Chapter 1
Introduction: Humans and Their Matrix

Why do others have behavioral influence on you? Who are they? How did they get that power? How do they exercise it and how does it work? Why do they want power over you? What can you do about it? How does this go beyond the personal to important national security issues? The answers involve the changes in information infrastructure, access, and use. The fog over the complex ecology of information and persuasion is lifting.

The motif of the universe is connectivity. It is so at the quantum level, in physics, in chemistry, biology, sociology, and in our traditional and digital networks (Schweitzer 2019). As part of this motif, there have always been battles of contending ideas up and down the human scale from dyadic relationships to the highest levels of national and international politics, policy and statecraft. The ascendant morphing of information as power neither negates the wisdom of Sun-Tsu nor the strategy of von Clausewitz. It does not obviate moving, shooting, and killing. What it does do is reframe them in a more complex matrix where the only restrictions are the laws of physics, access to information, and the boundaries of cognition.

*No sire, it’s not a revolt, it is a revolution,*

was the response of the Duke of Rochefoucauld to Louis XVI, following the storming of the Bastille (Walton 2016). What we are experiencing is a revolution in information, not a revolt. The distinction is that a change—paradigmatic, transformative and accelerating—in the entire world-order is taking place. Just as events in history must be understood in the matrix (conditions) of their age, today’s information conflicts must be understood in today’s matrix.

A “Revolt” implies a single action; whereas, “revolution” connotes a broader set of actions and changes. Our matrix is one of accelerating change within our surrounding complex adaptive systems and the accelerating change in the very nature of man as an emergent biological, psychological, sociological, technological, and information being. The revolution is in the technium (technology as a whole system), in the noosphere (the totality of information available to humanity), in man
and in our knowledge of man, including our “predictably, systematically irrational” aspects (Ariely 2009). As we experience these unrelenting paradigmatic, accelerating changes, it behooves us to detect them as soon as possible so that we have a hope of surviving them. First, our vision must encompass the enlarging arc of the cognitive contests. Secondly, with foresight and insight, we must navigate the novelty, produce best-in-class adaptations, and further our own new creations. Part of the future is already here; it’s just unevenly distributed (Gibson 2003). We must avoid being part of the past that is still here but not uniformly receding.

The U.S. Department of Defense has an acronym that is relevant: DIME. DIME refers to the levers of power: diplomacy, information, military, and economics (Hillson 2009). Information has always been one of the means to gain and use power. Unsurprisingly, in the “information age” the importance, manifestations, and strength of information have greatly increased.

The technium is involved; the noosphere is the medium; but humans are the target!

Information Warfare is a generic term. It is part of both conventional warfare and unconventional conflict (Hartley 2017, 2018). It is also a stand-alone operation (Kello 2017). However, we found many discussions to be incomplete, concentrating solely on the computer aspects. Further, the term “warfare” limits the discussion to the most violent levels of conflict. Certainly computer technology provides a major method for engaging in the conflict and information stored on computers is an important part of the conflict; however, because humans are the ultimate target, all information (including information stored in human brains and our augmentations) is at risk and the engagement modes include the Internet and other technologies, such as television, and non-technological modes, such as verbal communication.

We live in polarized times. Not only are there opinion sets that divide us, but we seem to get our information from separate sources, leading to disagreements about what seem to be the facts of many situations. We describe this as living in only partially overlapping bounded realities. There are many concepts that are connected to information conflict, such as cyber warfare and persuasion science. Persuasion has been weaponized to make information and cyber warfare effective. Cognitive superiority, controlling the cognitive or sixth domain, is the topic.

The Technium

The technium is technology as a whole system. It is inextricably intertwined with the noosphere. Kevin Kelly coined this work in his book, What Technology Wants. He needed a word to express his vision that technology not only extends beyond the physical machines of civilization to intellectual creations of all types, but it also includes systemic interconnections in which each technology depends on other technologies for its production and generative forces that encourage more technology creation. Further, as he saw it, this system has emergent properties, including
internal needs with external expressions as it interacts with the rest of the world. He was envisioning a system for which no word existed (Kelly 2010).

Technology is humanity’s accelerant (Kelly 2016). Our technium is different from the technium 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 did not spring full-blown from nothing; it evolved from the technium of the recent past, which evolved from the previous technium, and so forth. The technium of a time and place supports the noosphere of the time and place and is modified by that noosphere: they are interdependent. With regard to the conflict in the noosphere, the technium provides the computation, storage and transmission mechanisms for the conflict taking place in the minds of humans. When movable type supporting cheap printing entered the technium of the time, the conflict of the noosphere gained another mechanism to add to human conversation and penned letters. Martin Luther’s thoughts were spread throughout Europe in a new way. The technium includes hardware such as the printing press; however, it also includes conceptual mechanisms, such as the technical tools of persuasion.

The Noosphere

The noosphere, the total information available to humanity, is expanding exponentially. In today’s technological world, the noosphere is inextricably intertwined with the technium. The infrastructure of the noosphere is rapidly changing. Favored information access with analytics is critical (Aspesi & Brand 2020).

Teilhard de Chardin envisioned the noosphere as collective human consciousness, the next evolutionary step (Ockham 2013). Kevin Kelly reintroduced this concept in his book, The Inevitable, and even used it to refer to a possible future world brain (Kelly 2016). We will leave out the speculation. Thus, we restrict the concept to refer to the sum of human knowledge.

Epistemology, the theory of knowledge, its methods, validity, and scope, can no longer be relegated to abstract philosophy. The prevalence and power of fake news and related suspect information artifacts has made it salient to everyday life. Normally, we think of information as pertaining to facts—true things. However, when you think about it, this concept of information has never been accurate. The ancients accepted many things that we now know to be false: for example, the sun does not revolve around the earth. In scientific domains, we accept that our data have measurement errors, at best, and that our scientific theories are subject to modification, even paradigm shifts, as our understanding improves. Such things belong in the noosphere. We regard the scientific conflicts of information validity as benign conflicts in the noosphere. There are also malign conflicts in the noosphere. During World War II, the Allies sought to convince the Germans that the invasion that was to be in Normandy would occur elsewhere. They thus sought to corrupt the part of the noosphere perceived by the Germans, a malign act. Today, there is “fake news,” both real and falsely asserted (the assertion itself being the “fake news”). All of this
is in the noosphere. And this is part of the conflict in the noosphere. The noosphere provides the medium in which the conflict takes place.

An ontology is a tool for organizing what is known about a domain. It generally contains the elements of interest in the domain and relations among those elements. It may also contain multiple types of relations and other defining information. When particulars are added to the ontology, it is often termed a knowledge base. For example, bridge might be an element in an ontology about infrastructure, indicating that this is one class of infrastructure, and “London Bridge” might be a particular instantiation in a knowledge base. In a book that described an ontology for modern conflict, Hartley included several elements that are relevant to information conflict (Hartley 2020). This particular ontology covers much more than just information conflict and thus has a larger granularity than would be required for a complete description of information conflict. Upon occasion, we will describe parts of the noosphere and the technium in ontological terms.

**The Target: Humans**

Every facet of our complex humanness is measurable and targetable. There is a hierarchy of targets that extends from our plume and trail at the chemical level, through our psycho-social needs and drives, via our irrational aspects, to our educated, augmented optimal state. As the sum of human knowledge increases exponentially, it is not surprising that information ascends in power with Homo “Sapiens.” In his book, *The Virtual Weapon*, Lucas Kello said, “This then is the chief transforming feature of security in our time: Information has become a weapon in the purest sense (Kello 2017).” We address information conflict (which includes information war and the internal issues of conflicting information, "fake news", etc.) and bounded reality (both human and AI seeing only part of the world) and possible solutions. Thus, “Intentional Conflict in the Noosphere” refers to actions taken by significant individual actors, states, state-sponsored proxies or other non-state-group actors, to disrupt or modify the information available to humanity. In our case, we are concerned with the impacts on the U.S. and its allies.

Figure 1.1 shows one view of the relationships among the noosphere, the technium and humanity. The noosphere contains knowledge of the physical world and the mental world.

Some parts of the noosphere are false and are shown in the mental world because they do not represent reality. The technium also consists of things in the physical world, including things that intertwine with the mental world. It is shown as mostly contained in the noosphere; however, there are tools and techniques that we use but don’t fully understand, so a part of the technium is shown to be outside of the noosphere. Humanity is shown as partly in the physical world and partly in the mental world. It is shown as intersecting the noosphere, the technium and false knowledge. It can be argued that since the noosphere is the total knowledge of humanity, the noosphere should be contained in the representation of humanity. However, we have
chosen this representation to emphasize that the noosphere is the total information available to humanity and that no human knows it all and each person knows a very small portion of it. It is harder to argue that the technium should be contained in the representation of humanity, since so much of the technium consists of physical objects that are clearly not intrinsic to, but rather tools of, humanity.

This figure also suffers from this graphic’s dimensionality and the “apples” and “oranges” comparison. For example, the noosphere contains knowledge about the physical world and the technium contains objects in the physical world. This difference in the meaning of the intersections is the reason for the inclusion of the word “one” and its emphasis in the first sentence of this paragraph. Figure 1.1 is meant to help in the understanding of these important concepts, but does not show all possible relationships among them.

**Change**

Throughout human evolution, change was generally slow, driven by climate, culture and biology. Most of the time the rate of change would have been perceived as essentially zero (omitting daily and seasonal cycles. With the advent of human society, that has changed. The inventions of tools, agriculture, writing, money, and the formation of cities in prehistoric times caused humanly observable changes. The
The recent past has seen fundamentally important changes. Scientific advances, aided by experimentation and big data analytics, have converted persuasion from an art to a combination of art and science. Computer technology has yielded increased processing speed and capacity, increased memory both local and remote, and increasingly powerful software applications. Total computational power is increasing by a factor of ten each year (Seabrook 2019). The Internet has connected the world. Artificial intelligence and machine learning have begun a process of re-structuring many of the processes of civilization. Together, these four changes are making surveillance and control technologies ubiquitous.

These accelerating, paradigmatic, AI/ML changes have the effects shown in Table 1.1.
The rise of artificial intelligence/machine learning (AI/ML) and quantum technologies, sensing, computation, and communication will upend even more. These changes will affect things shown in Table 1.2. Information conflict can extend from individual interactions to the apex of international political power, framing the structure and meaning of information across digital and traditional media to individual computers and personal contact. This national security threat disrupts or modifies the noosphere through communication and computation, from fake news through cyber war to control of metanarratives, and is initiated by nation-states, non-state-groups, and individuals. Addressing our physical vulnerabilities is not sufficient. Because humans have predictably, systemically irrational traits and operate within bounded realities, we are vulnerable and our institutions are vulnerable. We discuss the character of the conflict, the nature of the battleground, and topics for preparation and prevailing in the conflict.

The force of natural evolutionary change is anentropic toward complexity, diversity and energy density (the opposite of entropic change, which is toward increasing disorder). Many changes that we see in society are anentropic. The motif in both is connectivity. The change in the noosphere (total information available to humans) and technium (technology as a whole system) is accelerating to a point that quantity brings change in quality, of the technium, culture and man.

Accompanying the changes will be changes in scale, connectivity, complexity, and the impact of randomness. As the changes grow, multiple paradigm shifts are extant and more can be expected.

| Table 1.1 | Changes due to AI/ML |
| --- | --- |
| Many businesses and even industries are becoming obsolete; |
| Hardware and software are becoming outdated more rapidly—before we have a chance to become expert or even competent on something, it is replaced and we are beginners again; |
| Machines, processes and environments are becoming cognified—computer enabled and connected; |
| On the other hand, some things no longer require excessive levels of expertise or vast financial backing, enabling malicious use by more individuals, rather than just by governments and their proxies. |

| Table 1.2 | Effects of AI/ML, quantum, and other technologies |
| --- | --- |
| Power and its distribution, warfare and how and by whom it is waged, how peace and prosperity can be achieved; |
| Commerce, industry, education, and research; |
| Our understanding of man, his vulnerabilities and potentials; |
| Trust, finding truth, social membership, human networks, the construction of identity, and |
| Emergent new forms in the system of complex adaptive systems we call cognition. |

The rise of artificial intelligence/machine learning (AI/ML) and quantum technologies, sensing, computation, and communication will upend even more. These changes will affect things shown in Table 1.2. Information conflict can extend from individual interactions to the apex of international political power, framing the structure and meaning of information across digital and traditional media to individual computers and personal contact. This national security threat disrupts or modifies the noosphere through communication and computation, from fake news through cyber war to control of metanarratives, and is initiated by nation-states, non-state-groups, and individuals. Addressing our physical vulnerabilities is not sufficient. Because humans have predictably, systemically irrational traits and operate within bounded realities, we are vulnerable and our institutions are vulnerable. We discuss the character of the conflict, the nature of the battleground, and topics for preparation and prevailing in the conflict.

The force of natural evolutionary change is anentropic toward complexity, diversity and energy density (the opposite of entropic change, which is toward increasing disorder). Many changes that we see in society are anentropic. The motif in both is connectivity. The change in the noosphere (total information available to humans) and technium (technology as a whole system) is accelerating to a point that quantity brings change in quality, of the technium, culture and man.

Accompanying the changes will be changes in scale, connectivity, complexity, and the impact of randomness. As the changes grow, multiple paradigm shifts are extant and more can be expected.
Defining Revolutions

Lucas Kello said, “The revolutionary potential of technology resides not in the invention itself but in its political and social effects (Kello 2017).” In looking at the type of revolution that computers and the Internet might induce, Kello started with a description of the current international relations theory, which describes a nation-state system, derived from the 1648 Treaty of Westphalia. This Conventional Model, also known as the Westphalian Order, consists of three sets of assumptions.

The first set of assumptions concern the organizing principle of the system. The units of the system are defined as the possible actors, such as nation-states, citizens, and an imperial hegemon. Each unit has its possible goals and capabilities defined in these assumptions. In the Conventional Model, states are the main units.

The second set of assumptions concern the structure, that is the relationships among the units. For example, the assumption that the units share a basic interest in survival and maintenance of order leads to a moderation of the rivalries among the units.

The third set of assumptions concern procedures, the laws, norms and institutions that the units have set up to govern their interactions.

Kello used these sets of assumptions to define a conceptual framework of varieties of revolutions. He described three varieties, from a third-order revolution, the least wide-ranging, to a first-order revolution, the most comprehensive.

A **third-order revolution** involves systemic disruption. In this type revolution, the structure is not affected. The conduct of the units may be disrupted, perhaps disastrously for some; however, the type of units that are the main units (here states) remain the main units. Kello described two types of change that fit into this type of revolution. The first type has to do with “material ingredients of power.” This can lead to changes in the relative dominance of particular states. The second type has to do with changes in the procedures. For example, changes in what is considered to be moral warfare or competition fall into this category. Thus, a third-order revolution can be extremely disruptive to certain states, but leaves the nature of the system basically unchanged.

A **second-order revolution** involves systemic revision. In this type of revolution, the structure is not affected; however, the procedures are profoundly affected. Kello described the Soviet Union’s actions to change the nature of internal workings of other states as an example of this type of revolution. He also described the project of creating the European Union, in which the procedures of interactions of the states in the European Union were radically changed, as an example of a second-order revolution.

A **first-order revolution** involves systems change. In this type of revolution, the nature of the units is changed. The structure of the system is affected. The existence of states may be challenged or their dominance in the system may be eliminated or greatly reduced. For example, the creation of an effective world government would constitute this type of revolution. Alternatively, the replacement of states by international corporations as the dominant actors would constitute a first-order revolution.
Kello described this as the replacement of the Conventional Model with some other model.

The meaning of the word “revolution” in Kello’s work differs somewhat from that of Fig. 1.2. Kello focused on the international world order; whereas the revolutions in the figure are of a larger significance, changes in the social order of mankind as a whole. Conceivably, one of these larger significance revolutions could leave the Conventional Model intact, just irrelevant.

The Cyber Revolution

Kello evaluated the existence of cyber capabilities and actions against his definitions of third and second-order revolutions and concludes that there are situations in which these capabilities and actions might be instrumental in causing revolutions of these orders. However, it is in the evaluation of the possibilities of a first-order revolution that the danger seems highest.

Kello argued that we already have a “partial but still notable force of systems change.” That is, we are undergoing a first-order revolution. He said, “This trend is evident in three ways. First, states are not the sole relevant source of threats to national security; nontraditional players such as political activists, criminal syndicates, and religious extremist groups can also cause significant harm against governmental, financial, even military interests. Second, states are not the only, or in some cases even the primary, providers of national-security. In some areas of national security, such as the operation of vital computer infrastructures or the collection and encryption or decryption (in forensic investigations, for instance) of personal data, the private sector is more important. Third, the traditional units are no longer able to maintain full control over the dynamics of conflict [against and] among them. Civilian culprits can disturb—sometimes gravely—the fragile political framework of interstate affairs (Kello 2017).”

More than Cyber

The conflict matrix of our age of accelerating paradigmatic change, including new forms of cognition, requires polythetic, multiordinal strategies, talent from new and transdisciplinary communities of knowledge, and minds prepared to meet the unexpected. The advances in persuasion science can use captology (computer assisted persuasion) and narratology on time scales ranging from the “always-on” news feeds to shi. Lifelong learning for all must address the exponential growth in the sum of human knowledge, the rapidly changing infrastructure of knowledge access, and new understanding of man’s vulnerabilities and augmented potentials.

Kello’s revolution is based on what may now be considered traditional computer issues: computers, networks, cognified machines, and malware. Other than malware,
these issues ignore the growing capabilities of computers. Artificial Intelligence (AI) was originally envisioned as creating general, flexible human level intelligence (or better) in a computer. We have not (yet) done that; however, we have created extremely powerful tools that are conventionally called AI and the methodologies of machine learning (ML). Kai-Fu Lee described his view of the coming AI/ML revolution in his book *AI Super-Powers* (Lee 2018). This vision is one of a “larger significance” revolution that begins where Kello’s first-order revolution leaves off and achieves a revolution in the sense of Fig. 1.2.

Additionally, quantum computing, communication and sensing are here in their embryonic stages. As they mature, we can expect major disruptions in digital security. The current security processes are expected to be easily defeated by quantum decryption. This is not just a “future problem.” Encrypted files and communications that are stolen today will be decrypted (retrograde decryption) in the future. The full scope of its coming impact is unknown. If Lee’s revolution is not as vast as he expects, quantum computing may provide the substitute. All of this is coincident and merging with the new persuasion science. The conflict is more complex, multi-domain, trans-domain, polythetic, multidimensional, more rapidly adaptive, and more patient than any previous conflict in history. We face adversaries who engage in unrestricted, rule-less means. Revolutions in the form of paradigm shifts are extant.

The exponential increase in the sum of human knowledge and its applications in the technium have brought emergent forms of the complex adaptive systems that we call cognition. (For example, we now discuss cognition in machines, where its quality, not its existence, is the topic.)

*Sensing—the Surveilled World (the Panopticon)*

In the Acknowledgements to his book, *Out of the Mountains*, David Kilcullen talked about leaving off of thinking about conflict in urban areas close to the sea to concentrate on the immediate wars following the attacks on 9/11 in 2001. He then said that when we return to thinking about them,

“... we’ll find that the same old challenges of the urbanized littoral remain, but that much of what we thought we understood has changed. Not only have enormous advances been made over the last decade in cloud computing, complex systems theory, big data analysis, remote observation, and crowd-sourced analytics—allowing new insights into old problems—but vast amounts of real-time data are now available to inform our thinking. Most important, the environment itself has changed. The level of connectivity and networked interaction (among populations all over the planet, and between and within coastal cities) has exploded in the last decade … (Kilcullen 2013)”

From a sensing point of view, the technology to sense and the technology to be sensed are different in capacities and in kind (for example, nuclear forensics). Not only can (by comparison) almost everything said or done be sensed, it can be attached to a person, analyzed, (more or less) “understood” automatically, curated, and recorded. These potentials can be realized for financial gain, political influence,
ideological conversion, and, in certain nation-states are being used to control populations. We are approaching the Panopticon where all is seen, and much is known and acted upon. The age of experimentation (on digital site users) is improving the vision of Panopticus.

**Complexity Science and Network Dynamics**

The first page of each Springer Complexity series book says, “*Complex Systems* are systems that comprise many interacting parts with the ability to generate a new quality of macroscopic collective behavior the manifestations of which are the spontaneous formation of distinctive temporal, spatial or functional structures” [emphasis added] (Fellman, Bar-Yam, & Minai 2015). The macroscopic collective behavior referred to is also called an “emergent property.” Because there may be complex systems that are not adaptive systems and do not exhibit emergence, we prefer to use the phrase “complex adaptive systems (CAS).” The simple truth is that a system for which a comprehensive description cannot be derived from a complete description of its parts is a CAS. It is more and different from the sum of its parts.

There are several organizations that study complexity science, such as the New England Complex Systems Institute, of which Yaneer Bar-Yam is President (New England Complex Systems Institute, n.d.). Perhaps the most famous is the Santa Fe Institute, founded by Murray Gell-Mann (Santa Fe Institute 2016).

A 2004 report by the Oak Ridge National Laboratory (ORNL) (Hartley, Loebl, Rigdon, Leeuwen, & Harrigan 2004) stated, “that without explicit treatment of commonality, undesirable and wholly unexpected performance will emerge to compromise the predictability, reliability, and consistency of complex systems and systems of systems (SoS).” [A version of this was presented at an international conference in 2005 (Loebl & Hartley III 2005).] The word “commonality” referred to functions in the parts of a system that should have the same representation and to the need for these functions to correspond to external reality. A 2018 review of the book *Meltdown: Why Our Systems Fail and What We Can Do About It* described the message of the book with the caption, “Thanks to dense networks and the complacency of groupthink, small glitches can cascade into catastrophic failures (Shaywitz 2018).”

The information battleground is not a simple, deterministic, Newtonian system. It is not just the sum of the individuals and the hardware/software objects that comprise it; but it also includes the interactions among them. It is complex and adaptive.

**The Six Domains of Conflict**

The US Department of Defense (DoD) currently lists five domains of military conflict: land, sea, air, space, and cyberspace (Chairman of the Joint Chiefs of Staff 2017). The land, sea and air domains are familiar, having been involved in conflicts
for a century in the case of the air domain, for all recorded history for the sea domain, and from pre-historical times for the land domain. The sixth domain, cognition, is extant but only now being recognized.

Figure 1.3 illustrates the “familiar” attacks: military attacks by a nation or proxies, which affect individuals, companies and our nation; terror attacks by non-state actors; economic attacks by nations or companies; and diplomatic “attacks” by nations. The U.S. is undergoing or threatened by all of these types of attacks from various opponents.

**The Fourth Domain: Space**

The space domain has not yet been involved in direct conflict and the extent of its possible involvement is not well-defined; however, there have been plenty of science fiction stories written about conflict in space to provide ideas of what might be possible. The U.S. has invested considerable resources in space over the last 60+ years. More than the investment, however, the value of space assets in terms of utility is large and growing. Satellites provide standard voice and television communications, location data through GPS systems, and internet connectivity.

The National Aeronautics and Space Administration (NASA) has announced its plan for a return to the Moon and human missions to Mars. A critical part of this plan is the Lunar Gateway—a spaceship in orbit around the Moon. The Gateway will provide access to the lunar surface, but also may become the hub of a cis-lunar economy (NASA 2020).
These assets are all vulnerable to both kinetic and cyberattacks. Julia Curlee, in a National Defense University capstone project, said, “An examination of potential scenarios for a war in space with China across the conflict spectrum suggests that Chinese attacks on US communications and Global Positioning Satellites (GPS) would likely feature early in a conflict (Curlee 2020).” The U.S. Space Force was created on December 20, 2019 to address these vulnerabilities and threats (Military.com 2020). Part of its mission is “to protect U.S. and allied interests in space and to provide space capabilities to the joint force (US Space Force 2019),” thus including defensive and offensive operations with an implied need for space superiority.

The Fifth Domain: Cyber

The cyber domain is so new that much of the applicable terminology is either unfamiliar to many or has varying definitions, depending on the source. We will use the following definitions when writing in our voice; however, when writing in the voice of a source, we will use that source’s definitions. Our definitions are provided by Lucas Kello, who approached the problem from an international relations perspective as opposed to a military perspective (Kello 2017).

Cyberspace is all of the computers and networks in existence, including computers that are isolated from networks (air-gapped). Note that this includes embedded computers, such as those in cars (at least one in each modern car, with some having more than 30 computers). Cyberspace is manipulable through code (and on/off switches).

The term “cyberspace” conjures a picture of an amorphous continuum; however, the reality is different. Figure 1.4 is a cartoon of the Internet. It is based on a backbone of links and nodes, illustrated with fat lines and large red circles. The backbone nodes are connected to major nodes (medium-sized red circles) with major links (medium-width lines). Ultimately, the major nodes are connected to various computers (red dots) by links (thin lines). (This is a cartoon, so there can be many intermediate sized links and nodes.) Some of these computers are server
farms that comprise various “Clouds.” Some of these computers are parts of local area networks (LANs), such as are found in many homes with multiple computers. (Most computers are actually connected to wide area networks (WANs), rather than directly to the Internet. Adding WANs to the cartoon would have made the drawing too cluttered.) The internet of things (IoT) is extant and rapidly growing. Some of these things are shown as green dots, connected (often wirelessly) to the Internet. One small group in the figure represents a few of the microprocessors in a car. The cyberspace is definitely not amorphous, just so complex that it is hard to grasp in its totality. Rothrock estimates that as of 2018, the number of nodes was about one trillion (Rothrock 2018).

The **Cyber domain** includes cyberspace and all of the human and institutional actors who operate and control cyberspace. The cyber domain also includes machinery that is controlled by cyberspace. The cyber domain affects and is affected by cyberspace and the human part is responsive to human inputs of a psychological, social and political nature.

“**Cybersecurity** consists of measures to protect cyberspace from hostile action.” It also includes measures to “protect the cyber domain from threats emanating from” cyberspace. When cybersecurity involves the military, it is called **cyber defense**.

**Information security** is used to describe the control of information flows. This can be the suppression of subversive information in an autocratic state or efforts to control the exchange of child-pornography. Information security is often conflated with cybersecurity.

“**Malware** denotes software designed to interfere with the function of a computer or degrade the integrity of its data.” Malware may directly affect cyberspace or may do so indirectly by affecting human operators who then install malware into cyberspace (usually inadvertently, although conceivably the threat of harm to the operator might lead to the operator knowingly installing the malware).

The term **cyberweapon** is restricted to malware that is capable of and intended to do sufficient damage that the effects would be classified as the effects of a weapon in the realm of international relations.

“**Cybercrime** entails the use of a computer for an illicit purpose under the existing penal code of a nation.”

“**Cyberattack** refers to the use of code to interfere with the functionality of a computer system for a political or strategic purpose.” “Neither the goal nor the effects of a cyberattack need to be contained in cyberspace.” “If the effects of a cyberattack produce significant physical destruction or loss of life, the action can be labelled **cyberwar**, a term that should be used sparingly.”

“**Cyber exploitation** refers to the penetration of an adversary’s computer system for the purpose of exfiltrating (but not defiling) data.” When the goal is to steal military or industrial secrets, the exploitation is known as **cyber espionage**. If the goal is to obtain sensitive information about a public official or organization to be released at an opportune influence government actions or undermine public confidence, then the exploitation is known as [cyber] **kompromat**.
Rothrock discussed the 2013–2014 Target attack, the 2014 Sony attack, and the 2016 Democratic National Committee (DNC) attack. He discussed three commonalities: all were network attacks; all had remote origins; and although all were cyberspace attacks, all had serious consequences in the real world (Rothrock 2018).

**Cognition, the Sixth Domain**

When we examined the cyber domain, we realized that it was a major but not final step in addressing a larger contest for power, a contest for cognitive superiority. New warfare confronts three emergent foci within technology writ large: (1) AI and other new forms of cognition; (2) advanced gene editing and synthetic biology; and (3) the subset of technologies labeled immersive technologies—extended reality (xR) (virtual reality (VR), augmented reality (AR), 360° video, and mixed reality). These foci are within the cognitive or sixth domain.

This cognitive domain involves a complementarity as it is both a power augmenting part of each of the current five domains but importantly also an emergent (more than the sum of the parts) separate sixth domain. It addresses the new forms of cognition, the unending exponential increase in the sum of human knowledge, and new communities of knowledge. It is intertwined with competing world views, grand strategies and metanarratives of power, diplomacy, science, metascience, and lifelong learning. It molds trust, social membership, meaning, identity, and power. The ultimate target of all conflict is the human mind, individually and collectively. This ultimate conflict domain is the Sixth Domain, the cognitive domain. The cognitive domain is both part of the other five domains and an emergent entity unto itself.

The cognitive domain entails a broad view of today’s accelerating change in man in his matrix—discrete accelerating changes in cognition, in the technium (particularly, but not limited to, AI/ML) and the noosphere, in connectivity and complexity, and in our understanding of man’s vulnerabilities and potentials. The DoD recognized that today’s conflicts involve more than just the military (Hillson 2009). The DIME paradigm represents this realization. Four “levers” of national power were identified: diplomatic, informational, military, and economic, as shown in Fig. 1.5.

The DIME paradigm was a description of the national levers of power. However, today we have to contend with non-nation-state actors, including individuals, who have the power of terrorism, asymmetric warfare, biological warfare, and cyber warfare to act against nation-states (or other organizations and individuals) as only nation-states could in the past. Accordingly, we have changed the label to be just “levers of power.”

As the figure shows, the conflict domains for diplomatic, informational and economic power are not usefully divided into land, sea, air, and space domains; however, they have their own traditional conflict domain divisions and they operate in their own part of the cyber domain. The inclusion of cyber within the diplomatic lever is arguable: the discovery and publication (or threat thereof) of politically damaging materials through cyber exploits could be contained in the informational lever; how-
ever, the particular impact of such an exploit and the potential for others leads us to include cyber. Similarly, the inclusion of cyber within the economic lever is based on the impacts of economic cyber exploits.

The informational lever of power is of particular interest in this book. Information conflict takes place among nation-states, group-entities and individuals. It took place before the advent of computers and continues after their creation. The informational lever of power originally could be characterized as spying (obtaining information from the enemy or competitor), deception (ensuring the incorrectness of the information that the other obtains), and counterintelligence (thwarting the attempts of the other to obtain information). The addition of the cyberspace domain has not removed these operations, but added to them. The technium can aid in the spying, deception and counterintelligence and can be used to corrupt the computers and cognified systems of the other side.

We have called the cognition domain the “sixth domain” (counting among the military domains) because we now have the ability to affect the cognitive abilities of humans (and augmented humans). We have practiced the art of persuasion (or rhetoric) since before the time of Sun-Tsu and Aristotle, but only recently have been creating an additional science of persuasion, which vastly improves the effectiveness of persuasive actions. We have developed new learning science interventions that affect cognition. In addition, we have developed tailored pharmaceuticals that affect cognition (beyond the unfocussed effects of naturally occurring drugs such as peyote, opium and the volcanic gases of the Greek oracles).

We are familiar with the need for air, land, and sea superiority. The corresponding need for space and cyber superiority is obvious, as is the need for diplomatic, economic and information superiority. However, over all we must achieve and maintain cognitive superiority. J. R. R. Tolkien’s saga, The Lord of the Rings, contains an *apropos* poem:

*Three Rings for the Elven-kings under the sky,*  
*Seven for the Dwarf-lords in their halls of stone,*  
*Nine for Mortal Men doomed to die,*  
*One for the Dark Lord on his dark throne*  
*In the Land of Mordor where the Shadows lie.*
Cognitive superiority is the “One Ring to rule them all.”

The Time Frames and Battlefields

The time frame of war is now multiordinal, from “Fast wars … something that we haven’t really understood yet (O’Neill 2019)”, that move at the speed of the electron, to the Hundred Year Marathon (Pillsbury 2015) using shi (Qiao & Wang 1999; Chinese Academy of Military Science 2018).

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. In the West, we had Aristotle (384—322 B.C.). In his book, Rhetoric, Aristotle defined his subject matter, “as the faculty of observing in any given case the available means of persuasion (Aristotle 2004).” Rhetoric is persuasion through verbal means. Aristotle emphasized ethos (credibility), logos (logic), pathos (emotion) and kairos (propitious timing). Now we have TV, the Internet, and cognified objects—all trying to persuade/sell us something. Persuasion is not just verbal-aural; it includes visual perception, still and motion, real and fake; and will include remote touch, taste, and scent in immersive technologies. Persuasion science continues to transform the art of persuasion, armed as it is with new methods and metrics of sensing and experimentation and targeting human hybrid (augmented-human) cognition. Utilizing these methods together with addictive technology, persuasion is ever more central to attaining power for statecraft, computational propaganda, marketing, lobbying, public relations, and narrative and memetic warfare using “slogans, images and video on social media (Donovan 2019).” This is also part of the beyond-limits battlefield of the Chinese (Qiao & Wang 1999).

Persuasion is ubiquitous across all circumstances of human endeavor. It varies in combinatorial complexity, can be apparent or hidden, and is constructed for immediate use and delivered with urgency or with patience for the long game. Overlapping waveforms of influence come at all scales of time from the momentary to the long game and can be wrapped in disparate packages, truth, deception, perfidy, serendipity with discernment of opportunity to shi. Shi is 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 (Pillsbury 2015).

As the battle moves from low intensity conflict toward warfare, the tactics of influence move from persuasion to coercion to control. This is true whether the lever being used is diplomatic, informational, economic, or military. As Carl von Clausewitz said, “war is only a branch of political activity; that it is in no sense autonomous (Clausewitz 1993).” [The emphasis is contained in the source.] In Fig. 1.6, we take a step back and derive all actions from the cognitive domain, with
the purpose of the actions being to impact the cognitive domain of the opponents. Naturally, the opponents are doing likewise, with the positions reversed. Achieving cognitive superiority is required for winning.

What is the nature of the battleground? While the cognified objects, hardware and software, are certainly part of the battleground, the most significant part is the wetware—human cognition. It is people who are affected by compromised objects and by their own exploitation. The nature of computers (at least non-quantum computers), cognified objects (objects with some level of cognition abilities), and their connection through the Internet are fairly well known and we will comment on them and their attributes without dwelling on them. However, recent advances in understanding neuro-cognition, dynamical systems theory, control theory, and human-computer interface optimization are not so widely known. These areas require a more extensive discussion. Winning on the information battleground requires an understanding of all facets of the battleground and time frames, most especially including an understanding of man and his matrix.

The imminent expansion of the digital battleground into extended reality (xR) as augmented reality (AR), virtual reality (VR) and multiple immersive technologies is terra incognita for persuasion and conflict. Research knows little of how AR will influence social interaction. What will be the effect of having a networked augmented avatar as a companion? Consider the work of the Stanford Virtual Human Interaction Lab, described on its website (Stanford University VHIL 2019).

**Biosecurity (the Essential Tool Is Information)**

A recently more obviously important, arguably under-addressed area in the sixth domain is biosecurity, in which there is “an expanding range of concerns (Evans et al. 2020).” Germs entering unprotected populations have repeatedly transformed history on an international scale (Diamond 2020). Whether the biological agents are
(1) feral diseases, (2) come from unintended releases, or (3) purposefully released, they can produce massive health and economic effects, as evidenced by the COVID-19 pandemic of 2020. N. b., although highly contagious, the lethality of COVID-19 is much lower than other biologic agents such as Ebola and Smallpox.

A low barrier to entry into the bio-war domain, the ability to scale an attack, and potentially problematic attribution make this an area of essential focus, needing best-in-class expertise and ability. Genomic science, advanced genetic engineering, synthetic biology, knowledge of network spread dynamics, augmented computational biology, and high-throughput experimentation (HTE) with automation and robotization contribute to the problem (Peplow 2019). All of these, together with big data analytics, network science, persuasion science, logistical and communication expertise, must be coordinated for security and defense (Desai 2020). Further, no knowledgeable adversary will miss the opportunity to superimpose an “infodemic (World Health Organization (WHO) 2020)” on an epidemic.

Synthetic biology can now create or modify—weaponize—a germ. The organism might be selected for high infectivity, high lethality and a low observed mutation rate. A vaccine could be produced, giving vigorous long-term immunity to the group (or country’s citizens) who receive the vaccination. The vaccination program could be presented with a false narrative or be clandestinely incorporated as part of a polyvalent established vaccination program. The secret development, selective vaccination program, and release of such an organism under attributional cover and coordinated dissociative “infodemic” would likely produce a catastrophic effect on the target. The unassembled modules of such a scenario are in forme fruste, but extant. With purposeful biosecurity threats we must consider multiple releases (vectors) in form, location and timing, in parallel with infodemics and complex, multi-domain orchestrated attacks.

The United States must develop “global readiness” with an international “shared understanding and shared vocabulary for pandemic preparedness with an early warning system that tracks global disease trends and distributes accurate real-time information.” Recommendations include: (1) Full support of the U.S. Pandemic Response Team within the National Security Council, including equipment surge capacity. (2) Expand public health capacity including surveillance structure, education and vigorous extant and more scalable vaccination capacity. (3) Innovation accelerators such as Coalition for Epidemic Preparedness Innovation (CEPI), which can develop a platform or platforms for technology innovation for rapid vaccination development (Desmond-Hellmann 2020), (4) “experimentation in biosecurity governance” with “sharing of case studies.” “At present no capability for systemic learning about the effectiveness and limitations of current biosecurity governance exists (Evans et al. 2020).”
The Combatants

We are facing today multi-agent, multi-pronged, multi-faceted attacks on our civilization. There are multiple national opponents, who are acting individually or through proxies, using multiple modes of attack on multiple facets of our national life. There are also multiple non-nation-state opponents, both external to our country and within it, who are doing the same. There are also individuals or small groups of individuals, acting on economic motives, doing the same. Additionally, our social media have created an environment that fosters individual attacks on other individuals. Further, there are the traditional corporate activities that seek to advance their own ends through influence operations. Moreover, our networked system creates cognitive demands that most users are not equipped to handle. When the computer was represented by large machines, tended by acolytes in white lab coats, users could safely remain ignorant of the demands of the technology. Now, each personal computer, smart phone, smart TV, or other device requires configuration and tending by its owner, who has not been supplied with a white lab coat or the knowledge and experience to service its demands (Rothrock 2018). Together, these actors are creating an environment of constant conflict, as illustrated in Fig. 1.7.

This constant conflict does not replace the familiar attacks illustrated in Fig. 1.3; rather these multi-agent, multi-pronged attacks are added to the familiar attacks. The individual conflicts comprising the constant conflict involve the individual, countless groups, and nations, using and exacerbating the changes already described. All of the conflict is not instantaneous. While some attacks, such as a particular phishing email, may be handled with a brief moment of attention, others are “persistent enduring attacks” (Rothrock 2018). In addition, the number of attacks continues to grow. CrowdStrike reported the number of events globally was 90 billion
in 2017 and 240 billion in 2018—per day (Crowdstrike 2019)! While the technium and the noosphere are the means, media, and immediate targets, the cognitive domain is the actual domain of conflict.

Winning in the Sixth Domain

We have a limited history to draw from because of the brevity of experience with the digital world, its accelerating rate of change, and the preference for secrecy concerning adverse experiences with the digital world. 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” may be at the speed of light over our fiberoptic networks. Our fate may be determined in nanoseconds after a clandestine polythetic prologue. We do not have the luxury of being unprepared.

The Cognitive Battleground

Computer systems are not human-level cognitive systems (yet) and the cyber domain is but part of the cognitive domain. However, the cyber domain is closer to the cognitive domain than are the physical domains of land, sea, air, and space. Therefore, the cyber conflict produces an understandable introduction to the larger cognitive conflict.

According to Rothrock, 76% of the respondents of one study reported a computer system compromise in 2016, up from 71% in 2015 and 62% in 2014 (Rothrock 2018). That means that every system should expect to be compromised—successfully attacked—despite having good defenses. We certainly need defenses of various types; however, we also require resilience to bounce back from successful attacks. Rothrock ascribed the following definition of resilience to Andrew Zolli and Ann Marie Healy. Resilience is “the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances (Rothrock 2018).” The U.S. demonstrated resilience after the attack on Pearl Harbor on December 7, 1941. We will need systems resilience at all levels. Simultaneously, we must successfully engage the Hundred-Year Marathon—the long game. Rather than a win-win game, others play a zero-sum game.

Kinetic superiority is no longer a certain guarantor. Now with multiple weapons and layers hidden by method and their “local habitation and name,” we must have cognitive superiority.

The goals and assumptions of humans, their differences, and perceptions and misperceptions about them are part of the cognitive domain. Samuel Visner, the Director of the National Cybersecurity FFRDC at MITRE, said the battleground is the “exercise of influence in cyberspace—as an instrument of national power (Visner
2018).” Significantly, he said that cybersecurity is viewed differently by different people, as shown in Table 1.3.

This last point of view is a critical difference between us and some adversaries. He said we regard cyberspace in much the way we regard the seas, as a global commons, whereas some countries look to claim portions of it as “territorial waters.” If the goal is cognitive superiority, it is critical to understand the opponent’s cognitive domain, from world-view to tactical view.

The battleground for cognitive superiority involves complex adaptive systems and systems of systems (SoS), with intelligent nodes, links, signals, and boundaries, digital, hybrid and human.

### Cognitive Superiority (Condensed)

The elements of cognitive superiority (listed here) will be discussed in the body of the book. In the conclusion (Chap. 8) we will present an expanded description of cognitive superiority.

Cognitive superiority is a relative attribute—sustained better thinking, more rapid learning, and superior information access than that of the opponents. Fortunately, it does not require that we are individually smarter than each of our opponents. It does require that collectively we are smarter. Achieving cognitive superiority will require an expanded understanding of the conflict, as shown in Table 1.4.

### Organization of the Book

Our questions about the complex adaptive systems of information as power require investigation into numerous domains of knowledge, covering many disparate, multiply interconnected topics. Some topics will be principally addressed in a single chapter and only mentioned peripherally elsewhere. Several themes are threads that weave through the whole book, not existing solely in one chapter. Therefore, some repetition is necessary so that the reader isn’t required to continually search back for earlier parts of the thread. More importantly, the complexity is best apprehended and appreciated from multiple points of view. The topics are artificial intelligence
(AI) and machine learning (ML), atoms and bits, biosecurity, change, cognitive superiority, communication and connectivity, complex adaptive systems (CAS), education, intelligence amplification (IA), network structure and dynamics, new knowledge of man, persuasion, profiles, quantum technologies, social membership, surveillance with experimentation, and trust. These are highlighted in the descriptions of the chapters below.

A note on terminology: the terminology within the domain of discourse of this book is fluid. The U.S. government has its own terminology, as do foreign governments, corporations, and individual writers. For example, Lt. Gen. Stephen Fogarty, commander of the U.S. Army Cyber Command, says that his command may change its name to something like the “Army Information Warfare Operations Command or Army Information Warfare Dominance Command (Seffers 2018).” There are two points, first that there are discussions about the relative advisability of the terms “information operations” and “information warfare” and second that there is support for broadening the domain from just cyber to cognition. Throughout this book we will use terms that may or may not match the exact terms used by others; however, we are not aiming to define usage, but describe concepts. We have tried to make the meanings clear and will leave it to others to decide just what will be the best terminology.

Chapter 1 is this introduction, providing a statement of the problem: the multi-pronged, multi-agent, multi-mode, polythetic conflict in which we are immersed. It introduces the technium, the noosphere, the humans as the target, and the revolutionary, accelerating changes that are part of our matrix. The chapter discusses the five classical domains of conflict, land, sea, air, space, and cyber, and introduces the sixth domain, cognition. It also provides a brief statement of the cognitive superiority solution.

Chapter 2 describes the technium, our technological environment that contains the attack tools, digital, cognitive, and biological, and many targets of conflict. It discusses communication from a technical point of view, persuasion as a method of
attack, surveillance as a support to attacks, and trust as a defense. This chapter discusses the tools for gaining power over people and how they are used. It concludes with change trends in the technium.

Chapter 3 discusses the noosphere, the total information available to humanity, and our bounded reality. This chapter discusses the nature of information, how we think—and limit that thinking, and how we communicate. It discusses atoms and bits, education, communication and trust as parts of cognition, which is a prerequisite for cognitive superiority. It concludes with change trends in the noosphere.

Chapter 4 describes the target of the intentional conflict: humans. This chapter discusses how and why the attack tools work on humans. It includes salient features of human nature and our individual natures, such as irrationality, biases, and human communication—the new knowledge of man. The chapter also discusses the nature and centrality of persuasion in human communications with respect to attacks. It discusses surveillance as a means of building profiles of people. Finally, change trends in our understanding of humanity are described.

Chapter 5 discusses several selected sciences and technologies to provide a deeper look at some of the transformative influences of our environment. The topics include CAS, novelty, AI/ML and the human brain, human and computer networks, quantum technologies, immersive technologies, and biosecurity. It also includes new technologies that may influence the future: superconductivity, nuclear thermal propulsion, and 3D printing. It discusses communication and connectivity as part of network science.

Chapter 6 describes the adversarial environment. Adversaries include individuals, groups, companies, non-state actors, nation-states, and digital adversaries. Their goals and intents include personal enmity, influence, surveillance, economic gain, philosophical and ideological causes, maliciousness, control, and war. The chapter concludes with a discussion of why this is important, now, more than ever before. It discusses persuasion as part of influence, a goal of many types of adversaries, and surveillance as an intermediate goal of many types of adversaries.

Chapter 7 describes the engagement. It is divided into two parts. The first part describes the strategy for winning the conflict: education, information access, communications, and organizational principles. The second part describes how to address the ongoing conflict during the implementation of the strategy. It describes past, present and proposed organizations, commercial, governmental and hybrid. It includes an action portfolio, potential changes to the conflict environment, and ideas on operating in the conflict as it evolves.

Chapter 8 recapitulates the situation: the accelerating changes, atoms and bits, and humanity in the matrix. It concludes with a prescription for achieving cognitive superiority in detail, including a proposed organizational structure, and a rationale for a Manhattan-Project-scale effort.

An appendix with two parts, discussions of the salient contents of selected sources, organized by topic, and definitions of selected is included.

A wide-ranging bibliography and an extensive index are provided at the end of the book.