4 OPERATIONAL ENVIRONMENT

"Unlike the land, sea, air and space domains, cyberspace is continuously evolving and adapting along with each entrepreneur, inventor and actor that uses it." [173]
- Lieutenant General Edward Cardon

Humans are very experienced with conflict in the physical world. Traditionally militaries have organized for conflict in four domains, and those domains are used to characterize the physical environments in which military forces operate. The Land domain was first, but with the addition of disruptive new technology, militaries now recognize other new domains. With the advent of ship building came the Sea domain; aircraft forced the acknowledgement of the Air domain; and rockets, satellites, and orbital vessels led to the acceptance of the Space domain. Organizations tailored to engaging in combat in each domain emerged as armies, navies, and air forces. The Laws of Physics held in these natural domains, and appropriate strategy and tactics emerged, fueled by advances in technology.

The birth of computers and networking and the eventual ubiquitous nature of the Internet as a deeply intertwined component of prosperity and national security led nations to declare cyberspace as a fifth domain. This changed some long-held beliefs about what a domain is. No longer just describing physical aspects of the environment, the cyberspace domain implies that the definition of domain is expanded to include abstractions beyond physical space when describing an operational environment. This represents a significant change, and change can be hard for some. Debates occurred between many traditional military leaders and some of the more adaptive, forward looking, and typically younger, service members, but the change

held. The United States created U.S. Cyber Command, along with service-specific subordinate cyber commands for its Army, Navy, Air Force, Marine Corps, and Coast Guard. We haven't yet gone as far as creating a separate military service for Cyber, but some predict that it will come in time.

Cyberspace is novel in that it is man-made, and while the fundamental Laws of Physics still apply, many underlying attributes of the Cyberspace domain are very much under the control of human architects. Cyberspace crosscuts each of the physical planes, akin to a parallel plane. Most people and technology have a presence both in the physical world and in cyberspace.

Surrounding each of the five planes is the Electromagnetic (EM) spectrum, the field of electromagnetic radiation that surrounds everything (see Figure 4-1). Examples include visible light, radio waves, and X-rays. The EM spectrum is special in that it is present in each of the physical domains and provides the communications substrate upon which cyberspace operates. The spectrum is finite and can become crowded, so governments and militaries seek to perform spectrum management to prevent one organization's communications from inadvertently colliding with others'. Militaries use the EM spectrum to communicate information, which in turn leads to attempts by adversaries to jam signals, delay communications, or more subtly deceive users through misleading messages. Direction-finding tools are used to find the location of sources of electromagnetic radiation. In fact, the EM spectrum is so fundamental to military operations that there is an ongoing discussion about whether it should be designated as a sixth operational domain.[174]

Cyberspace represents flows of information to machines and humans. As we discussed earlier, these flows of information have a physical manifestation and can create physical effects by altering the logic of computing systems. Information also has a cognitive component, and the right flow of information at the right time will alter the decision making of humans, whether they be governments, militaries, insurgent groups, businesses, or individuals. We can expect militaries to operate in cyberspace not just to cause physical effects on the battlefield or to gather intelligence, but also to carefully target the decision making capabilities of allies, adversaries, neutral parties, and populations. The strong influence of social media on the recent U.S. presidential election by a foreign power is a good example.

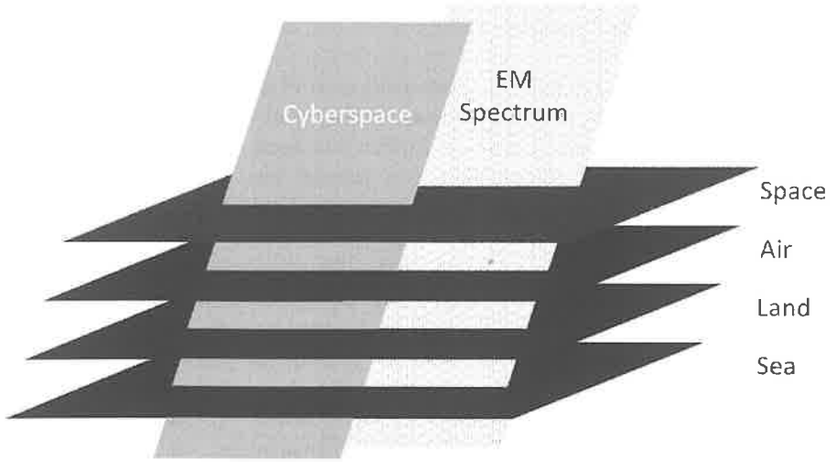

Figure 4-1: Diagram of the natural operational domains of Sea, Land, Air and Space, the cross-cutting man-made domain of Cyberspace as well as the Electromagnetic spectrum, which permeates all other domains.

The U.S. Military uses the concept of an Operational Environment (OE) to describe and analyze the conditions, circumstances, and influences that affect military operations.[175] This helps military members better understand the larger context in which they operate and how these aspects affect their employment of capabilities.[176] Actors work to shape the operational environment to their advantage to deter aggressors, seize the initiative, dominate in conflict, stabilize regions, and assist civil authority for themselves and allies. Most militaries would prefer to shape the operational environment to prevent conflict, but when it is necessary to seize the initiative, the goal is to dominate on the battlefield and return back to peace. See Figure 4-2 for a graphical depiction of such efforts from U.S. Military doctrine.[177]

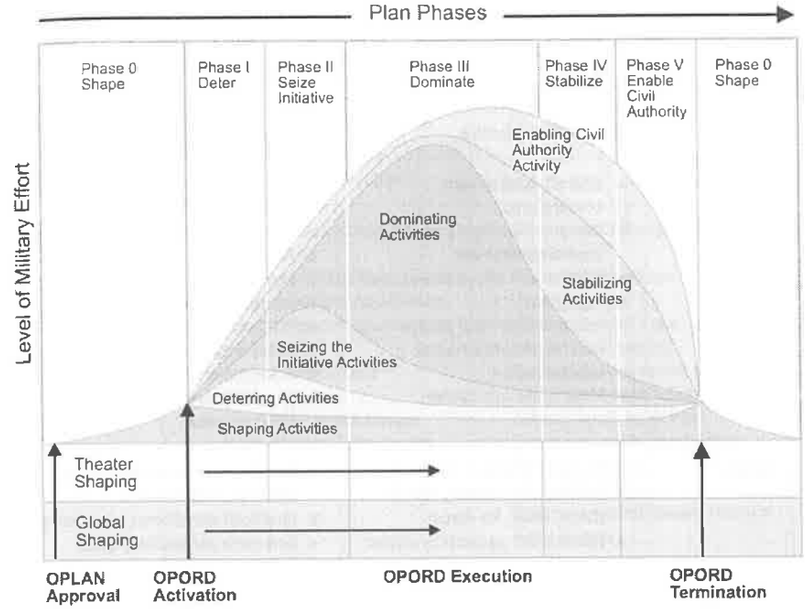

Figure 4-2: Notional depiction of phases of conflict. The U.S. Military prefers to shape the operational environment to prevent conflict, but prepares Operations Plans (OPLANs) to be ready. If conflict cannot be prevented, the U.S. Military issues Operations Orders (OPORDERS) to guide increasingly more aggressive military activities, with the goal of stabilizing the environment and enabling civilian leaders to transition to peace. Shaping of the military environment occurs throughout. (Image: U.S. Department of Defense)

Operational environments are complex and constantly changing. One useful framework for analyzing the operational environment uses the initialization PMESII-PT. Despite the unwieldy acronym, the concept is powerful and comprehensively includes key aspects that one should understand when considering operations in cyberspace: political, military, economic, social, information, infrastructure, physical environment, and time.[178] Table 4-1 provides key attributes for each of these areas. Note that the U.S. Army traditionally applies PMESII-PT to land domain activities, [179] so we've extended it to illustrate the framework's application in cyberspace operations.

Table 4-1: Using PMESII-PT to analyze an operational environment. The left column illustrates the traditional application. The right column applies the framework to cyberspace.

	Traditional Application	Cyberspace Application
Political	• Attitude toward your country/group • Centers of political power and type of government • Government effectiveness and legitimacy • Influential political groups • International/Inter-actor relationships • Major historical events	• Online political activity • Electronic voting • Online governance activities • Political messaging • Political fundraising • Recruiting • Political influence on cyberspace policy and standards • (Inter)national organizations governing use of the Internet and online access
Military	• Number, size, and capabilities of conventional military forces (Army, Navy, Air Force) • Government paramilitary/cyber forces • Non-state paramilitary forces • Unarmed combatants • Nonmilitary armed combatants • Military functions (including command and control, maneuver, intelligence, target acquisition, protective measures, logistics capabilities, intelligence)	• Number, size, and capabilities of military cyber forces • Unofficial/sanctioned cyber forces • Non-state paramilitary cyber forces • Noncombatant users and groups in cyberspace • Nonmilitary combatants in cyberspace • Maturity of SIGINT capabilities
Economic	• Per capita income • Key industries, agriculture, and natural resources • Employment status (poverty, percent unemployment) • Economic activity (exports, imports, inflation rate, debt) • Illegal economic activity • Banking and finance	• Electronic commerce activities • Permeation of ecommerce • Currencies (including cryptocurrencies) used online • Major payment card systems • Cost of online access • Online economic activity • Illegal online economic activity and marketplaces • Online banking and finance • Regulatory requirements
Social	• Demographics (population growth, density, immigration/emigration) • Volatility • Education (literacy rate, education level) • Major ethnic groups	• Degree of population with Internet access • Social media penetration and popularity • Technical literacy • Cyber cafes • Common online slang

	• Major religions • Major urban areas • Language(s) used • Criminal activity (effects on population, economy, and infrastructure) • Centers of social power • Cultural norms and values	• Online culture and social norms • Online communities and activist groups • Cyber criminal groups • Online anonymity • Identity spoofing
Information	• Media outlets (and their political slant) • Intelligence capabilities • Electronic warfare capabilities • Computer network operations capabilities • Deception capabilities • Freedom of media • Perception of media toward various relevant actor groups	• Government filtering of the Internet • Online news sources • Use of censors • "Sock puppets" / paid trolls[180] • "Fake" news stories • Extremist group online activities • Government-mandated cryptographic backdoors • Online deception capabilities • Freedom of online journalists/bloggers • Online sentiment toward relevant actor groups
Infrastructure	• Developed/developing regions • Building density • Utilities present • Transportation (routes into major cities, major choke points) • Fragility to adverse events	• Major data centers • Major ISPs • Major cell providers • Satellite ground stations (commercial / government) • Undersea cables • Cell/Microwave towers • Reliability of power grid • Back-up power sources • Continuity of Operations (COOP) facilities • Average home ISP bandwidth • Key infrastructure interdependencies
Physical Environment	• Type of terrain • Major landforms • Natural hazards • Climate • Weather • Historical natural disasters	• EM spectrum usage • Natural or man-made sources of EM interference • Broadband penetration levels
Time	• Cultural perception of time • Key dates	• Time synchronization mechanisms and location (e.g. Network Time Protocol (NTP) servers, Atomic Clock)

Cyberspace Permeation

If we dig a little deeper into the idea of the operational environment, we see it is built upon increasingly ubiquitous technology.[181] Technology pervades our lives, from implants inside our bodies[182] to satellites in space, most designed to improve quality of life (see Figure 4-3). Each of these devices once had, currently has, or will eventually have a presence in cyberspace. Imagine a city, with its millions of people, projecting itself into the ether of cyberspace: billions of "trusted" devices that create an ever-changing environment, allegedly performing some function designed to enhance people's lives. Each also has processing capability and storage, and most have sensors to sample aspects of their environment, and wireless network capabilities to facilitate communications. The complexity of this digital ecosystem is beyond human comprehension, creating an astronomically vulnerable attack surface.[183] Cyberspace is congested, and dominance is contested. Large swaths of cyberspace are built and operated by private industry, but the permeation of cyberspace into our daily lives is the result of private citizens who adopt new technologies. The sum of these devices provide the substrate for cyber conflict.[184] These devices, and the flows of information among them, will be co-opted, manipulated, and sometimes destroyed by actors with the power and motivation to do so.

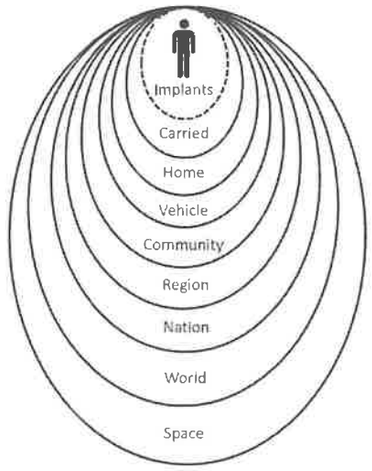

Figure 4-3: Analyzing the instrumented world. Humans are vigorously integrating technology into their lives, workplaces, and environment. This integration and increased dependency that comes with it create a fertile landscape for cyber conflict.

To understand our instrumented world, we think of concentric rings emanating from each individual. In each ring are devices, sensors, networks, and systems, with each sphere serving as a battlefield. Engagements can take place in any or all of these rings, even inside your body. This isn't the realm of fantasy. Former Vice President Dick Cheney had doctors disable the wireless functionality of his heart implant to prevent assassination attempts; cell phones have been turned into mobile tracking devices; hospitals' information systems are being held hostage for ransom money; and hackers, many think from Russia, have taken down portions of the Ukrainian power grid.[185] There are even allegations of state-sponsored cyber criminals attempting to influence U.S. presidential elections that have led to international sanctions.[186]

Implants – The most intimate of all technologies are those embedded in our bodies. Today these implants consist of medical devices, such as pacemakers and defibrillators and radio frequency identification (RFID) for tracking people and animals. We expect there will be a dramatic rise of future implant use as the technologies get smarter and scientists resolve issues between interfacing biology and technology. Right now the U.S. military is investing heavily on advanced implants to allow computers to communicate directly with the human brain.[187] Once a major breakthrough in neural interfacing takes place, the battlefield will shift from hacking commercial and military computing systems to literally hacking the brains of combatants. Imagine a situation where your very thoughts can be intercepted via vulnerable electronic systems designed by the lowest bidder. When that happens, we recommend buying stock in neural firewalls, intrusion/extrusion detection systems, and tamper-evident seals. These businesses will be booming.

On Our Person – One business area that is already booming is consumer technology. Consider all the technology you carry on your person when you travel: smartphones, tablets, book readers, fitness bracelets, electronic key fobs, and smart cards, for instance. And those are just the things we make the conscious decision to carry. Our clothing might still bear the electronic RFID tagging from the box store where we bought it.

Home – In our homes we have larger and more capable computing devices than the ones we carry on our persons, with increased network bandwidth and processing power. Take a look around your home and you'll see networked gaming consoles, smart televisions, alarm systems, set top cable boxes, printers, smart power meters, smart lightbulbs, and smart thermostats. The future lies in the Internet of Things, where increasing numbers of devices and appliances will be connected to, and a part of, the global information

grid. Business incentives push these devices not just to provide services, but also to possess myriad sensors that collect information on the environment and use it for easier purchasing and to allow data collection and user profiling for targeted advertising.[188] One smart TV manufacturer warns customers not to discuss sensitive or personal information within earshot of the device as these conversations might be unintentionally intercepted.[189] Importantly, these devices aren't static. Many have code that can be altered or updated remotely by the manufacturer. Governments see the Internet of Things as a rich resource for tracking and surveillance, and for good reason.[190]

"We don't have cars anymore;
we have computers we ride in.
We don't have airplanes anymore;
we have flying Solaris boxes connected to
bucketfuls of industrial control systems."
- Cory Doctorow [191]

Vehicle – Automobiles and the freedom they provide are a core part of the American ethos. Unfortunately, vehicles and transportation systems, whether personally owned or community-based, represent another zone of potential combat. As Cory Doctorow points out, such systems are no longer just simple mechanical systems, but complex computer systems that we ride inside. As with virtually all other types of computing systems, vehicles have proven to be vulnerable to attack and manipulation. For example, in 2008 a Polish teen modified a television remote control device and used it to control the local train system, causing a derailment.[192] Vehicles are also studded with sensors, radio transmitters, and a ubiquitous black box, providing such services as automatic toll payment, location tracking, concierge assistance, automatic accident alerting, vehicle performance tracking, and fleet monitoring services. Many insurance companies allow you to save money if you agree to provide data to them from sensors in your car that track speed, acceleration and deceleration, turns (to include G-forces for each), and time-of-day.[193] These advantages inadvertently create an additional attack surface[1] for actors to engage during cyber conflict. Law enforcement agencies have remotely activated in-car microphones to monitor conversations,[194] tire

[1] Attack Surface. This term is used to describe the myriad avenues through which an information system is vulnerable to cyber attack. As a system becomes more complex, the attack surface increases, making it more vulnerable. Countermeasures, such as network firewalls, can help decrease a system's attack surface; however, these systems are almost never completely effective in protecting against all existing vulnerabilities.

pressure monitoring systems broadcast unique serial numbers,[195] automated toll payment systems are being exploited to track user driving behavior,[196] and GPS systems allow continuous location tracking of taxis and riders.[197] Two independent security researchers discovered security flaws that provided the capability to remotely control many key aspects of certain models of automobiles. The vehicle manufacturer issued a recall for 1.4 million vehicles, perhaps the first automotive recall due to an active adversary rather than a design flaw.[198] Imagine what highly resourced threat actors would be capable of.

Community – At the community level, we transition from individual people and personal technologies to businesses and wide-area systems serving large groups. This category includes population centers ranging from small villages to megacities, so the population and technology densities will vary widely. There are, however, important common characteristics, particularly critical infrastructure which exist across the range of community sizes. The U.S. Department of Homeland Security lists 16 sectors at the strategic level, and we've highlighted the sectors most applicable to communities in Table 4-2.

While the DHS list is focused at the national level, we've extended their framework with examples from the local community. The DHS list is deficient because of its dismissal of "non-critical" infrastructure. Some of that infrastructure may not be critical from a strategic perspective, but can be considered so at local levels, particularly so because of its cumulative potential and capability of causing mass panic and break down of social order. Examples include public and private schools, bars, day care centers, law firms, churches, and the many aspects of the local community that are important to the population. Workplaces are of particular concern as they house innovation, processes, and proprietary information that make the economy run. We encourage you to think holistically about these and other facets of the community when conducting your analyses.

Table 4-2: Common Critical Infrastructure Sectors and Representative Examples at the Community Level

Sector	Community Examples
Commercial Facilities	Casinos, hotels/motels, theme parks, shopping malls, sports stadiums, bars and nightclubs
Communications	Telephone and cable infrastructure and control systems
Manufacturing	Local manufacturing plants
Emergency Services	911 systems, emergency notification systems
Energy	Power substation control systems, residential smart meters, dams
Financial Services	Local banks, ATMs, point of sale terminals
Food and Agriculture	Farms, grocery stores, automated irrigation systems
Government Facilities	Local government record keeping systems, electronic voting systems
Healthcare/Public Health	Hospital, medical clinic, and doctors' office medical technology and record keeping systems, pharmacy prescription systems, internal sensors and regulators
Information Technology	Internet service providers, cyber cafes, home networks
Transportation Systems	Toll payment systems, smart parking meters, air traffic control systems, gas stations, smart highways, GPS navigations systems
Water and Wastewater Systems	Water and sewage treatment plant industrial control systems

Ironically, the least technically advanced communities are sometimes the most resistant to cyber attack and exploitation. One reason Ukraine was able to quickly recover from the recent hack on portions of its power grid is because manual controls were still in place in their recently upgraded control centers. This is less likely to be the case in more modern systems where such backup functionality may no longer exist.

Local governments often look for more efficient ways to govern by investing in new technologies. We see change driven by governments, law enforcement and other agencies as well as private industry.[199] Networked red light cameras require fewer cops on the beat, smart power meters reduce

energy waste, and shopping malls track consumers as they shop. Perhaps the most pronounced change is seen in cities competing for leadership in "smart city" initiatives. Consider Barcelona, which was ranked the top smart city in the world by Juniper Research. A smart city seeks to improve the quality of life of its citizens, an admirable goal and one we would enjoy seeing realized. We see amazing innovation, apps portals for community-focused software, emergency response service for the elderly via telecare necklaces, community Wi-Fi, barcodes placed around the city for citizens to scan to learn more about a particular location, and even technological platforms to help city leaders make decisions in real time.[200] However, each initiative dramatically increases a community's attack surface.[201] If not properly secured, we may see smart cities turned into dystopic surveillance systems or simply razed to the ground by cyber siege.

Walk down any Main Street in America and try to count the surveillance cameras. Dozens of them peek out from banks, ATMs, shops, gas stations, parking areas, and police stations. Many commercial parking areas use surveillance cameras to both discourage and investigate vehicle break-ins and other crimes. Facial recognition systems designed to identify known terrorists and criminals have been used in football stadiums, Olympics venues.[202] Facial recognition technology was even used in downtown London in 2011 to identify suspects after widespread rioting following the August 4th police shooting of Mark Duggan during a vehicle stop.[203] It is not hard to imagine these surveillance systems being used along with other cellular and wireless technology to surreptitiously track individuals' movements from parking lot, to shop, to bank, to gas station.

An increasingly important trend in this area is the growth of megacities. Megacities are defined as cities with populations of 10 million or more people and are characterized by massive scale, intense population density, complexity, connectedness, and surface and sub-surface development.[204] Global drivers that are fueling this growth include war, increased numbers of disenfranchised youth, scarcity of resources, climate change, and unemployment.[205] Some of the largest megacities are merging into mega-regions like the East Coast of the United States. In China, the Hong Kong, Shenhzen, and Guanzhou region is home to approximately 120 million people.[206] Megacities and mega-regions present immense challenges to conventional military forces, and their footprint in cyberspace will eclipse many nations. Megacities and mega-regions must be part of future planning for both those seeking to defend those populations as well as cyber operators planning to exploit them.

Region – Sometimes it is useful to have a tier between the community and national level since regions often have unique attributes and are usually semi-autonomous. In some countries, regions might be states, provinces, or territories. Regions are characterized by having multiple population centers, regional military (National Guard) forces and law enforcement agencies, and large-scale facilities serving regional or global customers, such as hydroelectric dams, chemical plants, nuclear power plants, and large-scale agriculture. Regional presence in cyberspace is largely a linear extension based on the increased size of the population, regional governance, and specialized facilities.

Nation – Nation states are geographic regions that share common governance, language and cultural similarities and possess sovereignty. Entrance into and exit from nations in the physical world is often strictly controlled, and physical borders are well-understood. In cyberspace, these borders are blurred, but the concept of borders does still apply. Due to the intensely interconnected nature of cyberspace, it is very difficult to secure national borders in cyberspace, although some nations have tried. Examples include North Korea, which has severely limited Internet access to a few elites, government institutions, and academics, and China's Great Firewall, which attempts to regulate Internet access. Some nations are technologically advanced and possess a rich presence in cyberspace while other lesser-developed nations have very little presence and protection. Even in underdeveloped nations, citizens still seek Internet access and employ technologies such as mobile phones and Very Small Aperture Terminals (VSATs), which allow individuals and institutions to access it. The result is that Internet activities quickly leave the geographic confines of a given country. Lesser-developed nations sometimes leapfrog over older technologies, such as copper-based telephone service, to more advanced technologies, such as advanced cellular infrastructures. Many nations attempt to control disruptive information flows, but it is common for citizens to attempt to bypass government controls despite legal consequences and, in some cases, the very real possibility of physical harm. Nations employ surveillance technologies to monitor their populations to provide for their national security and stabilize the government. Despite even the best of intentions, such deeply embedded surveillance systems may be used for less altruistic purposes today and in the future.

World – Nations are interconnected through a series of surface and undersea fiber optic cables and satellites links, which have historically been subject to exploitation and attack. In cyberspace, network traffic is commonly routed through other nations, much of it through the United States in particular. Internet routing infrastructure has also been subject to misconfiguration and

attack that can shift the flows of traffic significantly.[207] Not all of the Earth's surface is occupied by nation states. Commons, such as the oceans, are shared by all, although there are certainly disputed regions. There are numerous international and intergovernmental organizations, most notably the United Nations, that attempt to advance collective agendas, keep the peace, and protect the rights and equities of the organization's constituents. Similarly, many large companies are global, with presences in multiple nations. Companies with global workforces are at increased risk for insider attacks and compromise through remote offices and diverse, and sometimes adversarial, national allegiances.

Space – The USSR launched the first satellite, Sputnik, in 1957, and since then mankind has used space for communications, science, and remote sensing. There are more than 1,000 satellites active in space and many more that are apparently inoperable. In particular, the region about 22 thousand miles into space, where satellite orbits match the rotation speed of the earth, is the home for hundreds of geosynchronous satellites that provide critical and continuous communications support. Significant satellites require years of effort to construct and can remain in orbit for many decades. Satellites are controlled by terrestrial ground stations, which transmit command and control instructions. As a result, satellites are remotely controlled and use aging technology. It should be noted that remotely controlled, aging technology has historically proven to be particularly susceptible to cyberspace attack.[208] Militaries are dependent on space systems for communication, global positioning, and intelligence collection. Expect space-borne cyberspace operations to be part of future large scale conflict between superpowers. How could it not?

Conclusions

Understanding the Operational Environment is essential to effective cyberspace operations and how they fit into a given actor's overall strategy of attack and defense. The PMESII-PT framework—political, military, economic, social, information, infrastructure, physical environment and time—is a powerful tool for analyzing the larger context. The Operational Environment is swathed with interconnected sensors, processors, and data storage, creating the terrain of cyberspace, which actors seek to defend and upon which they conduct operations. Cyber operators must understand that the rapid proliferation of technology is increasing the density and complexity of cyberspace. With this change comes both peril and opportunity.