Strategic Capabilities in the 21st Century

Michaela Dodge and David R. Inserra

Conventional and special operations forces are the most obvious expressions of U.S. military strength. Whether well-understood or not, they are the most visible manifestations of U.S. defense capabilities—especially since the terrorist attacks of September 11, 2001. Less visible and certainly less understood, but equally as vital to any defense of America's national interests, are three other capabilities: nuclear weapons, satellites, and cyber. Two of these capabilities—nuclear weapons and satellites—have been a part of defense calculations since the 1950s; cyber is a new domain that has emerged coincident with the evolution of the Internet and rapid development of computer-based information and communications technologies.

During the Cold War years, the U.S. made enormous investments to achieve and sustain a dominant position in nuclear and space affairs relative to the Soviet Union. Nuclear and space systems are seldom in the public eye these days but for different reasons.

Nuclear (then atomic) weapons made their appearance with the bombings of Hiroshima and Nagasaki that ended World War II and then became a central element of war planning during the 1950s and early 1960s. After taking a backseat to reporting on the conventional war in Vietnam, they surged back into prominence in the 1970s as tensions with the Soviet Union again became the dominant security issue.

Above-ground testing ended in 1963, and all other "yield producing" testing was halted in 1992, followed shortly by the U.S. decision to take its nuclear weapons off "ready alert" status as one of several measures implemented after the end of the Cold War. The "peace dividend" decade of the 1990s served to push nuclear matters even further off the public radar, with visibility (and even interest) clouded further by a decade of focus on counterinsurgency and counterterrorism operations.

Yet America's strategic security guarantees—for itself and to key allies—rest on its nuclear triad of aircraft-delivered bombs and land-based and submarine-based missiles. Of concern, then, is the almost complete absence of an informed debate about the health of America's nuclear enterprise.

Similarly, there is almost no public discussion about the health of the United States' space-based capabilities and the extent to which America depends on them not only in military affairs, but also economically and in broader national security matters. The military and intelligence communities and some portions of the economic sector are very aware of the importance of space. There is little public awareness, however, of the constant effort needed to maintain and upgrade the space-based systems that enable communications both at home and abroad and allow for the safe movement of nearly all forms of transportation that depend on the positioning, navigation, and timing (PNT) signals broadcast by Global Positioning System (GPS) satellites.

As for cyber, the economic, banking, and financial services sectors are at least as aware as the military and intelligence communities of the importance of this domain, within which information is continuously exchanged and through which attacks are constantly executed. Due to the sensitive nature of almost all factors bearing upon this topic, very little accurate information is available assessing the United States' capabilities and status relative to competitors. Nevertheless, no discussion of America's vital national interests and the relevant capabilities necessary to protect them would be complete without some understanding of this domain and the lengths to which the United States and others go in order to protect their interests.

Each of these areas is qualitatively and quantitatively different from the tools and environments normally associated with conventional "hard power." Yet without them, the exercise of such power would be nearly impossible. In the sections that follow, we will examine each of these unique strategic capabilities and outline the challenges that America faces in guarding its interests in all three areas.

Nuclear Weapons

In the waning days of World War II, the U.S. developed the ability to harness atomic power for military purposes. The U.S. started its program out of a concern that Nazi Germany would develop such a mighty weapon first and, as a result, win the war. As things turned out, the combined conventional forces of the Allied Powers defeated Germany, and it was Japan that experienced the power of the atomic bomb.

On August 6, 1945, the U.S. dropped the "Little Boy" bomb on Hiroshima, Japan. Highly enriched uranium provided the fuel for this bomb. Little Boy had the destructive equivalent of about 12 to 14 kilotons (12,000 to 14,000 tons) of TNT. The destruction caused by the attack has been compared to the bombing of the German city of Dresden in February 1945. In the Dresden attack, as many as 3,300 tons of bombs were dropped on the city by almost 1,300 bombers.

The second atomic bomb—the plutonium-based "Fat Man"—was dropped on Nagasaki three days after Hiroshima. These explosions marked the end of one of the most destructive conflicts in the history of mankind.

Over the next 40 years, a small set of technologically advanced countries developed atomic/nuclear weapons, including the U.S., the Soviet Union, the United Kingdom (U.K.), France, China, and India.[1] Beginning in 1945, the nuclear powers conducted thousands of nuclear weapons tests and yield-producing experiments of various weapon designs under a variety of conditions, with related advances in the ability to deliver nuclear weapons in different ways (missiles, bombers, strike aircraft, ships and submarines, and artillery) with increasing range and accuracy.

For many states, ballistic missiles remain the preferred means for delivering a nuclear weapon. This is because a ballistic missile attack maximizes the element of surprise for the attacker and the missiles can be deployed in a variety of survivable ways and are difficult to intercept. With intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs), it takes only half an hour to deliver a nuclear weapon from any launch location to a target anywhere in the world.

While experts usually distinguish between strategic nuclear weapons (heavy bombers, intercontinental-range ballistic missiles, strategic submarines) and tactical nuclear weapons (short-range and medium-range systems), it is important to keep in mind that any use of a nuclear weapon is strategic in its nature and consequences. Nuclear weapons are qualitatively and quantitatively different from conventional weapons.[2]

Nuclear command and control is essential both to nuclear deterrence and to maintaining the credibility of the U.S. nuclear weapons arsenal. America must be absolutely sure that the U.S. will be able to communicate with its nuclear platforms and that the President will be able to launch U.S. nuclear-armed delivery systems should a need to do so ever arise. It is also one of the most classified elements of the program. U.S. nuclear command and control is redundant, reliable, secure, and capable even though the U.S. needs to continue to modernize the network as new electronic warfare capabilities emerge.

The decades before the end of the Cold War were marked by an intense competition between the U.S. and the Soviet Union that led to increases in their respective nuclear weapons arsenals by tens of thousands. This multi-decade competition also necessitated a new level of thinking about warfare, deterrence, operational employment concepts, wargaming, and analysis of effects.

Nuclear forces have been a vital component of U.S. force structure. They have been the bedrock of the United States' posture for deterring strategic attacks against the U.S. itself and its allies under the policy of extended deterrence and assurance. They have also been an essential component of U.S. policy for limiting the proliferation of nuclear weapons.

As former Heritage analyst Baker Spring points out, due to their enormous destructive power packed in a relatively small weapon, nuclear weapons are different from conventional weapons. Nuclear weapons can defeat conventional weapons because of the unique nature and magnitude of their effects: massive blast, direct radiation, fallout, and electromagnetic pulse.[3] These qualitatively different effects of nuclear weapons compared to conventional weapons led policymakers to attempt to develop frameworks through which awesome atomic power would be restrained.[4]

Initially, the U.S. explored options for disarmament and international control of nuclear technology. The most prominent proposal was the Baruch Plan, named after Bernard Baruch, U.S. representative to the United Nations Atomic Energy Commission, who presented a U.S. disarmament plan to the commission on June 14, 1946.[5] The Baruch Plan proposed putting all atomic energy activities under the control of an International Atomic Development Authority. The plan would have required the renunciation of atomic bombs and would have established a system for punishing violators. It envisioned ending the manufacture of atomic bombs, disposing of existing bombs, and limiting possession of the technological knowledge needed to produce bombs to the authority. In other words, the U.S. attempted to eliminate the potential for atomic warfare immediately after its inception.

The Soviet Union, however, rejected the Baruch Plan. Consequently, with the start of the Cold War, the U.S. turned to exploring plans for using its nuclear forces to contain the military expansion of the Soviet Union. U.S. proposals for limiting nuclear arsenals—specifically, arms control and nonproliferation—were among the less ambitious diplomatic options compared to the Baruch Plan. In this context, two subsequent strategies emerged.

First, in the early 1960s, strategist Herman Kahn proposed that the U.S. should adopt a damage-limitation strategy to deter a possible Soviet attack on the United States and its allies. Kahn defined deterrence broadly to encompass both the goal of limiting the damage that would normally be inflicted by an attack that targeted one's offensive forces—a counterforce approach[6]—and the defensive measures necessary to achieve that goal, along with possession of one's own offensive nuclear forces. "I agree with our current national policy that the primary objective of our military forces is to deter war," Kahn said, summarizing his strategy. "However, I feel that there is a second but still very important objective: to protect life and property if a war breaks out."[7]

Second, at roughly the same time, economist and game theorist Thomas Schelling proposed that deterrence be defined much more narrowly. He argued that the goal of damage limitation and the accompanying protective measures were actually at odds with deterrence. While Kahn felt that strong defenses would cause an enemy not to attack, Schelling believed that an attacker would be deterred more effectively by fear that his own valued resources might be attacked. More specifically, Schelling argued that deterrence meant threatening to retaliate by targeting the attacker's population centers:

> Thus, schemes to avert surprise attack have as their most immediate objective the safety of weapons rather than the safety of people. Surprise-attack schemes, in contrast to other types of disarmament proposals, are based on deterrence as the fundamental protection against attack. They seek to perfect and to stabilize mutual deterrence—to enhance the integrity of particular weapon systems. And it is precisely the weapons most destructive of people that an anti-surprise-attack scheme seeks to preserve—the weapons whose mission is to punish rather than to fight, to hurt the enemy afterwards, not to disarm him beforehand. A weapon that can hurt only people, and cannot possibly damage the other side's striking force, is profoundly defensive: it provides its possessor no incentive to strike first.[8]

Schelling's retaliation-based deterrence strategy, which the Administration of Lyndon B. Johnson fashioned into a policy of mutually assured destruction (MAD), eschewed defenses, downplayed counterforce capability, and relied instead on survivable offensive strategic nuclear forces to provide for U.S. security. In fact, Schelling's strategy asserted that strategic defenses would be destabilizing by undermining the capacity of the retaliatory force, at least in the context of the Soviet threat and its accompanying bipolar international political structure. It explicitly argued in favor of mutual vulnerability for the populations and industrial capacities of the U.S. and the Soviet Union so that each side would fear the loss of its people and economy and would thus be deterred from attacking the other.

During the remainder of the Cold War, debate between proponents of these two schools of thought continued. On balance, however, Schelling's strategy of retaliation-based deterrence proved more popular during the Cold War and was a more powerful driver of the U.S. strategic force posture, although every subsequent Administration rejected the pure version of assured destruction.[9]

Both Kahn's damage-limitation strategy and Schelling's retaliation-based deterrence strategy were designed to prevent nuclear war in the bipolar structure of the Cold War. Neither, however, was designed to meet the security needs of the U.S. and its allies in today's multipolar world. And both Kahn's and Schelling's constructs assumed that the possessors of nuclear weapons would be states led by rational actors, an assumption whose merits are debated in today's world. While Schelling's strategy may have proved more popular during the Cold War, a variant of Kahn's strategy is better suited to meeting U.S. and allied security needs in a multipolar world marked by the proliferation of nuclear weapons and delivery systems.

Implications of Limits on Nuclear Testing. Concerns about the environmental and potential public health consequences of nuclear weapons detonations also led to early efforts to limit and restrict nuclear weapons testing. For instance, the U.S. and the Soviet Union entered a moratorium on atmospheric nuclear weapons test explosions between 1958 and 1961.

Washington was surprised when it learned that during the moratorium, the Soviets were preparing to undertake the largest series of nuclear tests ever conducted; Moscow unilaterally resumed atmospheric tests in 1961. The U.S. was also surprised to learn how quickly competency can be lost; when the U.S. resumed its own testing, it found a significant decrease in its competency to test nuclear weapons.[10]

Nuclear weapons testing is currently subject to four major international agreements: the 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and under Water (also known as the Limited Test Ban Treaty); the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (also known as the Outer Space Treaty), which prohibits nuclear weapons tests on the Moon and other celestial bodies; the 1974 Treaty on the Limitation of Underground Nuclear Weapon Tests (also known as the Threshold Test Ban Treaty), which bans nuclear weapons tests above 150 kilotons; and the 1976 Treaty Between the United States of America and the Union of Soviet Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes.

In addition, there are other international agreements that indirectly affect states' abilities to test nuclear weapons, such as agreements that established the treaties on nuclear-weapons-free zones. These agreements limit tests that would have a destructive impact on the environment.

It is important to understand that weapons in the current U.S. stockpile were designed and developed to meet stringent Department of Defense requirements during the Cold War. The current stockpile is thus based on technology from the 1970s. During the Cold War, key requirements addressed nuclear safety; operational reliability; yield; conservative use of nuclear materials (i.e., using no more material than is absolutely necessary); and operational simplicity.[11] They were driven primarily by the demands of Cold War deterrence based on the policy of mutually assured destruction, with the Soviet Union as the prime adversary.

During the Cold War, the United States replaced or modernized its weapons every 10–15 years, vastly increasing their capabilities over time.[12] Testing was considered essential throughout the entire operational cycle of a nuclear weapon. However, this testing did not focus on building databases or tools that would make it possible to ensure the reliability of weapons if testing ever ceased, because the technical feasibility of this approach was rejected.[13] Thus, the often cited argument that the United States has enough data to continue to confirm the reliability of its stockpile is open to question since both the data and the tools used to collect them are Cold War vintage and were never meant to be used in the absence of new data.

The military requirements of the 1970s also affected how the United States designed its delivery systems: bombers and, in particular, intercontinental-range ballistic missiles and submarine-launched ballistic missiles. Missiles have to withstand extreme temperatures and stresses during acceleration and re-entry to deliver the warhead to its intended target. Each type of warhead has to be carefully integrated with its delivery vehicle to ensure that the system as a whole will perform exactly as intended.

Given that America is preparing to recapitalize its delivery platforms, such exacting technical specifications could pose a challenge for U.S. engineers. These platforms will have to be made to "fit" the existing warheads, which means that their designs and parameters will have to be more conservative and perhaps different from missions for which the U.S. would design its warheads if it could start over.

The United States today has the oldest nuclear weapons arsenal it has ever had. The average age of U.S. nuclear warheads is approaching 27 years, which is well beyond their originally intended operational life.[14] Since 1992, the nation has been under a self-imposed moratorium on "yield-producing" experiments and has been relying on the Stockpile Stewardship Program (SSP) that, while it does include a suite of experiments, does not include explosive testing or the maintenance of existing warheads. At the heart of the SSP are supercomputers and computer codes based on data from previous nuclear tests and yield-producing experiments that were conducted between the late 1950s and 1992.

As nuclear weapons age, they depart from their tested envelopes, which, as noted, were developed decades ago. As a result, there is inherent risk in not performing explosive tests to confirm safety and reliability. This raises a question about whether the computer codes that American scientists and engineers use to predict and certify nuclear performance are correct. As David Sharp, chief scientist at the Los Alamos National Laboratory, points out:

> The only unequivocal way to demonstrate that predictions made with simulation codes meet expected standards of confidence is by establishing a track record of correct and reliable predictions that have been made using that code. For nuclear weapons this means successful prediction of nuclear performance. A track record of this kind is the essential reality check on claims of predictive capabilities; it is the indispensable source of confidence that is needed if codes are ever to replace nuclear tests. However, the ability to make correct, reliable predictions of nuclear performance using codes has not been demonstrated and cannot be demonstrated without a nuclear test program.[15]

The documentation from past explosive tests is not as complete as it might have been had the U.S. anticipated that a future test moratorium was possible. As a result, there are concerns about whether the computer codes that scientists and engineers use today based on previous test data are fully valid.

Dr. Kathleen Bailey, a senior fellow at the National Institute for Public Policy, argues that "Data from past nuclear testing is, in general, too coarse to test the validity of the high resolution, complex models that the SSP [Stockpile Stewardship Program] seeks to develop."[16] In addition, according to David Sharp, "the right answer could be obtained as a result of compensating errors, a circumstance in which two or more errors balance each other so they have no net effect."[17] This means that the final calculation might result as expected but that real errors and their potential risks are hidden.

At the time of the Comprehensive Test Ban Treaty in the 1990s, the directors of the U.S. National Nuclear Laboratories requested that the U.S. be allowed to conduct lower than one-kiloton experiments "to determine whether the first stage of multiple stage devices was indeed operating successfully."[18] The Clinton Administration, however, interpreted the treaty as banning all nuclear yield-producing experiments.[19]

Such errors could adversely affect judgments about the condition of the stockpile.[20] They are also problematic because other nations have taken a different approach and are testing nuclear weapons. Consequently, these countries are developing a body of data based on modern, real-world testing, potentially developing and trying new weapons designs.

While this proliferation of capabilities, generation of new knowledge, and emergence of new programs has been occurring, the U.S. has remained committed to its policy of banning all yield-producing experiments and refusing to allow nuclear weapons innovation in its National Nuclear Laboratories. It is also worth mentioning that Russia and China are developing new weapons as well as sustaining old ones. This means that their weapons complex is geared toward solving different problems than that of the U.S. Both Russia and China could potentially develop new and better capabilities.

The Nuclear Threat. Nuclear weapons possess awesome power and have a unique ability to harm U.S. vital interests, especially when coupled with ballistic missiles, which remain the weapon of choice for America's adversaries.

- Ballistic missiles enable an adversary to deliver an attack within minutes (about a half-hour, or less depending on launch and target location, in the case of intercontinental-range ballistic missiles).
- The U.S. and its allies still lack a comprehensive layered ballistic missile defense system that would protect America from missile attack and devalue ballistic missiles as weapons for potential adversaries.
- The knowledge about mechanics of nuclear weapons and the physics behind them is becoming more easily accessible. For example, rudimentary nuclear weapon designs are available on the Internet. The covert network run by Pakistani scientist A.Q. Khan demonstrated that it is possible to buy advanced nuclear technologies—and perhaps material—on the black market, and North Korea has provided covert nuclear weapons assistance to Iran.
- Finally, ballistic missiles provide a more assured means of getting a weapon to its intended target than delivery by aircraft or other means.

Nuclear weapons come in various yields and design types. The weapon's configuration will determine its effects, which can generally be summarized in six categories: blast, direct nuclear radiation, thermal radiation, fires, electromagnetic pulse, and fallout.[21] Depending on the yield and design type, the weapon's effects could dramatically affect the way the U.S. and its allies operate their forces. It is also worth noting that research and technology have progressed significantly since the U.S. stopped its yield-producing experiments.

New materials and technologies might perform in unexpected ways in a nuclear environment, as opposed to highly controlled testing and experimentation environments, thus introducing an additional layer of uncertainty when thinking through operational plans and contingencies under which an enemy might use a nuclear weapon or how the U.S. would operate its forces in a post–nuclear weapon attack environment. Extreme conditions and America's limited understanding of the physical processes going on during a nuclear weapons detonation and the consequences of such a detonation make it very difficult and costly to model the effects of nuclear weapons on the different materials that are now used to make them. Even then, assumptions built into nuclear effects modeling may result in misleading understanding and flawed estimates of what the real effects of the use of a nuclear weapon would be.

Current Nuclear Use. Although it may come as a surprise to some, the U.S. "uses" its nuclear weapons every day. As pointed out by General Larry Welch, former Commander of the U.S. Strategic Air Command and former Chief of Staff of the Air Force:

> The primary role of U.S. nuclear weapons for well over half a century has been to prevent their use. To that end, we have used them every second of every day since the first deterrent systems were deployed. They have worked perfectly. The nuclear deterrent is the only weapons system I know of that has worked perfectly without fail, exactly as intended, for their entire life span.[22]

U.S. nuclear weapons have played a key role in protecting all three vital U.S. interests discussed in the Introduction to this *Index*:

- Safeguarding the homeland from external attack; protecting Americans against threats to their lives and well-being; protecting America's territory, borders, and airspace.
- Preventing a major power threat to Europe, East Asia, or the Persian Gulf, where a regional war would be devastating to U.S. interests and could spin out of control into a global conflict.
- Maintaining the freedom of the commons: free and safe transit of sea-lanes and space upholding the principle of freedom of the seas and space to promote and protect commerce among nations.

Other nations rely on their nuclear weapons capabilities for geopolitical maneuvering as well. For example, North Korea "uses" its nuclear weapons to coerce South Korea and limit South Korea's response to North Korea's aggressive behavior. Russian nuclear weapons are the only reason why other nations think about Russia—a corrupt kleptocracy with enormous economic, demographic, ecological, and public health problems—as a superpower.

Where appropriate, this analysis will focus on states that possess nuclear weapons capabilities and have indicated an intent to attack one or more U.S. vital interests or that the U.S. government views as potential adversaries: e.g., Russia, China, and North Korea. France, the U.K., India, and Pakistan will not be considered threats to the homeland in this analysis because they have not communicated any intent to attack the U.S. (With respect to India and Pakistan, there exists the real possibility that these two nations could start a nuclear war with each other, and the effects of such a war would negatively affect the interests of the U.S. and its allies in the region.)

In addition, many experts believe that Israel possesses a nuclear weapons capability (Israel is not a party to the Non-Proliferation Treaty), although Israel has never publicly acknowledged the existence of its nuclear weapons arsenal. Israel does not have the intent to attack the U.S., so it will not be considered a threat for the purposes of this analysis.

It is also necessary to mention that nuclear weapons, if used, would probably not operate in a conventional conflict vacuum. A nuclear weapons attack would likely be accompanied by conventional operations aimed at achieving the military and political objectives of whichever nation decided to use nuclear weapons. A nuclear weapon could also be used during a conventional conflict as a next step on an escalatory ladder and to signal resolve. A nuclear weapon could also be used as a final resort when the leadership of a warring nation had nothing left to lose. Few countries, however, possess the capability to attack and threaten the U.S. homeland with nuclear weapons, and even fewer have the intent to do so.

The Nuclear Operating Environment. Since the end of the Cold War, the world in which U.S. nuclear forces operate has changed significantly. While the main focus of deterrence, the Soviet Union, receded in importance, the U.S. has had to adjust its posture to be able to deter new actors armed with nuclear weapons as well as emerging nuclear weapons states. India conducted five nuclear explosion tests in May 1998; Pakistan followed suit later that month with six nuclear tests of its own. North Korea conducted three nuclear device tests, in 2006, 2009, and 2013. Iran does not have a nuclear weapon yet, but the International Atomic Energy Agency has found evidence of weaponization activities, uranium enrichment activities, and even uranium diversion. Iran has not been able to explain these activities in a manner that would allay the agency's suspicion.

Successive Nuclear Posture Reviews (in 1994, 2001/2002, and 2010) have struggled to address these challenges and adjust U.S. strategic posture to the post–Cold War world. With the end of the Cold War, the U.S. nuclear arsenal was dramatically downsized from over 30,000 warheads (its peak in 1967) to its current inventory of less than 5,000 warheads consisting of about 500 tactical nuclear weapons (TNWs); about 1,585 deployed warheads, according to data from the latest New Strategic Arms Reduction Treaty (New START) data exchange; and the remainder in reserve.[23]

Since the end of the Cold War, the U.S. has made substantial adjustments in its nuclear posture, while working to preserve deterrence of attack. During the Cold War and Moscow's rapid disintegration, the U.S. focused primarily on the Soviet Union. One of the significant consequences of the dissolution of the Soviet Union was that the nuclear target set got smaller, which allowed for unprecedented reductions in U.S. strategic weapons and U.S. forward-deployed nuclear weapons. Many argued that with the Soviet threat receding, the nation lacked justification for maintaining not only a varied inventory, but also the infrastructure needed to design, develop, test, and maintain nuclear weapons. The U.S. conducted its last nuclear weapons test in 1992.

In the post–Cold War years, working in conjunction with the Soviet Union/Russian Federation, the U.S. has participated in four major programs designed to alter the size and composition of both nations' nuclear weapons arsenals. Counting rules under each of the treaties are different, so the real number of warheads and systems reduced will also be different for each of the treaties.

- On July 31, 1991, the United States and the USSR agreed to the Strategic Arms Reduction Treaty I (START).[24] The agreement entered into force in 1994. The accord dictated that each state reduce and limit its strategic armaments to no more than 6,000 "accountable" warheads and 1,600 delivery vehicles. START I relied on extensive verification measures that included data exchanges and on-site inspections that were either prearranged or conducted on short-notice.[25]

- The Strategic Offensive Reductions Treaty (Moscow Treaty, or SORT) entered into force in 2003. Rather than attaching warhead quantities strictly to delivery vehicles, SORT concentrated not on "accountable" warheads, but on actual operationally deployed warheads. Each state was allowed a range of 1,700 to 2,200 deployed warheads and the ability to determine the structure of its offensive strategic arms.[26] SORT relied on START I verification measures, which expired in 2009. By 2009, the United States had fulfilled its treaty obligations by lowering the number of deployed warheads to below the maximum allowed under SORT.[27]

- The New Strategic Arms Reduction Treaty (New START) agreement entered into force in 2011. New START limits deployed warheads to 1,550 for each party and the number of deployed strategic nuclear delivery vehicles to 700 for each party.[28] Under New START, each bomber counts as only one deployed warhead out of the 1,550 despite the fact that many bombers can carry many more than one warhead (up to 16 for the B-2 and up to 20 for the B-52).[29] New START's verification regime is not as stringent as that defined by START I.[30] This change is due in part to the dramatic decrease of inspections allowed to each nation.[31] After the treaty is implemented, nuclear forces levels established in New START will be 74 percent lower than the limit of the START I Treaty and 10 percent–30 percent lower than the deployed strategic warhead limit under SORT.[32]

In addition to these treaties, in 1991, President George H.W. Bush and eventual Soviet President Mikhail Gorbachev (and subsequently Russian President Boris Yeltsin) declared that both countries would reduce their arsenals of tactical nuclear weapons and delivery vehicles reciprocally and unilaterally. These statements are known collectively as the Presidential Nuclear Initiatives (PNIs).[33] Unlike arms control treaties, the PNIs are politically but not legally binding.

As a result, the U.S eliminated all of its ground-launched short-range theater nuclear weapons, reduced its nuclear artillery shells and short-range ballistic missile warheads, and withdrew all TNWs from surface ships and attack submarines, as well as TNWs associated with U.S. land-based naval aircraft.[34] President Bush's initiatives led to an 85 percent reduction in U.S. operationally deployed TNWs between 1991 and 1993.[35] Russia, however, is said to be in violation of its political commitments under the PNIs.[36]

President Barack Obama's 2010 Nuclear Posture Review (NPR), the first U.S. NPR made available to the public, set five objectives of U.S. nuclear weapons policy and posture:

1. Preventing nuclear proliferation and nuclear terrorism;

2. Reducing the role of U.S. nuclear weapons in U.S. national security strategy;

3. Maintaining strategic deterrence and stability at reduced nuclear force levels;

4. Strengthening regional deterrence and reassuring U.S. allies and partners; and

5. Sustaining a safe, secure, and effective nuclear arsenal.[37]

The underlying goal of the President's current nuclear weapons policy is to achieve "the peace and security of a world without nuclear weapons."[38] The President operates under the assumption that if the U.S. and Russia reduce their respective nuclear weapons arsenals bilaterally, this will put pressure on others to follow suit and reduce and/or dismantle their own nuclear weapons capabilities.

This assumption seems to go against the historical evidence. The U.S. has reduced its nuclear arsenal dramatically since the end of the Cold War. Washington maintains less than 5,000 nuclear warheads today, down from a peak of about 31,000 in 1967.[39] Yet North Korea, Pakistan, and India emerged as nuclear weapons players at the time of massive reductions in the U.S. nuclear arsenal (and also while the U.S. stopped yield-producing experiments on its nuclear arsenal).

Iran seems to be conducting activities that are consistent with the intent to weaponize its nuclear program, although it does not have a nuclear weapon yet.[40] The massive resources and manpower that

Iran spends on developing ballistic missiles that can reach U.S. allies and could reach the U.S. in the next few years also point to its intent to develop a payload that would be potent enough to coerce the U.S. and other regional powers and alter their calculus regarding possibly taking action against the interests of Tehran.

With the emergence of these new nuclear weapons actors after the end of the Cold War, the U.S. had to reexamine its Cold War notion of deterrence, which was based on the policy of mutually assured destruction. While U.S. policymakers were willing to accept mutual vulnerability in the deterrence equation vis-à-vis the Soviet Union and later Russia, they were not willing to accept retaliation-based deterrence vis-à-vis newly nuclear-armed nations. U.S. decision-makers recognized their limited insight into how the newly nuclear armed nations would operate their nuclear forces; how their command and control structures would operate; under what conditions their leaders would consider actually using a nuclear weapon, and what the U.S. might need to credibly deter these new actors.[41]

The U.S. operates in an asymmetrical deterrent environment because it values its population centers and economy, which are far easier to destroy than the hardened leadership bunkers, tools of internal oppression and external attack, and military infrastructure that some of its potential adversaries value.[42] With the Soviet Union, the U.S. also developed a common understanding of nuclear weapons terminology and concepts through an elaborate arms control process and decades of verification experience, something that is absent from the relationship with the new nuclear powers.

Interactions between the U.S. and these powers on nuclear issues have been limited to trying to convince these actors to give up their weapons and the technologies that pose a proliferation risk. It is not at all clear that these nations have a good understanding of U.S. nuclear weapons policy and potential "red lines." In the case of North Korea, for example, the U.S. has very limited insight into the inner workings of the hermit kingdom and even less information regarding North Korea's decision calculus on the use of nuclear weapons. The U.S. will have to understand these new nuclear-armed states and think about how to apply its military capabilities to threaten what they value if the U.S. is to deter them from attacking U.S. interests.

U.S. Nuclear Weapons Outside U.S. Territory. Understanding the perspectives of newly armed nuclear weapons states takes on additional importance because the U.S. has extended nuclear deterrence commitments to over 30 nations around the world with whom the U.S. has alliance commitments.

To that end, the U.S. maintains about 200 B61 gravity bombs in Europe. Deployed to Belgium, Germany, Italy, the Netherlands, and Turkey, these bombs can be employed by U.S. or NATO nuclear-certified aircraft (U.S. F-16 and F-15E aircraft and various European dual-capable aircraft such as the German Tornado). The B61 is the only remaining operationally deployed tactical nuclear weapon in the U.S. arsenal.[43]

Over the course of decades, the U.S. developed elaborate command and control arrangements through NATO. NATO's senior body on nuclear matters is the Nuclear Planning Group, where all NATO members (with the exception of France) participate in discussing various policy issues related to nuclear weapons.

NATO's 2010 Strategic Concept, a document outlining the purpose and nature of NATO's security tasks, states that:

> Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy. The circumstances in which any use of nuclear weapons might have to be contemplated are extremely remote. As long as nuclear weapons exist, NATO will remain a nuclear alliance.[44]

The Strategic Concept also explains the relationship between U.S. strategic nuclear forces and the nuclear weapons arsenals of France and the United Kingdom:

> The supreme guarantee of the security of the Allies is provided by the strategic nuclear forces of the Alliance, particularly those of the United States; the independent strategic nuclear forces of the United Kingdom and France, which have a deterrent role of their own, contribute to the overall deterrence and security of the Allies.[45]

In 2012, the alliance conducted a comprehensive Deterrence and Defense Posture Review (DDPR), which reaffirmed that "Nuclear weapons are a core component of NATO's overall capabilities for deterrence and defence alongside conventional and missile defence forces." The DDPR also recognized the contribution of missile defense to NATO's security and reaffirmed the importance that the alliance assigns to the U.S. nuclear presence in Europe.[46]

With regard to missile defense, the U.S. is pursuing a "phased adaptive approach." This plan for the protection of the European allies is based on an assessment of the threat from Iran's short-range and medium-range ballistic missiles. The plan was announced in 2010 and was characterized by the White House Press Office as follows:

- Phase One (in the 2011 timeframe)—Deploy current and proven missile defense systems available in the next two years, including the sea-based Aegis Weapon System, the SM-3 interceptor (Block IA), and sensors such as the forward-based Army Navy/Transportable Radar Surveillance system (AN/TPY-2), to address regional ballistic missile threats to Europe and our deployed personnel and their families;

- Phase Two (in the 2015 timeframe)—After appropriate testing, deploy a more capable version of the SM-3 interceptor (Block IB) in both sea- and land-based configurations, and more advanced sensors, to expand the defended area against short- and medium-range missile threats;

- Phase Three (in the 2018 timeframe)—After development and testing are complete, deploy the more advanced SM-3 Block IIA variant currently under development, to counter short-, medium-, and intermediate-range missile threats; and

- Phase Four (in the 2020 timeframe)—After development and testing are complete, deploy the SM-3 Block IIB to help better cope with medium- and intermediate-range missiles and the potential future ICBM threat to the United States.[47]

The U.S. cancelled Phase Four in 2013 and decided to deploy 14 additional Ground-Based Midcourse Defense Interceptors to address the North Korean and Iranian long-range ballistic missile threat to the U.S. homeland."[48] Construction of the missile defense sites in Romania is proceeding on schedule.

The deep level of cooperation and integration that exists between the U.S. and European allied forces on nuclear weapons does not exist in Asia. Japan and South Korea have never been integrated into nuclear planning and operations for cooperative defense in the same way that European NATO allies have been. Some of these countries hosted U.S. nuclear weapons or supported U.S. nuclear weapons deployments in their regions in the past—Japan, for example, supported deployment of the Tomahawk Land Attack Missile/Nuclear (TLAM/N) systems—but the U.S. retired all of its TLAM/N systems in 2013 and currently does not deploy nuclear weapons outside of NATO and the U.S. territories.[49] The potential to forward deploy dual-capable aircraft with the B61 TNW remains a key option for reassuring Asian allies of America's commitment to their defense.

U.S. Nuclear Forces and Infrastructure. Following release of the 2010 Nuclear Posture Review, President Obama directed that the U.S. employment strategy guiding U.S. nuclear weapons policy be revised. The Nuclear Posture Review Implementation Study (NPRIS), announced in June 2013,[50] called for additional nuclear weapons reductions.[51] The Administration concluded that "we can ensure the security of the United States and our allies and partners and maintain a strong and credible strategic deterrent while safely pursuing up to a one-third reduction in deployed strategic nuclear weapons from the level established in the New START."[52]

Recently, consensus within Congress regarding funding for National Nuclear Security Administration (NNSA) weapons activities has begun to unravel. The Administration achieved consensus before Senate approval of New START,[53] pledging to invest over $85 billion between fiscal year 2011 and FY 2020. This funding was intended to support costs for maintenance of the nuclear weapons stockpile and associated infrastructure, including the Chemistry and Metallurgy Research Replacement (CMRR) plutonium facility and the Uranium Processing Facility. The NNSA, a semi-autonomous agency within the U.S. Department of Energy, is responsible for nuclear weapons infrastructure recapitalization and nuclear weapons sustainment, and the military services exercise responsibility for the delivery systems.

Due in part to the Budget Control Act (BCA) and the resulting budget sequester, and in part to serious cost escalation in Life Extension Programs and infrastructure recapitalization programs, the Administration's budget requests since 2010 have not reflected the commitment to fully fund key nuclear programs on the schedule that it specified to the Senate in November 2010. Congress has decided to support the Administration's request to defer certain programs and slip the schedule for others. The Administration effectively cancelled the CMRR facility in its FY 2013 budget request. Impacts of the BCA and the cost escalation of critical programs will continue to delay and complicate nuclear weapons infrastructure modernization and stockpile sustainment activities.

The U.S. currently operates under a policy constraint that does not allow the National Nuclear Laboratories to develop new nuclear warheads or conduct yield-producing experiments on the current inventory of nuclear warheads. This policy also prohibits supporting development of new military missions for nuclear warheads or providing for new military capabilities.[54] Rose Gottemoeller, the State Department's Acting Under Secretary for Arms Control and International Security, summarized this policy as follows: "We're not modernizing. We're not modernizing. That is one of the basic, basic, I would say, principles and rules that have really been part of our nuclear posture view and part of the policy."[55]

These policies constrain U.S. activities that could lead to the development of new, safer warheads, because new safety features would require yield-producing experiments to make sure that the new designs perform as expected. These policies will also make it more difficult to preserve the agility within the United States' knowledge and technology base that is necessary to adjust rapidly to surprise developments in other nations' nuclear weapons programs.

The Ongoing Challenge. The U.S. currently deploys nuclear weapons to Europe and is the only nuclear weapons state that deploys nuclear forces outside of its own territory. It is important that the U.S. be able uphold the principle of deploying weapons outside of its territory, because a deployment of nuclear weapons on allied territory is both an important contributor to assuring allies and clearly preferable to having allies develop their own nuclear weapons capabilities.

At the same time, the U.S. will continue to face challenges presented by its aging stockpile, a lack of funding for nuclear weapons modernization and infrastructure recapitalization, and policy constraints on yield-producing experiments. Complex and interdependent missile defense programs are likely to face their own developmental challenges.

National Security Space Systems and Satellites

The ability of the U.S. military to project combat power against an enemy force anywhere in the world depends on an array of command and control, logistics, and other support systems that are made possible by the country's national security space systems and other satellites. In fact, many critical functions can be performed (or performed acceptably) only by satellites, just one example being the American-produced and American-maintained Global Positioning System (GPS) upon which the world's interconnected transportation system relies.

The GPS constellation provides unmatched positioning, navigation, and timing (PNT) capabilities that are used not only by civil aviation, commercial shipping, and directionally challenged drivers everywhere, but also by the military for which it was originally designed. Satellites also enable global communications, which allows for effective command and control of conventional and strategic forces, and play an important role in intelligence gathering: the information on which U.S. forces rely to formulate plans and execute the best battlefield decisions. Military satellite systems also provide early warning and tracking of ballistic missiles, giving the U.S. time to take appropriate defensive measures.

Knowing the status of these systems is important if one is to understand the extent to which they are able to contribute to the viability of U.S. military power. These systems can be assessed across three important characteristics:

- The lifespan of these systems, which is a measure of their health and readiness;
- The number of satellites in orbit, which is a measure of satellite coverage and resiliency; and
- Their ability to provide support-on-demand, which is usually measured in available bandwidth capacity.

These characteristics are interconnected, but the specific purpose for which satellites are deployed determines their numbers, capabilities, and system configuration. For example, fewer highly capable satellites might be better for certain tasks than greater numbers of less capable systems, as is the case with very high orbit or geostationary systems;

in other cases, the number of satellites in orbit might be more important than the number of more capable or longer-lived ones.

Lifespan. The lifespan of satellites is determined largely by the amount of fuel onboard the satellite. In decades past, battery function and component survival against space radiation were key lifespan factors. Satellite technology has now advanced to make these problems less critical than the amount of thruster fuel maintained aboard the satellite.[56] The gravitational pull of the Earth, Moon, and Sun, together with solar wind and other features of space, can affect a satellite's speed and position, thus changing its position over time.[57] As a result, satellites must make small adjustments with thrusters to stay in their assigned orbit, a process called "station keeping."[58]

Currently, most GPS satellites orbiting the Earth have a designed lifespan of 7.5 years, though they have often surpassed that figure, and advances in satellite materials are increasing platform life.[59] The newest GPS model in operation was designed with a 12-year lifespan, and the next generation of satellites is supposed to remain in orbit for 15 years.[60] The early warning and missile defense satellite known as SBIRS GEO (Space-Based Infrared System–Geosynchronous orbit) has a lifespan of 12 years, and both of the U.S.'s new communications satellite systems (WGS and AEHF) have a designed lifespan of 14 years. [61]

The older Milstar communication satellites that provide secure communications were designed for 10 years of service, a target exceeded by the first two systems, which approached or reached 20 years of service.[62] Similarly, the legacy DSCS III communication satellites have surpassed their 10-year service lives, with the satellites functioning on average at least 50 percent longer than their designed life.[63] The Defense Support Program (DSP) satellites being replaced by SBIRS also have had significantly more longevity than planned, with lifespans exceeding design by as much as 250 percent.[64]

Satellite lifespan most closely equates to the readiness of a warship or an aircraft. As the average amount of time remaining on U.S. satellites decreases, the U.S. either has to spend the money necessary to replace these satellites or lose the critical support functions they provide. As noted, the actual lifespan of satellites is often more than expected, but this does not guarantee that all satellites will see extended use, and the U.S. should not expect to rely on satellites well beyond their intended service lives.

Number of Satellites. GPS satellites are so important that the U.S. maintains excess capacity in the GPS constellation to ensure redundancy, thus reducing risk should any node fail. The constellation requires 24 satellites, but the U.S. routinely operates 27 and maintains four backup satellites flying as well.[65]

The SBIRS satellite system, though significantly behind schedule, currently operates two GEO satellites, with two more nearing completion and two more to be produced. Additionally, two HEO (highly elliptical orbit) systems are in orbit, with a third delivered in mid-2013 but not yet launched and a fourth in production.[66] While the U.S. waits for the full constellation of SBIRS satellites, no more than five legacy DSP satellites continue to supplement SBIRS satellites in supplying early warning of ballistic missiles.[67]

The WGS satellite constellation of six satellites is working and is supplemented by several of the eight remaining legacy DSCS III satellites, which have exceeded their designed lifespan.[68] Additionally, it is expected that three extra satellites will be added to the constellation by FY 2018.[69] The AEHF constellation is currently composed of three satellites, with a fourth in production and two more under contract.[70] AEHF also uses the five Milstar satellites that were in operation as of February 2014.[71]

There is also a variety of other satellite systems, including various high-end reconnaissance satellites and the Mobile User Objective System that, with two of a planned five satellites deployed, provides better connectivity to warfighters in the field and on the move.[72]

Bandwidth and Processing Capacity. The strength of U.S. satellite constellations is further evidenced by the capacity of satellites to transmit data, as well as by their unique design capability, which allows them to carry out a variety of important tasks. GPS satellites have been updated consistently, adding additional and more powerful signals, anti-jamming capabilities, and accuracy.[73] SBIRS similarly advances beyond DSP capabilities by providing more reliable, detailed, and timely information to military forces.[74]

The WGS provides a dramatic increase in capability over the DSCS system, with one WGS satellite providing greater communications capacity than the entire DSCS III constellation or more than 10 times the capacity of one DSCS III satellite.[75] Similarly, the AEHF can handle 10 times more data than Milstar and provides each user with more than five times the bandwidth.[76] AEHF is better able to communicate with other satellites to speed the flow of information and has more antennas able to support specific operations.

Providing direct satellite communications support to battlefield users, however, remains difficult, especially with regard to mobile frontline forces. In 2010, before the launch of two MUOS satellites, Rebecca Cowen-Hirsch, then president of Inmarsat Government Services, Inc., stated that "[T]actical communications in narrowband is one of the areas that is so significantly broken right now.... [F]or every one request for UHF [Ultra-high frequency] capacity [that's accepted], five are denied."[77] With MUOS satellites providing "a 16-fold increases in transmission throughput over the current UAF satellite system," this support gap is being addressed.[78]

Threat to Lifespan, Number, and Capability. U.S. capabilities in space are unmatched, but with competitors improving their satellite and anti-satellite technologies, continued U.S. dominance is by no means guaranteed. For example, the Chinese BeiDou-2 global navigation system of satellites is operating in East Asia with at least 14 operational satellites in orbit, and Beijing plans to expand this constellation to as many as 35 by 2020.[79] Additionally, China has at least two communication satellite constellations, a weather satellite constellation, and a number of reconnaissance and intelligence satellites.[80] The Chinese have also engaged in numerous tests of anti-satellite capabilities without customary warnings to the international community.[81]

Moreover, China is not the only one of America's geopolitical rivals pushing forward with new satellite and space system technology. Russia, for example, has its GLONASS system composed of 24 operational satellites, giving it global coverage.[82] Russia also maintains a series of communications and reconnaissance satellites.[83] The secrecy surrounding space programs makes any full assessment of space capabilities difficult, but enough evidence exists to show that what was once a nearly exclusive advantage for the U.S. is increasingly less so.

As U.S. systems and operations increasingly use and rely on satellite support, satellites and the capabilities they provide will become more critical. Consequently, one would expect to see a prioritization of funding for satellites, but that has not been the case. Instead, spending on military space systems declined from around $15 billion in FY 2000 to approximately $8.5 billion in FY 2010.[84] In 2012, President Obama requested an additional 22 percent cut in military space spending for his FY 2013 budget. Although Congress rejected this request, the overall pressure on defense spending is likely to stress funding for national security space systems at the same time that the U.S. is increasingly reliant on them.

In fact, it is estimated that some 80 percent or more of the satellite bandwidth currently used by the U.S. military is supplied by the private sector and full motion video.[85] Data, especially imagery, from various reconnaissance systems including UAVs, ground systems, and other sources that use satellites as relays take up an enormous amount of bandwidth. As a result, the Department of Defense has had no choice but to move this information over commercial satellites.

While considered less secure than military-grade satellites, commercial satellites have the advantage of being more numerous and more frequently updated as private-sector companies compete with one another.[86] Other nations, like the United Kingdom, have closer cooperation and partnerships between their military and commercial providers, but the U.S. has not yet established this sort of clear relationship, and this limits the effectiveness of the means by which draws on commercial satellites.[87]

With regard to satellite systems, the needs of the U.S. military are currently being met. U.S. military forces are able to do what they need to do with such systems.[88] However, as data transmission demands continue to increase, the military's needs will soon exceed America's existing satellite capacity. Constrained budgets are causing senior leaders to consider ways to manage constellation degradation, to include greater reliance on commercial systems. While this option works well in peacetime, it accepts significant risk in war, especially given the effort by competitors such as China to develop anti-satellite capabilities and the growing challenges to ground station control capability posed by cyber attacks.

In 2011, then-Secretary of the Air Force Michael Donley and then-Vice Chairman of the Joint Chiefs of Staff General James Cartwright suggested looking to partner nations in Europe and perhaps even geostrategic competitors (like China) to supplement U.S. capabilities.[89] Doing so would certainly account for shortfalls in U.S. proprietary capacity, but it also would accept significant risk in defense planning—a situation that is in no way conducive to protecting the United States' vital national interests.

Cyberspace: A New Domain with Unique Challenges and Opportunities

Cyberspace could be said to have begun on October 29, 1969, when engineers 400 miles apart at the University of California in Los Angeles and the Stanford Research Institute (SRI) sent data over the "Arpanet," a network whose name derived from the agency funding the undertaking, the Defense Department's Advanced Research Projects Agency (ARPA).[90] The network began when one scientist attempted to log in remotely to a computer at SRI. He first typed the letter "L," then "O," then "G." Then the system crashed. Three hours later, it was up and running again, and the world has been "logging on" ever since.

In the 1970s, more computers, mostly at research institutions and military organizations, were added to "ARPANET," and basic applications like e-mail were created. Upgrades to ARPANET's protocols that enhanced "Internetting," or the improvement of communication between networks, were developed throughout the decade. As the Internet grew, so did the potential for malware, and the first known virus, dubbed "Brain," was discovered in 1986.[91]

Important transitions of protocols occurred in the early 1980s, enabling a split between research organizations and military operational organizations. Other government agencies and communities saw the power of the early Internet and latched onto it as well. By the end of the 1980s, private companies were able to participate in the development and use of the Internet.[92] In 1998, the U.S. government relinquished control of the Internet's naming function to the Internet Corporation for Assigned Names and Numbers (ICANN) under contract to the Department of Commerce, leading to the recent dramatic expansion of Internet-based technologies.

With these advances, however, has come the potential for exploitation. An increase in the capability to break into computer systems for espionage, crime, political statements, cyber destruction, and even physical destruction has paralleled the expansion of cyberspace. Malware, malicious hardware, and other types of cyber attacks are inherent in cyberspace and have created the need for cybersecurity.

Due to the devastating impact that they could have on critical infrastructure and military systems, cyber weapons—as well as the cyber capabilities of geopolitical rivals—pose a serious threat to U.S. interests.[93] Cyber attacks could be used in tandem with efforts to attack or coerce the U.S. or its allies such as Israel, Taiwan, Japan, Poland, or Estonia. Cyber weapons also could be employed at a sufficiently serious level by such belligerent actors as Iran, North Korea, or terrorists who are interested in a show of strength or simply destruction and terror.

While cyber-espionage, cyber-crime, and other cyber threats to U.S. interests and the freedom of the Internet are serious offenses, such actions are, by definition, not a use of hard power: defined as military might or the ability to project physical force.[94] The *Tallinn Manual*, an effort by 20 respected legal experts to apply various laws of war to cyber conflict, provides perhaps the clearest definition of when to treat a cyber attack as an "armed attack," or the clear use of hard power that justifies military self-defense.

The manual sees hard-power use of cyber capabilities (i.e., armed attack) as those cyber operations whose "effects … were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack."[95] Therefore, this *Index* will focus on cyber operations that are of sufficient scale and effect that they could be considered hard power and used as part of an "armed attack." The experts of the manual were divided on whether an operation whose scope and magnitude causes "extensive negative effects," including economic or physical disruptions, but without large-scale fatalities should be considered an armed attack.[96] Given that such an attack could be considered an armed attack by different actors, it will also be examined in this *Index*.

Cyberspace as an Operating Environment. Cyberspace is a unique operating environment that challenges the U.S in multiple ways. These challenges include the cyber domain's reach, speed, anonymity, and offense-dominated nature. Being a relatively new field of warfare, the cyber environment is one within which the U.S. is learning to operate. Understanding the unique nature and challenges of this realm, as well as the U.S.'s policies and the capabilities of its allies, is important to an assessment of the U.S. military's ability to conduct military operations in the 21st century.

Cyberspace can be defined as "the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds."[97] Looking even closer, cyberspace is composed of four layers:

- **Physical systems.** These include computers, machines connected to or controlled by a remote source, wires and cables, routers, and other pieces of physical hardware that allow for the interconnectivity between and operation of devices.

- **Logical systems.** Beyond hardware lie the important logic and software that make up the current Internet and cyber domain. The current system is defined by certain protocols and rules that allow different programs to be compatible and communicate with each other. From this logic come various forms of software and applications, all of which build on each other and work together to complete certain tasks.

- **Information.** To some extent, each system in cyberspace stores, sends, and receives information. Before the interconnectivity of computers, this information was still stored digitally but was not easily accessible to other individuals or devices. Cyberspace is defined by the unlocking of this information from its physical location and allowing it to transit the world for analysis, use, and even theft or exploitation at a rapid pace.

- **People.** Ultimately, cyberspace serves the needs of individuals and groups by providing the ability to communicate or analyze information, start or stop a process, or engage in countless other activities across the world and in conjunction with others. The customs, needs, organization, and training of different peoples affects the way in which cyberspace is used.[98]

Together, these four layers, interconnected around the world, form the foundations of cyberspace as it is known today. Flowing from this construct, cyberspace contains three unique features that not only support U.S. civilian and military activities, but can also be used against the U.S. Specifically, cyberspace is:

- Ubiquitous,

- Anonymous, and

- Offense-dominated.

Ubiquitous. Cyberspace is defined largely by its vast reach and the ability of an individual to communicate with any computer in the world and vice versa.[99] According to various estimates, at the end of 2008, there were at least 1 billion personal computers in use around the world—a number that it is estimated will double to 2 billion by 2015. Additionally, there were an estimated 1.4 billion smartphones in use at the end of 2013 and countless other cyberspace-connected devices, both in the civilian world and in the military, known as the "Internet of things."[100]

Each of these devices has the ability to access information and send commands across the Internet, interacting with any number of other devices. In most cases, this capability is peaceful and productive. However, it also allows hackers or those who seek to exploit unauthorized access to a computer system or network, whatever their allegiance and wherever they are, to abuse cyberspace and use it for their own ends.

As the world's most technologically advanced military, the U.S. military uses cyberspace in numerous ways. In some areas, cyberspace has not only enhanced, but profoundly changed the way in which the U.S. military operates. Several of the most critical areas include:

- Command and control systems;

- Communications;

- Guidance and navigation systems;

- Intelligence and information-gathering, information-analyzing, and information-sharing systems;

- Vehicle, aircraft, and ship operations;

- Offensive cyber operations;

- Logistics, or the sustainment of military operations; and

- Research.

Most of these areas affect critical warfighting capabilities spread across all four branches of the U.S. military.

Additionally, the U.S. homeland depends on 16 sectors of interdependent critical infrastructure, most of which are reliant on cyberspace. The Department of Homeland Security, together with other government agencies, is responsible for protecting these sectors. The 16 critical infrastructure sectors are:

- Chemical;
- Commercial facilities;
- Communications;
- Critical manufacturing;
- Dams;
- Defense industrial base;
- Emergency services;
- Energy;
- Financial services;
- Food and agriculture;
- Government facilities;
- Health care and public health;
- Information technology;
- Nuclear reactors, materials, and waste;
- Transportation systems; and
- Water and wastewater systems.[101]

Most of these sectors depend either directly or indirectly on cyberspace. For example, a power plant and other parts of the electric grid are managed and controlled by Internet-based communication and control systems, such as Industrial Control Systems (ICS) and Smart Grid technologies.[102] Should these systems be disabled, a cascade of failures could begin. For example, a grocery store depends on electricity to use cash registers, run refrigerators, and order more food. The supply chain depends on communications and logistics systems that rely on electricity and Internet-based communications. Even farm irrigation systems may require electricity.

Such interdependence within critical infrastructure and widespread reliance on cyberspace creates serious vulnerabilities that can be exploited. Compounding these vulnerabilities, much of the critical infrastructure in the U.S. is owned and operated by the private sector, meaning that the government does not control their operations—even if it is charged with their protection.

Anonymous. Perhaps the most often remarked feature of cyberspace is its anonymity.[103] It is difficult to determine the origin of a cyber attack or probe. First, an attack or penetration must be noticed. Then, forensic analysis of the attack mechanism must be undertaken to pinpoint the source of the intrusion and trace it back to the attacker. Depending on the complexity or type of attack, this process could take a significant amount of time. Even if the geographic origin of the attack is confirmed, it may be difficult to determine who exactly is responsible.[104]

This problem is exacerbated by the ability of hackers to redirect their attacks through other locations, making it difficult to pinpoint the true origin of the attack. For example, an attack by China could be routed through U.S. systems to appear as though the attack originated within the U.S.[105] While not impossible to solve, misdirections require time and resources that might not be available during a period of crisis.

For all of the difficulty ascribed to attributing cyber attacks to the correct actor, the "attribution problem" may in some circumstances be overstated.[106] The ability to break through the anonymity of cyber attacks is improving as defenders are using the vulnerabilities and mistakes of hackers to track them down faster and more effectively.[107] (For example, in December 2014, the U.S. government determined within a number of days that a cyber-attack on Sony Pictures Entertainment originated with the government of North Korea.) In some cases, a devastating cyber attack could be sourced by placing the attack in the context of other global affairs. For example, if the West Coast power grid and U.S. military systems in the Asia–Pacific theater were disrupted, and if China at the same time began aggressive or coercive action against Taiwan or Japan, such events could inform the U.S. attribution process.

Similar examples can be seen with other actors that might be expected to pair their cyber attack with physical attacks or coercion—for example, as seen during Russia's invasion of Georgia in 2008.[108] Additionally, while any one cyber attack may be difficult to attribute to an actor, a series or campaign of attacks gives more data points with which to identify an attacker. Nevertheless, the attribution challenge and anonymous nature of cyberspace do still complicate U.S. responses to cyber attacks.

Offense-Dominated. For multiple reasons, cyberspace is currently considered an offense-dominated domain. It is easier, cheaper, and generally more effective to engage in offense rather than in defense. Cyber action is both instantaneous and constantly changing, which makes defense difficult. The dissemination of interconnected systems means that millions of potential targets are vulnerable to exploitation. And because the attacker has to find just one hole to exploit, cyber aggression is an appealing and cheap form of asymmetric warfare. Each of these reasons deserves greater explanation.

First, a main feature of cyberspace that contributes to the superiority of offense is its speed and dynamic nature.[109] Though it can take months to find and exploit a vulnerability, the actual cyber attack occurs instantly. Furthermore, danger in the cyber-sphere is constant. Of the weapons in the arsenals of potential enemies, cyber weapons are the fastest and often provide little or no warning, making it difficult for defenses to be prepared and reinforcements brought to bear.[110]

Compounding these challenges, new types of cyber attacks and vulnerabilities are constantly being discovered and developed by hackers. As a result, cybersecurity defenders are constantly playing catch-up.[111] Of course, this assumes that defenders are even aware of a potential intrusion. Incomplete security systems or brand-new types of threats could evade the watchful eye of cybersecurity professionals until well after significant damage has been done.

Second, the wide variety of targets means that defenders have a lot to defend.[112] As noted, the military and critical infrastructure sectors of the U.S. and other nations are all largely dependent on cyberspace.[113] Worse, cyber attacks have the capability to target important systems indirectly by instead assaulting different systems on which the original systems rely. For example, attacking the command and control system of a B-2 might be easier than attacking the B-2 itself. Given the constantly evolving nature of cyberspace, it is practically impossible to secure every system perfectly—especially since the vast majority of critical infrastructure belongs to the private sector, with companies all at different places in their cybersecurity development.

Third, cyberspace is filled with potential adversaries who either have or could relatively easily acquire significant offensive cyber capabilities.[114] This is driven by the low cost of entry for cyber warfare and the great potential for damage, making it similar to other inexpensive forms of asymmetric warfare.[115] An opponent may not be able to field a global navy or large squadrons of advanced fighter jets, but it can still wreak significant levels of destruction with a much less expensive cyber force.[116]

Many militaries and nations around the world are therefore interested in developing cyber capabilities that can help them to level the playing field. This is certainly true of potential cyber adversaries such as North Korea, Iran, Russia, and China, not to mention terrorists. Thus, the U.S. should expect to see a continued buildup of cyber capabilities by actors around the world as an asymmetric challenge to U.S. capabilities.

Cyber Attacks and Their Effects. Given these features of the cyber environment, cyber attacks are a serious avenue through which attacks can be launched, affecting the confidentiality, integrity, and availability of information or systems. If information is not private, the commands flowing from a system are not trusted, or a system is unavailable, then capabilities are weakened.[117]

Part of having a comprehensive grasp of the cyber-operational environment is an understanding of what cyber attacks are and what effects they can have. It is worth repeating that for purposes of this report, only cyber attacks that have severe consequences will be considered, as such attacks would threaten a critical national interest much as the large-scale use of conventional weapons would threaten them. While many military systems operate on their own closed networks, they are still vulnerable to attack.[118] Similarly, attacks against critical infrastructure could overwhelm various systems since many sensitive control systems are insecurely connected to the Internet. [119]

TABLE 1

World Cyber Threats

The most serious threats in cyberspace come from nation-state and associated actors. With more resources and greater ambitions and objectives than most criminal organizations, nation-state attacks and hacks are among the largest, most aggressive, and most noteworthy acts of cyber-aggression.

E Economic
M Military
P Political

Country	**North Korea**	**Russia**	**Iran**	**China**
Capability	Limited Capability	Very Capable	Moderate Capability	Very Capable
Overview	Aggressive, unpredictable, scattered across the world	Non-government and criminal "patriotic hackers," technologically advanced	Social network savvy, regional economic destabilizer	Globally diverse campaign of economic and military espionage, strategic mindset
International Attacks 	P 48,000 South Korean bank, media, and government computers and servers attacked in 2013 P Various attacks on South Korean and U.S. institutions coinciding with July 4 events and annual U.S.-South Korea military exercises	M P 54 government, finance, and communication websites attacked during invasion of northern Georgia in 2008 P Estonian banks and government websites attacked following the moving of a Soviet war memorial in 2007	E P Oil company Saudi Aramco attacked in 2012, destroying 30,000 computers E P Qatari natural gas company Rasgas's computer networks attacked in 2012	E Theft of hundreds of billions of dollars in IP from numerous nations across the world P Hong Kong's voter registration system attacked after protests of China's involvement in selecting a new state leader in 2014
Attacks on U.S. Systems 	P 2009 attacks on U.S. and South Korean government websites, including crashing the Federal Trade Commission site	E 2012 data theft by "Energetic Bear," targeting the international energy sector, manufacturers, and defense contractors E P Campaign of infiltration of U.S. energy and critical infrastructure networks by the "Black Energy" malware starting in 2011 and discovered in 2014	P Crashing of major U.S. bank websites following the 2012 sanctions on Iran E P Since 2012, "Operation Cleaver" has been breaching U.S. military, airline, energy, and other companies' networks, as well as a variety of other worldwide targets	E 2009 theft of F-35 plans from U.S. Department of Defense E U.S. Department of Justice charges Chinese military officials in 2014 with hacking and economic espionage against six U.S. energy, mining, and manufacturing companies from 2006 to 2014

Source: Heritage Foundation research and analysis provided elsewhere in this study.

heritage.org

Malware. Malware stands for "malicious software" and includes viruses, worms, Trojans, rootkits, and many other types of attacks.[120] Malware often has the ability to replicate and spread with little or no help from human users. While many forms of malware, such as spyware, act surreptitiously and try to avoid being seen, such malware are generally associated with cyber espionage or crime—activities that are not hard-power uses of cyber weapons—although they can be used to create backdoors or vulnerabilities in computer systems that can later be used for other purposes.

On the other hand, some malware can be highly destructive to the functioning of a system. Trojans can take over control of a computer, obviously a dangerous capability in the hands of an adversary. Viruses and worms are the most easily spread forms of malware as they can replicate on their own. Among their more malicious capabilities, viruses and worms can disable computers by deleting critical data and preventing correct operation.[121]

For some, disabled military platforms are merely an annoyance; for others, successful operation depends entirely on a working computer system or program. Even systems that are "air gapped," or not connected to the Internet, are at risk via the supply chain when infected devices are connected to the closed system during updating or just by accident, or through other clever forms of transmission.[122] Malware's ability to spread, permanently disable, or even control a system makes it a dangerous cyber weapon in the hands of a dedicated opponent.

Denial of Service. Billions of computers are connected to the Internet with access to millions of other computers and websites.[123] When too many computers try to connect with a website or computer, the target will slow down or even fail as scarce resources are used up trying to process these requests.

Denial-of-service (DOS) attacks send a flood of partial or flawed communications to a target system or site, leaving the target unable to respond effectively. These requests build up and eventually cause the target to slow down or crash. DOS attacks can be strengthened when a hacker places malware on thousands of other computers, thereby allowing the hacker to control these computers or "bots." These otherwise innocent computers will then do the hacker's bidding, multiplying the faulty requests sent to a website or system in what is known as a distributed DOS or DDOS attack.[124]

While DOS attacks can blind and disrupt, they are generally temporary in nature and do not leave any permanent cyber damage, though some advanced techniques, known as "phlashing" or "bricking," can render hardware inoperable.[125] Prolonged DOS attacks have been used to great effect, notably in Russia's campaign against Georgia in 2008, in which debilitating DOS attacks froze the websites of Georgian government and media organizations. These attacks, in addition to limiting Georgia's ability to communicate with its citizens and the outside world, coincided with a Russian military incursion in different areas of Georgia.[126] DOS attacks will likely be part of any coordinated cyber attack against the U.S. or its allies, but they are generally the least harmful.

Malicious Hardware. Military and some critical infrastructure systems are at least somewhat protected from cyber attack because they reside on closed systems. Hardware threats avoid this potential defense, however, by being physically built into a computer system so that, regardless of how connected a device is to cyberspace, malicious instructions can be carried out. Given the interconnected nature of the technology industry's supply chain, a single device can be made of thousands of parts, each built by a different contractor in a different country, making it difficult to be assured of a device's security and integrity.

Hardware threats are generally less known and can be difficult to identify because they often go unnoticed until activated.[127] Finding malicious hardware can be extremely difficult, since computer systems are often created from a multitude of parts, all potentially originating from different countries and different companies, with multiple contractors and subcontractors. Furthermore, testing hardware to find potential flaws or malicious circuitry is extremely problematic because testing cannot be exhaustive enough to cover all potential inputs or commands that a computer or individual chip might be given.[128]

If hardware contains malicious circuitry, it can be activated at certain times, in certain places, or on demand. Once activated, malicious hardware can fail outright or just operate in an impaired manner.[129] Hardware can also serve as a backdoor for the introduction of malware.[130] Malicious hardware can build up over time, waiting for a potential conflict, and serve as a strategic way for an adversary to compromise another nation's cyber systems.

Insider Attacks and Social Engineering. It is worth mentioning that a potential attacker may use employees, contractors, or other people with inside access to an organization to provide the opportunity for an attack. This can occur directly, in the case of insider attacks where a mole creates a vulnerability through which attackers can unleash an attack, or indirectly, in the case of social engineering that tries to trick individuals into giving up sensitive information or unknowingly enable a larger attack to come through.

Targeted and Advanced Persistent Threats (APT). While not a type of attack itself, it should be noted that advanced bad actors could use a combination of sophisticated and specifically tailored attack mechanisms to attack a target or group of targets persistently. Such strategies are often the work of nation-states or large criminal-hacker enterprises with significant amounts of resources.[131] Importantly, these attacks can often bypass security measures and exploit holes in cyber defenses known as "zero-day" vulnerabilities, or vulnerabilities that were not known until they were used by hackers to exploit a system.

Additionally, many APT attacks follow an attack sequence that includes initial reconnaissance, the initial attack that breaches a system, building additional backdoors into the compromised system, gaining privileges and command and control powers, finding information, and exfiltrating information, all while continuing to hide one's presence and establishing additional backdoors and privileges. This process can continue for years as the victim is continually robbed or harmed.[132]

Advanced attacks can even result in physical damage. One the first examples of such an attack occurred in 1982 when the U.S. introduced faulty software into the pipeline control program of a Soviet gas pipeline. The program caused excessively high pressures within the pipes, causing what *The Washington Post* called "the most monumental non-nuclear explosion and fire ever seen from space.[133]"

More recently, Stuxnet, one of the most complex pieces of malware the world has ever seen, caused the centrifuges at the Iranian nuclear facilities to spin occasionally at speeds that would damage the sensitive machinery.[134] Stuxnet did so subtly, thereby concealing its actions from the Iranians for over a year. Physical damage from advanced cyber attacks is likely to become more common as more and more physical items are connected to the Internet of things.[135]

The military, like any other community, is reliant on the cyber domain in everything it does, from simple administrative tasks to conducting war. Every feature of cyber is dynamic, from the scope and breadth of the domain itself to the tools used to conduct legitimate business and for malicious purposes, as well as for offense and defense in military affairs.

It took armies 50 years to digest the implications of industrialized warfare, from the time high-volume firepower and nearly instantaneous communications were introduced to the battlefield in the U.S. Civil War to their slaughtering effects on Europe's battlefields in the First World War, and 25 years to understand the implications of airpower and the mechanization of forces as they evolved from their first appearances in World War I to their full manifestation in World War II.

The U.S., its friends, and its competitors are likewise trying to understand the nature and implications of the cyber domain. There is no question, however, that competence in this field, both to defend one's own cybersystems and to challenge enemy cybersystems in wartime, is critical. America's investments in this field should be made accordingly.

Endnotes:

1. Israel likely possesses nuclear weapons capabilities, although it has never officially admitted to possessing them. Pakistan openly demonstrated its nuclear capabilities in 1998, with a series of six tests in response to testing by India. North Korea conducted tests in 2006, 2009, and 2013, and is thought to possess a few weapons.
2. Amy F. Woolf, "Nonstrategic Nuclear Weapons," Congressional Research Service, January 3, 2014, http://www.fas.org/sgp/crs/nuke/RL32572.pdf (accessed September 16, 2014).
3. Fallout is radioactive debris that results from a nuclear explosion, is carried aloft into the air at considerable distance from the detonation, and then returns to Earth and contaminates areas potentially far removed from the original blast site. Electromagnetic pulse (EMP) is also an effect created by a nuclear blast in which a massive burst of electromagnetic energy is generated and propagated through the atmosphere and possesses the ability to damage electronic equipment.
4. Baker Spring, "Congressional Commission Should Recommend a 'Damage Limitation' Strategy," Heritage Foundation *Backgrounder* No. 2172, August 14, 2008, http://www.heritage.org/research/reports/2008/08/congressional-commission-should-recommend-damage-limitation-strategy.
5. Bernard Baruch, "The Baruch Plan," presented to the United Nations Atomic Energy Commission, June 14, 1946, http://www.atomicarchive.com/Docs/Deterrence/BaruchPlan.shtml (accessed May 22, 2014).
6. "Counterforce targets" refers to a set of targets that have a political and military value (e.g., bomber bases, army battalions, or leadership). Countervalue targets are economic and civilian centers (e.g., cities or food factories).
7. Herman Kahn, *On Thermonuclear War* (Princeton, NJ: Princeton University Press, 1961), p. 96.
8. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), p. 233.
9. For a detailed examination of the evolution of the theory and practice of deterrence from the 1960s to the present, see Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008).
10. William Ogle, "An Account of the Return to Nuclear Weapons Testing by the United States after the Test Moratorium 1958–1961," United States Department of Energy, Nevada Operations Office, October 1985.
11. George H. Miller, Paul S. Brown, and Carol T. Alonso, *Report to Congress on Stockpile Reliability, Weapon Remanufacture, and the Role of Nuclear Testing*, Lawrence Livermore National Laboratory, October 1987, p. 3, http://www.osti.gov/scitech/servlets/purl/6032983 (accessed November 20, 2014).
12. Thomas Scheber, "Reliable Replacement Warheads: Perspectives and Issues," United States Nuclear Strategy Forum, August 2007, pp. 4–5, http://www.nipp.org/Publication/Downloads/Publication%20Archive%20PDF/RRW%20final%20with%20foreword%207.30.07.pdf (accessed September 16, 2014).
13. Kathleen C. Bailey, "The Comprehensive Test Ban Treaty: The Costs Outweigh the Benefits," Cato Institute *Policy Analysis* No. 330, January 15, 1999, p. 9, http://www.cato.org/pubs/pas/pa330.pdf (accessed September 16, 2014).
14. Transcript, "National Defense Industrial Association, Air Force Association and Reserve Officers Association Capitol Hill Breakfast Forum with Don Cook, Deputy Administrator for Defense Programs, National Nuclear Security Administration, on Nuclear Weapons Sustainment," July 7, 2012, http://secure.afa.org/HBS/transcripts/2012/7-10-2012%20Dr.%20Donald%20Cook.pdf (accessed November 20, 2014).
15. David H. Sharp, "Nuclear Testing: Deterrence, Stewardship, and Arms Reduction," Los Alamos National Laboratory, Report No. LA-UR-08-06803, p. 10.
16. Kathleen C. Bailey, "The Comprehensive Test Ban Treaty: An Update on the Debate," National Institute for Public Policy, March 2001, p. 10, http://www.nipp.org/National%20Institute%20Press/Archives/Publication%20Archive%20PDF/CTBT%20Update.pdf (accessed September 16, 2014).
17. Sharp, "Nuclear Testing: Deterrence, Stewardship, and Arms Reduction," p. 11.
18. Ambassador C. Paul Robinson, John Foster, and Thomas Scheber, "The Comprehensive Test Ban Treaty: Questions and Challenges," Heritage Foundation *Lecture* No. 1218, November 7, 2012, http://www.heritage.org/research/lecture/2012/11/the-comprehensive-test-ban-treaty-questions-and-challenges (accessed June 25, 2014).
19. The Comprehensive Test Ban Treaty does not define what constitutes a nuclear weapons experiment.
20. Michaela Dodge and Baker Spring, "Keeping Nuclear Testing on the Table: A National Security Imperative," Heritage Foundation *Backgrounder* No.2770, February 27, 2013, http://www.heritage.org/research/reports/2013/02/keeping-nuclear-testing-on-the-table-a-national-security-imperative (accessed September 16, 2014).
21. Office of Technology Assessment, *The Effects of Nuclear War*, May 1979, http://ota.fas.org/reports/7906.pdf (accessed September 16, 2014).
22. General Larry Welch, USAF, transcript of remarks, Air Force Association Huessy Congressional Breakfast Series, May 25, 2012, http://secure.afa.org/HBS/transcripts/2012/5-25-2012%20Gen%20Larry%20Welch%20v2.pdf (accessed September 16, 2014).

23. The Heritage Foundation "Nuclear Powers Emerge as U.S. Stockpiles Shrink," May 25, 2010, http://www.heritage.org/multimedia/infographic/nuclear-powers-emerge-as-us-stockpile-shrinks; U.S. Department of State, "Fact Sheet: New START Treaty Aggregate Numbers of Strategic Offensive Arms," April 1, 2014, http://www.state.gov/t/avc/rls/224236.htm (accessed October 7, 2014). It is important to recognize that arms control treaties since the end of the Cold War have used different counting rules. The U.S. currently maintains around 2,000 real nuclear warheads.
24. Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START Treaty), signed July 31, 1991, http://www.state.gov/t/avc/trty/146007.htm (accessed November 20, 2014).
25. These transparency measures remained in effect until START I's expiration in 2009.
26. Treaty Between the United States of America and the Russian Federation on Strategic Offensive Reductions (SORT / Treaty of Moscow), signed May 24, 2002, http://cns.miis.edu/inventory/pdfs/aptsort.pdf (accessed September 16, 2014).
27. Julian Borger, "Nuclear Weapons: How Many Are There in 2009 and Who Has Them?" *The Guardian Online*, September 25, 2009, http://www.theguardian.com/news/datablog/2009/sep/06/nuclear-weapons-world-us-north-korea-russia-iran (accessed June 6, 2014).
28. Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START Treaty), signed April 8, 2010, http://www.state.gov/documents/organization/140035.pdf (accessed September 16, 2014).
29. Keith B. Payne, "Evaluating the U.S.–Russia Nuclear Deal," *The Wall Street Journal Online*, updated April 8, 2010, http://online.wsj.com/news/articles/SB20001424052702303720604575169532920779888 (accessed June 11, 2014).
30. Paula DeSutter, "Verification and the New START Treaty," Heritage Foundation *Lecture* No. 1160, July 12, 2010, http://www.heritage.org/research/lecture/verification-and-the-new-start-treaty.
31. New START Working Group, "New START: Potemkin Village Verification," Heritage Foundation *Backgrounder* No. 2428, June 24, 2010, http://www.heritage.org/Research/Reports/2010/06/New-START-Potemkin-Village-Verification.
32. News release, "Key Facts About the New START Treaty," The White House, March 26, 2010, http://www.whitehouse.gov/the-press-office/key-facts-about-new-start-treaty (accessed September 16, 2014).
33. Michaela Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security," Heritage Foundation *Backgrounder* No. 2875, February 18, 2014, http://www.heritage.org/research/reports/2014/02/us-nuclear-weapons-in-europe-critical-for-transatlantic-security.
34. Ibid.
35. John T. Cappello, Gwendolyn M. Hall, and Stephen P. Lambert, "Tactical Nuclear Weapons: Debunking the Mythology," USAF Institute for National Security Studies *Occasional Paper* No. 46, August 2002, p. 11.
36. Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security."
37. U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010, p. iii, http://www.defense.gov/npr/docs/2010%20nuclear%20posture%20review%20report.pdf (accessed September 16, 2014).
38. News release, "Fact Sheet: Nuclear Weapons Employment Strategy of the United States," The White House, June 19, 2013, http://www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states (accessed September 16, 2014).
39. U.S. Department of State, "Fact Sheet: Transparency in the U.S. Nuclear Weapons Stockpile," April 29, 2014, http://www.state.gov/t/avc/rls/225343.htm (accessed September 16, 2014).
40. International Atomic Energy Agency, "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran," Report by the Director General, GOV/2011/65, November 8, 2011, http://www.iaea.org/Publications/Documents/Board/2011/gov2011-65.pdf (accessed September 16, 2014).
41. We must not forget that the newly armed nations are already "using" their nuclear weapons in a nonmilitary sense: for example, to prevent significant intrusions into their political structure despite massive human rights violations or to limit retaliation in response to their aggressive behaviors. See Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt and Company, 2012).
42. Spring, "Congressional Commission Should Recommend a 'Damage Limitation' Strategy."
43. Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security."
44. North Atlantic Treaty Organization, "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization," Adopted by Heads of State and Government at the NATO Summit in Lisbon, November 19–20, 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (accessed September 16, 2014).
45. Ibid.
46. Press release, "Deterrence and Defence Posture Review," North Atlantic Treaty Organization, May 20, 2012, http://www.nato.int/cps/en/natolive/official_texts_87597.htm (accessed September 16, 2014).
47. News release, "Fact Sheet on U.S. Missile Defense Policy: A 'Phased, Adaptive Approach' for Missile Defense in Europe," The White House, September 17, 2009, http://www.whitehouse.gov/the_press_office/FACT-SHEET-US-Missile-Defense-Policy-A-Phased-Adaptive-Approach-for-Missile-Defense-in-Europe (accessed September 16, 2014).

48. Amaani Lyle, "Hagel: U.S. Bolstering Missile Defense," American Forces Press Service, March 15, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119543 (accessed September 16, 2014).

49. U.S. Department of Defense *Nuclear Posture Review Report*, April 2010.

50. "Fact Sheet: Nuclear Weapons Employment Strategy of the United States."

51. Ibid.

52. Ibid.

53. News release, "Fact Sheet: An Enduring Commitment to the U.S. Nuclear Deterrent," The White House, November 17, 2010, http://www.whitehouse.gov/the-press-office/2010/11/17/fact-sheet-enduring-commitment-us-nuclear-deterrent (accessed September 16, 2014).

54. U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010.

55. Transcript, "2013 Carnegie International Nuclear Policy Conference: Morning Plenary Session: Prague 2.0? Deterrence, Disarmament, and Nonproliferation in Obama's Second Term," April 8, 2013, http://carnegieendowment.org/files/0410carnegie-morning-plenary.pdf (accessed September 16, 2014).

56. Michael Dowd, "How Rad Hard Do You Need? The Changing Approach to Space Parts Selection?" Maxwell Technologies White Paper, January 21, 2012, http://www.maxwell.com/images/documents/case_study_micro_e_how_rad_hard.pdf (accessed August 19, 2014); Eagle Picher Technologies, LLC, "Sar-10197 Aerospace Battery," http://www.eaglepicher.com/images/Li-Ion/EP-SAR-10197-DATA-SHEET.pdf (accessed August 19, 2014).

57. *Enyclopedia Britannica*, "Satellite Communication," December 26, 2013, http://www.britannica.com/EBchecked/topic/524891/satellite-communication/288217/How-satellites-work (accessed August 19, 2014).

58. Intelsat, "Tools & Resources: Satellite Station-Keeping," http://www.intelsat.com/tools-resources/satellite-basics/satellite-station-keeping/ (accessed August 19, 2014).

59. News release, "Lockheed Martin-Built GPS Satellite Exceeds 10 Years On-Orbit," Lockheed Martin, February 15, 2011, http://www.lockheedmartin.com/us/news/press-releases/2011/february/gps-10yr-anny.html (accessed August 19, 2014).

60. GPS.gov, "Space Segment," August 2, 2014, http://www.gps.gov/systems/gps/space/#generations (accessed August 19, 2014).

61. Aerospace-Technology.com, "Wideband Global SATCOM (WGS) Satellite, United States of America," http://www.aerospace-technology.com/projects/wgs-satellite/ (accessed August 19, 2014).

62. National Aeronautics and Space Administration, "Milstar 1," http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1994-009A (accessed August 19, 2014); National Aeronautics and Space Administration, "Milstar 2," http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1995-060A (accessed August 19, 2014); fact sheet, "Milstar," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5328 (accessed August 19, 2014).

63. News release, "Military Communications Satellite Built by Lockheed Martin Achieves 10 Years in Service," Lockheed Martin, February 26, 2010, http://www.lockheedmartin.com/us/news/press-releases/2010/february/DSCS-10-YR.html (accessed August 19, 2014).

64. News release, "Northrop Grumman-Built DSP Flight 14 Celebrates 20 Years On-Orbit," Northrop Grumman, June 12, 2009, http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=167062 (accessed August 19, 2014); news release, "Defense Support Program Satellite Decommissioned," Northrop Grumman, July 31, 2008, http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=147496 (accessed August 19, 2014).

65. GPS.gov, "Space Segment."

66. News release, "Lockheed Martin Delivers Third SBIRS HEO Satellite Payload to U.S. Air Force," Lockheed Martin, July 1, 2013, http://www.lockheedmartin.com/us/news/press-releases/2013/july/0701-ss-sbirs.html (accessed August 19, 2014).

67. Fact sheet, "Defense Support Program (DSP) Satellites," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5323 (accessed August 19, 2014); Missile Threat, "Defense Support Program (DSP)," last updated April 29, 2013, http://missilethreat.com/defense-systems/defense-support-program-dsp/ (accessed August 19, 2014).

68. News release, "6th Boeing-built Wideband Satellite Expands Tactical Communications," Boeing, August 7, 2013, http://boeing.mediaroom.com/2013-08-07-6th-Boeing-built-Wideband-Satellite-Expands-Tactical-Communications (accessed August 19, 2014).

69. Fact sheet, "Wideband Global SATCOM Satellite," U.S. Air Force Space Command, June 8, 2012, http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=5582 (accessed August 19, 2014).

70. Lockheed Martin, "Advanced Extremely High Frequency (AEHF)," http://www.lockheedmartin.com/us/products/advanced-extremely-high-frequency--aehf-.html (accessed August 19, 2014); fact sheet, "Advanced Extremely High Frequency (AEHF) Satellite System," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5319 (accessed August 19, 2014).

71. Ibid.

72. Lockheed Martin, "Mobile User Objective System (MUOS)," http://www.lockheedmartin.com/us/products/mobile-user-objective-system--muos-.html (accessed August 19, 2014); U.S. Navy, Space and Naval Warfare Systems Command, "MUOS-2 Launch from Cape Canaveral Air Force Station, Fla., July 19, 2013," http://www.public.navy.mil/spawar/Press/Pages/MUOS-2.aspx (accessed August 19, 2014).

73. GPS.gov, "Space Segment."

74. Lockheed Martin, "Space Based Infrared System," http://www.lockheedmartin.com/content/dam/lockheed/data/space/documents/sbirs/1_SBIRSInformationalBrochure.pdf (accessed August 19, 2014).

75. Boeing, "Transformational Wideband Communication Capabilities for the Warfighter," http://www.boeing.com/boeing/defense-space/space/bss/factsheets/702/wgs/wgs_factsheet.page (accessed August 19, 2014); U.S. Air Force Space Command fact sheet, "Wideband Global SATCOM Satellite."

76. Lockheed Martin, "Advanced EHF: Assured, Protected, Survivable," July 25, 2013, http://www.lockheedmartin.com/content/dam/lockheed/data/space/documents/AEHF/B1369220_AEHF_7.25.13.pdf (accessed August 19, 2014); Northrup Grumman, "AEHF Payload: Assured, protected, survivable communications," 2014, http://www.northropgrumman.com/Capabilities/AdvancedEHFPayloads/Documents/pageDocs/AEHF_datasheet.pdf (accessed August 19, 2014).

77. Barry Rosenberg, "DOD's Reliance on Commercial Satellites Hits New Zenith," Defense Systems, February 25, 2010, http://defensesystems.com/articles/2010/03/11/cover-story-the-satcom-challenge.aspx (accessed September 18, 2014).

78. Lockheed Martin, "Mobile User Objective System (MUOS)."

79. International GNSS Service, "BeiDou Constellation Status Information," February 25, 2014, http://igs.org/mgex/Status_BDS.htm (accessed August 19, 2014); BBC News, "China's Beidou GPS-Substitute Opens to Public in Asia," December 27, 2012, http://www.bbc.com/news/technology-20852150 (accessed August 19, 2014).

80. Dean Cheng, "Prospects for U.S.–China Space Cooperation," testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate, April 9, 2014, http://www.heritage.org/research/testimony/2014/04/prospects-for-us-china--space-cooperation.

81. Dean Cheng, "China's Space Program: A Growing Factor in U.S. Security Planning," Heritage Foundation *Backgrounder* No. 2594, August 16, 2011, http://www.heritage.org/research/reports/2011/08/chinas-space-program-a-growing-factor-in-us-security-planning.

82. Stephen Clark, "Third Soyuz Launch in a Week Bolsters Glonass System," *Spaceflight Now*, April 26, 2013, http://www.spaceflightnow.com/news/n1304/26soyuz/#.U-uxP2Oa-0Y (accessed August 19, 2014).

83. Anatoly Zak, "Spooky World of Military Satellites," RussianSpaceWeb.com, August 3, 2014, http://www.russianspaceweb.com/spacecraft_military.html (accessed August 19, 2014); Stephen Clark, "Russia Launches 3 New Military Satellites," Space.com, January 17, 2013, http://www.space.com/19307-russia-launches-military-satellites.html (accessed August 19, 2014).

84. Jeff Kueter and John B. Sheldon, "An Investment Strategy for National Security Space," Heritage Foundation *Special Report* No. 129, February 20, 2013, p. 3, http://thf_media.s3.amazonaws.com/2013/pdf/SR129.pdf.

85. Rosenberg, "DOD's Reliance on Commercial Satellites Hits New Zenith."

86. Ibid.

87. Kueter and Sheldon, "An Investment Strategy for National Security Space," p. 15.

88. The phrase "able to do what they need to do" is a relative condition in that requests for support will likely always exceed available resources. Space-based platforms are limited in number, while the intelligence targets on which one might want to collect information or the global activities of the U.S. military for which one likely needs support are expansive. Thus, demands for satellite support are prioritized, and resources are allocated accordingly. If a higher-priority request arises, some ongoing task of lesser priority gets "bumped." Still, in general terms, the U.S. military is able to execute the missions assigned to it. Whether the U.S. intelligence community is likewise able to do so is a matter of conjecture given the high levels of classification that accompany intelligence collection operations. It is also important to note that the role of warning/intelligence becomes even more critical when the size and capabilities of one's armed forces shrinks.

89. Robert Butterworth, "In Space, Doing More with Less Much Scarier than Budget Cuts," George C. Marshall Institute, March 5, 2012, http://marshall.org/space-policy/in-space-doing-more-with-less-much-scarier-than-budget-cuts/ (accessed September 18, 2014).

90. Mark Ward, "Celebrating 40 Years of the Net," BBC News, October 29, 2009, http://news.bbc.co.uk/2/hi/technology/8331253.stm (accessed February 7, 2014).

91. Rupert Goodwins, "Ten Computer Viruses that Changed the World," ZDNet, August 3, 2011, http://www.zdnet.com/ten-computer-viruses-that-changed-the-world-3040093590/ (accessed August 8, 2014)

92. Barry M. Leiner et al., "Brief History of the Internet," Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (accessed July 23, 2014).

93. The cyber community lacks a clear, agreed-upon definition of "cyber weapon." That said, one prominent definition put forward by security researchers at London's King's College defines a cyber weapon as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings." This definition allows for a range of cyber weapons, from the weak denial of service attack to the advanced attacks that cripple or destroy physical devices. Some have argued that such a definition remains too broad and ought to be limited to more severe attacks with physical effects. Be that as it may, this *Index* uses one broad definition so as to not miss a cyber attack that could be considered a cyber weapon. For more information, see Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal*, Vol. 157, Issue 1 (2012), pp. 6–13, http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule (accessed August 8, 2014).

94. "What Is Cybercrime?," Norton by Symantec, http://us.norton.com/cybercrime-definition (accessed July 23, 2014); "Cyberespionage," Oxford Dictionaries, http://www.oxforddictionaries.com/us/definition/american_english/cyberespionage (accessed July 23, 2014); Dimitar Kostadinov, "Cyber Exploitation," InfoSec Institute, February 25, 2013, http://resources.infosecinstitute.com/cyber-exploitation (accessed July 23, 2014).

95. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, ed. Michael N. Schmitt (Cambridge, UK: Cambridge University Press, 2013), p. 54, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 (accessed August 8, 2014).

96. As illustrated by these experts' division on the issue (see *Tallinn Manual*, p. 56), ascertaining where exactly hard power ends and softer forms of power such as espionage and sabotage begins is difficult. This index will not try to solve this definitional and legal problem but will merely consider a viable but not overbroad definition that could be used by the U.S. or other nations in determining their response to serious cyber attacks.

97. Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Vol. 73, Second Quarter 2014, pp. 12–19, http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/8461/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx (accessed August 8, 2014).

98. David Clark, "Characterizing Cyberspace: Past, Present and Future," MIT CSAIL, Version 1.2 of March 12, 2010, https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed July 23, 2014); Department of the Army, *The U.S. Army's Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet No. 525-7-8, February 22, 2010, http://fas.org/irp/doddir/army/pam525-7-8.pdf (accessed August 8, 2014).

99. Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, March 20, 2012, http://belfercenter.ksg.harvard.edu/publication/22046/on_the_use_of_offensive_cyber_capabilities.html (accessed July 23, 2014).

100. Heather Leonard, "There Will Soon Be One Smartphone for Every Five People in the World," *Business Insider*, February 7, 2013, http://www.businessinsider.com/15-billion-smartphones-in-the-world-22013-2 (accessed July 23, 2014); "Computers Sold This Year Worldwide," Worldometers, http://www.worldometers.info/computers/ (accessed July 23, 2014).); Emily Adler, "Here's Why 'The Internet of Things' Will Be Huge, and Drive Tremendous Value for People And Businesses," *Business Insider*, December 7, 2013, http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10#ixzz39ojCP5oL (accessed August 8, 2014).

101. News release, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed July 23, 2014).

102. Steven P. Bucci and Andy Bochman, "Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity," Heritage Foundation *Special Report* No. 150, January 29, 2014, http://www.heritage.org/research/reports/2014/01/plotting-a-more-confident-course-rethinking-oversight-of-the-electric-sector-and-critical-infrastructure-cybersecurity.

103. Belk and Noyes, *On the Use of Offensive Cyber Capabilities*, p. 16.

104. In the event of a serious attack, however, nations that are attacked might attach certain levels of responsibility to the nation that is the source of the attack, depending on the perceived complicity of the source country's government in such attacks. For more information, see Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Atlantic Council *Issue Brief*, January 2012, https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf (accessed August 8, 2014).

105. Nicole Perlroth, "Chinese Hackers Infiltrate New York Times Computers," *The New York Times*, January 30, 2013, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0 (accessed July 23, 2014).

106. Stewart Baker, "The Attribution Revolution," *Foreign Policy*, June 17, 2013, http://www.foreignpolicy.com/artic les/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks (accessed July 23, 2014); Alexander Melnitzky, "Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses," *Cardozo Journal of International and Comparative Law*, Vol. 20, Issue 2 (Winter 2012), pp. 537–570, http://www.cjicl.com/uploads/2/9/5/9/2959 791/cjicl_20.2_melnitzky_note.pdf (accessed July 23, 2014).

107. Baker, "The Attribution Revolution."

108. David M. Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (accessed July 23, 2014).

109. Belk and Noyes, *On the Use of Offensive Cyber Capabilities*.

110. Maren Leed, "Offensive Cyber Capabilities at the Operational Level: The Way Ahead," Center for Strategic and International Studies and Georgia Tech Research Institute, September 2013, http://csis.org/files/publication/130916_Leed_Offensiv eCyberCapabilities_Web.pdf (accessed July 23, 2014).

111. William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed July 23, 2014).

112. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, p. 2, http://www.defense.gov/news/d20110714cyber.pdf (accessed July 23, 2014).

113. Lewis Page, "Upgrade Drags Stealth Bomber IT Systems into the 90s," *The Register*, July 11, 2008, http://www.theregister.co.uk/2008/07/11/stealth_bomber_upgrades/ (accessed July 23, 2014); David Noland, "Could One Email Have Stopped a $1.4B Stealth Bomber Crash?" *Popular Mechanics*, July 2, 2008, http://www.popularmechanics.com/technology/military/planes-uavs/4271563 (accessed July 23, 2014); U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, p. 3.

114. James A. Lewis and Katrina Timlin, Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, United Nations Institute for Disarmament Research, 2011, http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (accessed August 8, 2014)

115. Lynn, "Defending a New Domain."

116. Leed, "Offensive Cyber Capabilities at the Operational Level," p. 1.

117. Margaret Rouse, "Confidentiality, Integrity, and Availability (CIA Triad)," WhatIs.com, May 2013, http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA (accessed August 8, 2014); Shirley Radack, "Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology, http://www.itl.nist.gov/lab/bulletns/bltnmar04.htm (accessed August 8, 2014).

118. Pranita Joshi, Gajendra Singh Chandel, and Subham Joshi, "A Survey on: Resource Consumption Index of Denial of Service Attack in MANET," *International Journal of Science, Engineering and Technology Research*, Vol. 2, No. 2 (February 2013), http://ijsetr.org/wp-content/uploads/2013/07/IJSETR-VOL-2-ISSUE-2-314-318.pdf (accessed July 23, 2014).

119. Edison Electric Institute, "Frequently Asked Questions About Cybersecurity and the Electric Power Industry," June 2013, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity_FAQweb_June2013.pdf (accessed July 23, 2014); Bucci and Bochman, "Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity"; U.S. Department of Homeland Security, "Securing Industrial Control Systems in the Chemical Sector," April 2011, http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf (accessed July 23, 2014).

120. These colorful terms all have rather specific meanings. Some, like "ransomware," one can understand from the name itself. Others, like "rootkit," are more technical and obscure. For a useful guide to the bestiary of malware, see Roger A. Grimes, "Your Quick Guide to Malware Types," *InfoWorld*, December 23, 2012, http://www.infoworld.com/d/security/your-quick-guide-malware-types-205450?page=0,0 (accessed September 30, 2013), and Symantec Corporation, *Internet Security Threat Report*, Vol. 18, April 2013, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18 (accessed September 30, 2013).

121. Veracode, "Common Malware Types: Cybersecurity 101," October 12, 2012, http://blog.veracode.com/20 12/10/common-malware-types-cybersecurity-101/ (accessed July 23, 2014).

122. Rachael King, "Why 'Air Gaps' Don't Always Work in Cybersecurity," *The Wall Street Journal*, July 3, 2014, http://blogs.wsj.com/cio/2014/07/03/why-air-gaps-dont-always-work-in-cybersecurity/ (accessed August 8, 2014); David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2880, March 6, 2014, http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

123. Rod Soderbery, "How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?" *Forbes*, January 7, 2013, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/ (accessed September 30, 2013); Julie Bort, "How Many Web Sites Are There?" *Business Insider*, March 8, 2012, http://www.businessinsider.com/how-many-web-sites-are-are-there-2012-3 (accessed September 30, 2013).

124. U.S. Computer Emergency Readiness Team, "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," last revised February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-015 (accessed September 30, 2013).

125. Cory Jannsen, "What Is Phlashing?" *Techopedia*, http://www.techopedia.com/definition/15270/phlashing (accessed July 23, 2014).

126. Hollis, "Cyberwar Case Study: Georgia 2008."

127. Inserra and Bucci, "Cyber Supply Chain Security."

128. John Villasenor, "Compromised by Design: Securing the Defense Electronics Supply Chain," Brookings Institution, Center Technology Innovation and Center for 21st Century Security and Intelligence, November 4, 2013, http://www.brookings.edu/research/papers/2013/11/4-securing-electronics-supply-chain-against-intentionally-compromised-hardware-villasenor (accessed July 23, 2014).

129. Working in an impaired manner may be just as dangerous as or even more dangerous than causing a system to fail outright. For example, a bug that made every missile miss its target by several yards might not be immediately apparent as a cyber attack, even though it is dramatically affecting the effectiveness of U.S. weapons. Systems that are not working properly, on the other hand, might pose an immediate problem, but alternative systems and replacements can mitigate this difficulty.

130. John Villasenor, "Ensuring Hardware Cybersecurity," Brookings Institution *Issues in Technology Innovation* No. 9, May 2011, http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity (accessed September 30, 2013).

131. Symantec Corporation, "Advanced Persistent Threats: A Symantec Perspective," White Paper, 2011, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (accessed September 30, 2013).

132. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 18, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed August 8, 2014).

133. Alec Russell, "CIA Plot Led to Huge Blast in Siberian Gas Pipeline," *The Telegraph*, February 28, 2004, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html (accessed July 23, 2014).

134. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed July 23, 2014).

135. One of the most notable examples of large-scale physical damage caused by a cyber attack is the "Aurora" experiment. In 2006, controlled hacking by the Idaho National Laboratory was able to cause a large electrical generator to break. For more information, see CNN, "Staged Cyber Attack Reveals Vulnerability in Power Grid," September 27, 2007, https://www.youtube.com/watch?v=fJyWngDco3g (accessed August 8, 2014); Rid and McBurney, "Cyber-Weapons."