in learning, we encounter what the military calls “negative training (Hartley 1995).” Fogg said it is bad enough to have negative training just to make the video game fun; however, video games can be engineered to influence gamers’ social and political views without allowing for conscious consideration of arguments concerning the influence. Finally, he warned of individualized or micro-targeted persuasion profiling. Advertisements are selectively placed on our web search results based on previously collected information on our activities. There are even more subtle strategies in which our decision-making is analyzed to create an iteratively adaptive personalized profile of our susceptibility to particular persuasion techniques. This profile can then be used later to more accurately persuade us to buy, vote, or act as desired by the site owner. Computational social science has arrived.

In 2005, Zappen surveyed the literature of digital rhetoric. He said it “encompasses a wide range of issues, including novel strategies of self-expression and collaboration, the characteristics, affordances, and constraints of the new digital media, and the formation of identities and communities in digital spaces (Zappen 2005).”

**Persuasion Through Search Engines**

Dr. Robert Epstein, past editor-in-chief of *Psychology Today* and currently Senior Research Psychologist at the American Institute for Behavioral Research and Technology, testified before the Senate Judiciary Subcommittee on Constitution that between 2.6 and 10.4 million votes were manipulated in the 2016 election by Google. He testified that through bias (picking one candidate over the other) and the search engine manipulation effect (SEME), the search suggestion effect, the answer-bot effect, and other techniques Google increased the votes of one candidate. In 2020, 15 million votes could be shifted (Senate Judiciary Subcommittee on Constitution 2016). Epstein’s research on SEME was published in the Proceedings of the National Academy of Sciences (PNAS) (Epstein & Robertson 2015).
Persuasion in the xR World

xR refers to extended reality technology and experience. It is immersive and includes virtual reality (VR), augmented reality (AR), 360° video, and mixtures of these (MR). The use of xR is rapidly expanding, including commerce, education, entertainment, and warfare.

The new virtual reality (VR) world has been *terra incognita* of social interaction metric and analytics. This is changing with the new Stanford University Virtual Human Interactions Lab (Stanford University VHIL 2019). New persuasion forces are expected from virtual reality and companion avatars. We have seen hints of this where simulations lead to errors in learning, encountering what the military calls “negative training (Hartley 1995).”

Persuasion in the AI World

In an age of both massive and personalized surveillance, digital social networks can be personalized and “optimized for engagement,” using “glimmers” of novelty, attention channeling messages of affirmation and belonging, and messages of outrage toward preconceived enemies, for affiliative or dissociative ends. AI-empowered suggestion engines, armed with conditional probabilities (driven by machine learning) are powerful persuaders (Polson & Scott 2018).

“But it doesn’t take an authoritarian state to turn a neural network toward evil ends. Anyone can build and train one using free, open-source tools. An explosion of interest in these systems has led to thousands of new applications. Some might be described as ‘helpful,’ others ‘strange.’ And a few—though developed with the best of intentions—are rightly described as nothing less than ‘mind-bendingly terrifying (Singer & Brooking 2018).’”

“They can study recorded speech to infer meaning, these networks can also study a database of words and sounds to infer the components of speech—pitch, cadence, intonation—and learn to mimic a speaker’s voice almost perfectly. Moreover, the network can use its mastery of a voice to approximate words and phrases that it’s never heard. With a minute’s worth of audio, these systems might make a good approximation of someone’s speech patterns. With a few hours, they are essentially perfect (Singer & Brooking 2018).”

The largest digital platforms can gather and dispense attention on a world-wide scale. Recent advances in combinatorial persuasion, armed with AI, augmented with personal and group metrics can make many individuals and the masses more prone more to follow suggestions. The resolute can become sequacious.

The technium can accelerate the decision process and thus alter the probability of an outcome.
Fake News and Disinformation (the Power of Perfidy)

A fundamental humans bias is our default to truth or initial assumption of truthfulness (Gladwell 2019). This default bias can aid in adaptive affiliation but leaves us vulnerable as described in The Misinformation Age (O’Connor & Weatherall 2019), Weaponized Lies (Levitin 2016), and the newer methods of false memory insertion (Ramirez et al. 2013). We also have a countervailing “open vigilance” or “reactance” that must be overcome for us to move from our initial opinion or be persuaded. Most efforts at mass persuasion fail (Mercier 2020).

Whereas malware is a tool in the information conflict; fake news is both a product of the information conflict and a tool in the conflict. An article in Science defines “fake news’ to be fabricated information that mimics news media content in form but not in organizational process or intent.” According to the authors, this distinction is important because it plays on the trust gained by standard news media. “Failures of the U.S. news media in the early 20th century led to the rise of journalistic norms and practices that, although imperfect, generally served us well by striving to provide objective, credible information (Lazer et al. 2018).”

In a chapter titled “Fake News and Information Warfare,” Guadagno and Guttieri discussed fake news in detail. They concluded that “there are many personal, political, and psychological factors” that relate to answering the questions of who spreads fake news, who falls for fake news, and what makes fake news effective. Historically, fake news has existed for a long time. Social media has made the spread of fake news easier. The allure of conspiracy theories supports some forms of fake news. Motivated belief (confirmation bias), emotional contagion, and delusions support the acceptance of fake news. The existence of political filter bubbles also supports fake news (Guadagno & Guttieri 2019).

Having been used to accepting information from news media, people are likely to be relatively uncritical in accepting fake news. Where there is conflicting information, “people prefer information that confirms their preexisting attitudes (selective exposure), view information consistent with their preexisting beliefs [their preconceptions] as more persuasive than dissonant information (confirmation bias), and are inclined to accept information that pleases them (desirability bias) (Lazer et al. 2018).” As illustrated in Figure 2.14, the aphorism “garbage in, garbage out” holds true for people as well as for computers.

In Weaponized Lies, Daniel Levitin said, “We have three ways to acquire information: We can discover it ourselves, we can absorb it implicitly, or we can be told it explicitly (Levitin 2016).” Figure 2.15 shows how each means of acquiring knowledge can be corrupted. We have a bounded reality (see Chap. 3); our discovery of new knowledge is limited by our own preconceptions. When we play computer games, we follow the rules of the game, whether they are valid representations of reality or not. The more realistic the game seems, the more likely that we will absorb lessons that we will apply to reality. This means that we are vulnerable to someone engineering the rules to fit their desires. [This is true for books, also. If the books always present stereotypes of humans, whether racial stereotypes or sex-based stereotypes, we are likely
to absorb these stereotypes into our own thinking.] When we are told something explicitly, we do have the opportunity to believe or disbelieve it. However, the alleged authority of the source can affect our choice. Creators of fake news can subvert our choice by mimicking or discrediting authoritative sources.

Within the numberless diversities and manifold singularity and forms of false information, we have selected exemplars of types and corrective responses (not to be confused with a *summa summarum*). The scale and frequency are evinced by the estimate that more than half of web traffic (legitimate and illegitimate (Neudert 2019)) and a third of Twitter users are bots (Woolley & Howard 2019). “Twitter falsehoods spread faster than the truth (Temming 2018).” This danger led the 2014 World Economic Forum to identify the rapid spread of misinformation among the 10 perils to society (Woolley & Howard 2019).
Search engines, filtering and ranking algorithms, social media platforms, blogs, Twitter threads, feckless celebrity posts, journalist reporting trending false stories, bad science, graphical bias, bad statistics, the absence of critical thinking, perfidy and computational propaganda abound. Deepfake technologies to manipulate images, including video, are extant and rapidly improving in sophistication. Among disinformation bots we find sleeper bots—a variety of implanted impact bots that establish a following at scale; amplifying bots that use liking or sharing and producing complaints to send requests for social media platforms to ban entities; tracking bots to detect and drive attention; and service bots to help automate other functions. All are among the numberless streams of misinformation (Dubois & McKelvey 2019; Wooley & Howard 2019b). Further, some bots do not act individually, but form botnets that communicate with each other and their owner. These bots have co-opted the computers on which they reside and can perform such actions as engaging in massive denial of service attacks on some other computer system (Clarke & Knake 2019).

Preference profiles “used by the giant search engines skew efforts at exhaustive search.” “The process of producing misinformation involves five key elements: publishers, authors, articles, audiences and rumors. Publishers run distributive platforms which have codes of conduct, style guides and journalistic guidelines. Some are more formal and rigorous (for example, well respected mainstream media publishers) and some are entirely informal (for example, content mills for clickbait). Authors live within the world of publishers (Ruths 2019).” “Social media platforms have been implicated as a key vector for the transmission of Fake News … using human hybrid accounts and increasingly sophisticated tools embedded in social media (Grinberg, Joseph, Friedland, Swire-Thompson, & Lazer 2019).”

This is not a theoretical problem. Tufekci discussed the increasing use of media platforms for active disinformation campaigns (Tufekci 2018). Current claims of accurate identification of fake news on the Internet using structured vocabulary and spread dynamics generally vary from 69% to 84%. Optimal identification is still unsettled, with a potential for the unintended consequence of labeling a true story as fake (Temming 2018). Further, we now have the capability to use competing AI programs, called generative adversarial networks (GAN), to produce fake news (Giles 2018).

Singer and Brooking described the propagation of fake news. “Modest lies and grand conspiracy theories have been weapons in the political arsenal for millennia. But social media has made them more powerful and more pervasive than ever before. In the most comprehensive study of its kind, MIT data scientists charted the life cycles of 126,000 Twitter ‘rumor cascades’—the first hints of stories before they could be verified as true or false. The researchers found that the fake stories spread about six times faster than the real ones. ‘Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information,’ they wrote (Singer & Brooking 2018).”

Singer and Brooking reported on fake news resulting in real threats of war, which did not escalate when the fake news was debunked. They continued, “Sadly, not all false online reports have been stopped before they’ve sparked real wars. In
mide-2016, the rival armies of South Sudan’s president and vice president had settled into an uneasy truce after years of civil war. But when the vice president paid a visit to the presidential palace, his spokesperson published a false Facebook update that he had been arrested. Reading the post, the vice president’s men paid an angry (and heavily armed) visit to the palace to rescue him. The president’s bodyguards in turn opened fire—igniting a series of battles that would leave over 300 dead and plunge the nation back into conflict (Singer & Brooking 2018).”

AI is contributing to the alteration of the perception of reality. A small note in Forbes (Bosilkovski 2018) said, “In November 2016, Adobe introduced Sensei (Japanese for “teacher”), artificial-intelligence and machine learning software that can, for instance, recognize facial features in a Photoshop file and allow a person’s expression to be changed without making the image look unnatural.”

Detecting Fake News and Disinformation

“If there is no truth, there can be no trust” “with the attendant corrosion of group identity and national unity (Snyder 2018).” Deepfakes must be unmasked using image verification technology.

“Information overload and the average web surfer’s limited attention span aren’t exactly conducive to fact checking.” “People will likely choose something that conforms to their own thinking, even if that information is false (Temming 2018).” The computer programs designed to detect fake news are now in their infancy and give rough conditional probabilities. Substance, style, structure, word choice and social network structures are guides in this imperfect art/science of fake news detection.

“False articles tended to be shorter and more repetitive with more adverbs. Fake news stories also had fewer quotes, technical words and nouns.” “Fake news like a virus can evolve and update itself (Temming 2018).”

There is a nascent, expanding understanding of the skills of correcting misinformation. Of course, it is preferable to get the facts and incorporate the facts before the misinformation to take advantage of the anchoring bias of initial opinion.

Narrative Warfare

As Ajit Maan put it, “[narrative warfare] is not information warfare; it is warfare over the meaning of the information (Maan 2018).” Narratives tell the meaning of the facts. Narratives have always been central to persuasion. The tools of persuasion are manifold and powerful. Persuasion is undergoing an accelerating growth in complexity and change in the morphology of its causal chains and systems of power at multiple scales. Persuasion operates at all levels of power: political, diplomatic, commercial, military, financial, educational, and personal.

Narrative warfare consists of a coherent strategy that uses honest or fake news as a tactic. “The currency of the narrative isn’t truth, it is meaning (like poetry) (Maan 2018).” The idea is to create a story that leads to the desired conclusion. The story
need not be “true,” but it must resonate with the audience. It is effective because it bypasses critical thinking and shapes the identity of the receptive audience, and thus its beliefs and actions (Maan 2018). The relationship between the persuader and persuadee is central (Martin & Marks 2019). Knowledge of the audience is critical from their orienting, metanarratives from world view to politics, personality and local matrix of relationships and identity (see section on Persuasion in Chap. 4). It is essential to understand the distinctive features of efforts to correct misinformation versus having a clean slate of a neutral recipient.

“Narratives are the building blocks that explain both how humans see the world and how they exist in large groups. They provide the lens through which we perceive ourselves, others, and the environment around us. They are the stories that bind the small to the large, connecting personal experience to some bigger notion of how the world works. The stronger the narrative is, the more likely it is to be retained and remembered (Singer & Brooking 2018).”

“[C]ognitive science has demonstrated countering lies by repeating them with the word ‘no’ (or some other negative) actually has the opposite effect. That strengthens the false statement in the mind of the audience (Maan 2018).” To counter the false or the established opinion, we must understand the audiences’ assumptions, preconceptions, social memberships, and identity as currently constructed. It is often best to avoid a direct counter narrative and instead use a larger metanarrative to reframe or encompass the opposition. Generally, it is important to actively engage the listener. Offer a bigger, better, stronger, smarter alternative way of understanding, of identifying, of acting (Maan 2018). If the persuader is seen as an “authority,” “them,” or not one of “us” by the persuadee, it may be useful to begin with a faint denouncement of oneself to be sure you are on eye level with the audience as a step toward common ground (Berger 2020).

**Surveillance and the Panopticon (Our Surveilled World)**

Surveillance is the fusing of sensing (both outward and inward), communication and computation. Ubiquitous surveillance is inevitable. “We are on our way to manufacture 54 billion sensors every year by 2020 (Kelly 2016).” Panopticus was the mythical Greek Giant who saw all with his many eyes. Now by extension, the Panopticon refers to the surveillance state, where the state sees all and knows much. The Internet is the world’s largest and fastest sensing machine. Early awareness of discovery and emergence within the noosphere and technium is critical, as surveillance technologies from satellite imagery to single photon detection are rapidly increasing in power and scope.
Sensing and Communication

The domain (what is sensed), matrix (the environment within which the sensing takes place), and technology of sensing are morphing. The domain now must include awareness (traditional sensing), emergence and reification in the noosphere and technium, as well as traditional spying. A critical example of change in both domain and matrix of sensing is “quantum inspired computational imaging (Altmann et al. 2018).” With quantum-inspired computational imaging and “fusing of high temporal resolution (a trillion frames a second) together with single photon sensitivity (Hadfield 2009; Migdall, Polyakov, Fan, & Bienfang 2013) and advanced computational analysis techniques, a new generation of imaging devices is emerging.” The 3D images can be taken of a scene that is hidden behind a wall or through fog.

Our digital society is approaching the Panopticon, in which everything is observed, recorded, analyzed, and (potentially) acted upon. Currently, almost anything that can be tracked is being tracked. Everything means all communications, whether audio, video or text, location and movement, activity types, and computer data. Data on our click streams, our online activities, and our on-and-off-line human networks are available. New technologies are permitting the addition of social signals (non-verbal clues to thinking and feeling) to this mix (Pentland 2008). Pentland described using monitoring and analysis to design “better” city environments and to design better, smarter, more effective teams and larger social groups. Utilizing sociometric badges for collecting data and sociometrics for analysis resulted in findings of improved collective cognition (Pentland 2014). Human senses can be augmented with multiple points of view from satellite to microscopic views. For example, the Mojo Lens replaces AR headsets with a contact lens that displays context-related information on the retina using “invisible computing (Mojo Vision Inc 2019).” The surveilled data is quantified, producing biometrics (physiologic and behavioral), psychometrics, neurometrics, and sociometrics. Use of GPS, voice and facial recognition is widespread. More and more often, sensing data is processed using AI/ML to infer new patterns and produce data about data (metadata). Multimodal sentiment analysis and other new disciplines of knowledge are upending traditional surveillance modalities and changing cognition (Poria, Hussain, & Cambria 2018). Continuous sensing allows experimental design and implementation for iterative additive influence (Luca & Bazerman 2020).

The future may hold additional surveillance threats. Single photon detection is nascent and will extend surveillance into the dark and through selected walls and barriers (Hadfield 2009; Migdall et al. 2013). Commercial, hand-held digital olfaction tools are in use (Bombgardner 2020). Each person is enveloped in a genomic, epigenomic, proteomic, and microbiomic plume and leaves a trail when moving. (Did you think bloodhounds track people by magic?) Automated methods of location, tracking and contact tracing (for marketing, surveillance, and public health) of individuals are extant (Stern 2020). Neuralink seeks to directly connect the individual brain to the silicon computer world (Neuralink Corp 2018; Hernandez & Mack 2019). There are current DOD efforts to effect a direct brain/computer
interface, the place where silicon and carbon meet (Tullis 2019). Consider the possibility of hacking our brains through such a link.

Meanwhile, wide-area surveillance technology continues to advance. “Over a period of three months in 2016, a small aircraft circled above the same parts of West Baltimore that so recently drew the ire of President Trump. Operated by a company called Persistent Surveillance Systems, the plane was equipped with 12 cameras which, at 8000 feet, could take in 32 square miles of city in minute detail (Mims 2019a).” Christopher Mims reported that this and other similar systems permit tracking suspects from a crime scene to getaway cars. Other systems can then identify the cars’ license plates as they pass by closed-circuit cameras. He reported that some multi-camera systems used to cost a half million dollars, but now cost between $82,000 and $140,000 and will cost half that for their next versions. He continued, “But as the technology rolls out—and roll out it will—it’s likely to stoke considerable debates about a new definition of privacy.” In the new age of experimentation, the vision of the Panopticon is extended by designed experiments on the users of digital platforms (Luca & Bazerman 2020).

**Computation**

There is new data science and technology to gather and analyze big data to discover individual identity and social signals. The data are enhanced with experimentation and data-driven predictive analytics. Data are gathered from our monitored world and from social media use and directly from smart phone use. We are subject to hacking into our home security system, cars and even baby monitors. We regularly are subject to phishing, attempts to induce us to reveal information, such as passwords and credit card numbers through false, but ostensibly valid, emails. Hackers, corporations, digital social media platforms, nation-states, and data brokers are pervasive in the world of surveillance.

Profiling and targeting for influence will soon use much finer granularity and quantities of information from an ever widening variety of sources, such as persuasion science (utilizing AI/ML to claim the propitious moment (see Humu, below)) and information from man’s genomic, epigenetic, proteomic, and microbiomic plumes and trails.

An exemplar of the nascent emergence of the Orwellian power to influence (control) man is seen in Humu (Humu, Inc. 2018). Here the potential of the confluence of learning science, persuasion science, motivational science and network science arrives with statements of beneficence. Humu advertises that it will “Transform your organization.” It has a Nudge Engine® to deliver personal suggestions. Traditionally, the manifold forms and forces of persuasion were found in stories, speeches, ceremonies, and symbols. Now to these can be added algorithms that can drive systems of persuasion. The new ability can be embedded in AR, VR, xR, cognified objects and the software that enwraps our wetware (*a persuasion matrix*).

Workplace or human analytics sounds benign and possibly beneficial. However, the analyses require data and that data are being collected from the workers—and
not always “anonymized”—the data are tied to each worker to allow improvement efforts. The data can include recipient and timing of emails, contents of texts and phone calls, appointment calendars and actual meetings, duration data on time spent on various activities at work and at home, tonal analysis of conversations in meetings, behavior patterns such as talking over others, speech speed and volume, stress levels, network connections within and outside of the company, movement within the office, keystrokes and screens viewed on the computer, even videos of the worker taken from the computer. Companies such as TrustSphere, Microsoft, Teramind, and Humanyse provide software, hardware and services to capture and analyze these data (Krouse 2019). Cutter and Feintzeig describe companies who market and companies who use software to monitor employees’ happiness and general mental states (Cutter & Feintzeig 2020). China is expanding the requirement that digital communication device owners download an aggregating surveillance app (Li & Wen 2019b).

**Status**

The U.S. has a history of antipathy toward spying and the military in general. Henry Stimson shut down the State Department’s cryptanalytic office in 1929 saying, “Gentlemen don’t read each other’s mail (Stubblebine 2018).” During the Vietnam War, ROTC was kicked off many college campuses (Cohen 2010). Recently more than 100 students, many from Stanford University, signed a petition to boycott Google until it quits defense work. And 4000 Google staffers signed a petition for Google to withdraw from a defense contract analyzing military drone data (Baron 2018). In the United States, public opinion limits the government. Our intelligence agencies have the capabilities to create a Panopticon, but are restricted by law from doing so—although there are recent reports of using driver licenses to create a database of faces for facial recognition (Harwell 2019).

However, Google, Facebook, Amazon, and perhaps other corporations are closing in on their own versions of the panopticon (McNamee 2019). In other countries, such as China, the state is not so restricted and is rapidly approaching their own Panopticon. China even has access to almost all individual purchase information (Lee 2018). Facebook has set about creating its own crypto-currency (similar to Bitcoin), called Libra (BBC 2019). One fear is that this will give it access to similar data on purchases external to the Internet-world. The surveillance state and the major corporate Internet platforms have bio-behavioral personalized metrics to target for maximum influence; thus, we are more easily persuaded, influenced and potentially controlled.

The COVID-19 pandemic has provided a justification for some surveillance. For example, hospitals are installing automated, face-recognition thermal cameras for detecting the temperatures of people entering the building. Similar systems have been discussed for sporting events, casinos, theme parks, airline terminals, and businesses (Taylor 2020). The concept is that someone with a fever may have the virus and can be excluded. This type of surveillance and other surveillance systems that
have been added in response to the pandemic cost money. When the pandemic is over, will these surveillance systems be dismantled—or retained and repurposed?

The relevant fields, beyond governance, include cognitive science, information science, and psychology, and are delivering results such as our new understanding of man’s predictably, systematically irrational aspects. Artificial Intelligence / Machine Learning (AI/ML) armed with big data analytics from the Panopticon (surveillance state) can micro-target or sway a group.

**Biological Tools**

In the twentieth century man began to develop biological tools to cure diseases, influence mood and optimize cognition. More recently, partial control at the fundamental information/genetic level has become extant.

**Biosecurity and Biological Attacks**

Whether biological agents (1) are feral diseases, (2) come from unintended releases, or (3) are purposefully released, they can produce massive health and economic effects. A low barrier to entry into the bio-war domain, the ability to scale an attack, and the potential of problematic attribution make this an area of urgent concern. Genomic science, advanced genetic engineering, synthetic biology, and augmented computational biology with high-throughput manufacturing could contribute to a biological attack. Further, the World Health Organization (WHO) coined the word “infodemic” to refer to the deluge of discussions, including misinformation, that the COVID-19 pandemic engendered (World Health Organization (WHO) 2020). In the future, no knowledgeable adversary will miss the opportunity to superimpose an infodemic on an epidemic.

**Directed Human Modification**

Up to this point, we have considered human nature and even a given person’s nature as relatively static, i.e., changes took place in slowly in the past. The techno/info parts of the model of humanity permit new ways for a person to change or be changed (Hartley & Jobson 2014). This model will be discussed in Chap. 4.

Operant conditioning is learning brought about by reinforcements or punishments. Classical conditioning arises from repeatedly pairing a stimulus with a response. Conditioning by modeling (moving the subject through an action) is observational learning—a form of human modification.

Pharmaceuticals supply an avenue for changing psychology. Treatments of many general medical, neurologic and psychiatric conditions influence cognitive capital. Illness or intentional new forces can produce mild cognitive decline, attentional
deficits, and mood and anxiety disorders, modify impulsivity or conflict aversion, influencing cognitive capital. The basic use of digital enhancement, exercise, chronotherapeutic optimization, the current, even if temporary, influence of affect, positive expectation and the field of nootropics, are areas of interest (Turner et al. 2003; Sahakian & Morein-Zamir 2007; Mohammed & Sahakian 2011). Biologic cognitive enhancement effects are (currently) largely experimental. Cognitive enhancement effects range from genetic considerations to Sahakian’s recent selected use of modafinil at the Cambridge Brain Institute (Seife 2014) and by extension the prospect of the use of D-cycloserine to promote neuro-plasticity (new learning) for fear extinction (Kuriyama, Honma, Koyama, & Kim 2011). The possibility that PTSD might be detected through blood tests (Kesling 2019), expands the possibility of understanding it biochemically or using it as a surface of attack.

Neurotoxicants are substances capable of causing adverse effects on the nervous system and sense organs. The huge number and variety of potentially neurotoxic substances include metals, inorganic ions, botanical toxins, and other organic matter and their sources include solvents, pesticides, fine particle air pollution, agricultural soil contamination, and inappropriate pharmaceutical use. Entry can occur via absorption, ingestion, or injection and can be active from in-utero to current.

The integrated stress response (ISR) is a complex cellular physiologic system to coordinate difficult adaptive optimization. Its allocation of brain protein synthesis makes it relevant to cognitive capital maintenance and optimization. Where possible, we should optimize our ISR (Costa-Mattioli & Walter 2020).

Advanced genetic engineering and synthetic biology are extant. The modified and “very fast” CRISPR plus gene-drive technology cuts and splices large segments of the genome, not just short contiguous segments, and spreads them rapidly (Service 2019; Liu et al. 2020). The ‘prime’ gene-editing system could surpass CRISPR. David Liu, a chemist at the Broad Institute in Cambridge, Massachusetts, said “Prime editors offer more targeting flexibility and greater editing precision (Champer, Bushman, & Akbari 2016; Cohen 2019).” Synthetic biology is at hand.

A “direct” brain-computer interface is an obvious objective. It is in the laboratory but not yet realized in the field, but the race is on (Tullis 2019). Both wire and electromagnetic wave crude connections are extant. Companion VR teaching avatars are coming (Stanford University VHIL 2019).

**Trends in the Technium**

Kevin Kelly’s central thesis in *The Inevitable* is that there are technological forces that are emerging and can be expected to exert increasing influence as time progresses (Kelly 2016). Kelly made the following points, each of which is accompanied by a comment on its relevance to national security. (The authors have inserted the text in square brackets and the comments in italics.)
1. We can expect to be perpetual novices: not only will our computers develop new functions that we will always be behind in mastering, but so will our phones, our cars, our refrigerators, everything! *We know that our military hardware is no longer driving newness, but cannot keep up with civilian applications. Will this continue or will national defense hardware and software require this rapid change? What are the training implications?*

2. Kelly cited three breakthroughs in producing real AI applications: a. cheap parallel computation, b. big data [and analytics], and c. better algorithms. He was not worrying about “the computer comes alive and takes over the world.” He started with the things we can see happening: specific machine skills, such as winning at chess; more general skills, such as Alexa understanding what you ask for and finding it and then doing it; and the implications. He called these machines “robots,” for simplicity. He categorized their future jobs as, (1) jobs humans can do but robots can do even better, (2) jobs humans can’t do but robots can, (3) jobs we didn’t know we wanted done, and d. jobs only humans can do—at first. *What national defense jobs will robots be doing and which ones do we definitely not want them doing? Just think of the implications of a self-driving tank—it cuts the crew by 25%. We’ve already considered an automated loader—that means the crew is down to 2. Who or what makes targeting decisions? Can the tank be hacked?*

3. Virtual reality [(VR), augmented reality (AR), 360° presentation, and mixed reality (MR), together called extended reality (xR)] technology is rapidly improving. The military training applications are already here. The military uses mixes of live simulations (sometimes called wargames), virtual simulations (using VR of various types), and constructive simulations (computer-driven simulations). Some of the VR simulations are 360° presentations. The mixed simulations are essentially AR simulations.

4. There is increasing surveillance and tracking of almost everything. An amazing number of things are tracked already, including your (modern) car’s position, speeds, accelerations, etc. We don’t have “Big Brother,” we have lots of “big brothers.” *Suppose we don’t want our national defense organizations to access, compile and integrate all of this information. How do we prevent adversaries from doing so?*

Kelly re-emphasized that all of these technological forces are just beginning to operate and show no signs of slowing or stopping. So, this is just the beginning. (During the research for this book, the authors kept finding new technologies that had only recently been developed. As you are reading this, you may know of even newer technologies, developed since the book went to press.)

Samuel Visner, the Director of the National Cybersecurity FFRDC at MITRE, saw a coming change in the technium that will radically change the world. Internet Protocol version 4 (IPv4) defines slightly more than four billion addresses ($2^{32}$). The new version of the protocol, IPv6, will have $2^{128}$ addresses, approximately $3.4 \times 10^{38}$ addresses. That is a factor of more than a billion billion billion larger—not a billion billion billion more addresses, but a billion billion billion times as many addresses.
This huge number of addresses will allow almost everything to be connected—an internet of things. The new fifth generations (5G) networks will, of course, provide higher speed connections. However, it will also allow for direct connections between all of those (almost) innumerable things in the internet of things. The implications are still being pondered. Any emergent properties are likely to be unforeseen.

Kai-Fu Lee concentrated on the trends in the coming AI revolution (Lee 2018). Lee divided technological changes of the past into two kinds of disruptors: simple (change to a single task such as typewriters, elimination of a kind of labor such as (human) calculators, and a single industry disruption such as the cotton gin) and general purpose technology (GPT) disruptors. He identified only three GPT events in recent history: the steam engine, electricity, and information and communication technology. Lee identified the AI revolution as a fourth GPT. And he said this GPT will cause massive job displacements.

Within physical labor, Lee classified jobs by two dimensions: highly social versus asocial interactions and low dexterity/highly structured environment versus high dexterity/unstructured environment. These dimensions divide physical labor into four quadrants:

1. **Danger Zone**: high risk of replacement. Jobs in the danger zone are in the low dexterity/highly structured environment, asocial interactions quadrant. These include such jobs as teller/cashier, truck driver, assembly line inspector, and fast food preparer. AI systems will be able to do all of these within the near future.

2. **Safe Zone**: very low risk of replacement. Jobs in this zone require high levels of social interaction and high dexterity in an unstructured environment. These include such jobs as hair stylist and physical therapist.

3. **Human Veneer**: job enhancement. Jobs in this zone require high levels of social interaction and low dexterity/highly structured environment. Jobs in this zone will require humans as the interface with customers with AI support systems. These include such jobs as bartender and café waiter.

4. **Slow Creep**: job reduction over time. Jobs in this zone will gradually be replaced by AI systems as the AI systems improve in capability. These include such jobs as taxi driver and night-watch security.

Within cognitive labor, Lee also classified jobs by two dimensions: highly social versus asocial interactions and optimization-based versus creativity or strategy-based. These dimensions divide cognitive labor into four quadrants:

5. **Danger Zone**: high risk of replacement. Jobs in the danger zone are in the optimization-based, asocial interactions quadrant. These include such jobs as telemarketer, basic translator, personal tax preparer, and radiologist. AI systems will be able to do all of these within the near future.

6. **Safe Zone**: very low risk of replacement. Jobs in this zone require high levels of social interaction and are creativity or strategy-based. These include such jobs as psychiatrist, CEO, and social worker.

7. **Human Veneer**: job enhancement. Jobs in this zone require high levels of social interaction and are optimization-based. Jobs in this zone will require humans as
the interface with customers with AI support systems. These include such jobs as wedding planner, teacher, doctor (GP), and financial planner.

8. **Slow Creep**: job reduction over time. Jobs in this zone will gradually be replaced by AI systems as the AI systems improve in capability. These include such jobs as graphic designer, financial analyst, medical researcher, and scientist.

Lee then discussed the scale of job losses to be expected. He estimated that between 40 and 50% of the jobs in the U.S. can be automated within 10–20 years. He went on to say that there will be forces that reduce the rate of job losses, such as social friction, regulations and “plain old inertia.” Further, there will be new jobs that are created. Still, he estimated net unemployment increases in the 10–25% range.

In an article in the Wall Street Journal, Eric Morath provided support for some of Lee’s thesis. Morath described how AI targets higher-paying jobs, such as radiologists, financial advisers, market research analysts (Morath 2020).

Finally, it should be noted that the cognification of objects brings new opportunities and vulnerabilities.

Learning science, motivation and persuasion science are now in play. From augmented reality to single photon detection to the psychopharmacology of cognition, impulsivity and aggression in man can be changed.

Academic discussions of such potentialities exist. However, the authors can certainly envision those who might want to reduce the will to fight or induce group violence in others. The cyber and psychosocial surfaces of attack are part of our continuous change.

The vulnerable points, dynamics, and other complexities of the battlefield are morphing with increasing speed. The internet of things brings new connectivity and vulnerabilities. New understanding of the multitude of human biases and irrational aspects opens ways to connect to affiliative and dissociative opportunities. A conspicuous example of morphing of the dynamics is the new learning about propagation dynamics in social systems. Here we find the difference in moving information (simple contagions) across the system versus complex contagions of behavior beliefs and attitude (Centola 2018a, 2018b).