THE AMERICAN FOREIGN POLICY COUNCIL
Defense Technology Program Brief

March 2016 | Washington, D.C. | No. 15

Cyber Threats in the Space Domain

By: Eric Sterner and Jennifer McArdle

Briefing Highlights

Space systems lie at the heart of American military power… Global Positioning System (GPS) satellites are integral into precisely maneuvering military units on a global scale and guiding smart bombs… By 2009, commercial satellites met roughly 96% of U.S. Central Command's bandwidth needs.

• • •

A wide range of ground, sea, and air-based satellite terminals could be compromised with malware, enabling a hacker to remotely access the terminal. Such attacks could enable an attacker to compromise the reliability and accuracy of the data moving through a space system.

• • •

It is unfortunately conceivable that U.S. space assets, especially less shielded commercial systems, have already fallen prey to malicious Russian cyber activity and are rigged with "hidden backdoors" for future sabotage or espionage. As the Kremlin looks to bolster its offensive cyber forces, such insidious threats will continue to rise.

• • •

While China is developing "hard-kill" and "soft-kill" counterspace capabilities, recent Chinese military writings have highlighted a preference for "soft-kill" attacks as they provide greater deniability and potentially fewer diplomatic consequences than "hard-kill" attacks, which may generate orbital debris.

• • •

The implementation of passive and active cyber defenses to mitigate known threats will help ensure the security of space-based and space-enabled systems. The application of layered defenses, network segmentation, firewalls, and aggressive patch management should help ensure that systems are protected against previously identified threats.

Table of Contents

Vulnerability and Threat at the Space-Cyber Nexus

By Eric Sterner

The ability to access and exploit space has long been woven into the fabric of American national power. It is a critical component of global political leadership, the economy, and military power. Unfortunately, those pillars are increasingly at risk. The spread of space technology to new international actors and the increasing sophistication of those capabilities have made it possible to threaten American space systems directly. The national security community is accustomed to analyzing these threats and vulnerabilities and is pursuing a reasonable mix of policies and programs to address them. (Whether those actions are sufficient is subject to debate). However, over the last decade space and cyberspace have grown increasingly integrated. This opens up new vulnerabilities in American space systems, and gives a greater number of actors the potential to exploit those vulnerabilities.

Whereas an adversary might have once needed space capabilities of its own to attack U.S. space systems, an adversary with access to cyber capabilities—

Eric Sterner *is a Washington-based national security analyst and an adjunct faculty member on Missouri State University's Graduate Department of Defense and Strategic Studies. He held senior Congressional staff positions for the House Committees on Armed Services and Science and served in the Department of Defense and NASA.* ***Jennifer McArdle*** *is a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies and a PhD candidate in War Studies at King's College London. She leads a program on simulation and virtual reality for next generation warfare and also serves as a subject matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index Project.*

either indigenous or obtained from third parties—may now be capable of doing so. Addressing this problem requires a holistic approach that treats space systems as vital components of U.S. power, treating all attacks on them, whether kinetic, electromagnetic, or cyber, akin to those on its critical infrastructure.

Space and the National Interest

Space systems sit at the foundation of American power in multiple areas: politics, economics, and national security. Virtually since the dawn of the space age, the United States saw space exploration as an opportunity to promote U.S. global leadership. In 1958, the Eisenhower administration's initial take on space policy (NSC 5814) observed:

> The beginning stages of man's conquest of space have been focused on technology and have been characterized by national competition. The result has been a tendency to equate achievement in outer space with leadership in science, military capability, industrial technology, and with leadership in general… To be strong and bold in space technology will enhance the prestige of the United States among the peoples of the world and create added confidence in U.S. scientific, technological, industrial, and military strength.[1]

To that end, the Administration created the National Aeronautics and Space Administration, NASA, specifically as a civilian agency to promote the peaceful development and use of outer space that would appeal to the world. Today, NASA has cooperative projects with 26 nations, which give it some ability to influence the directions in which those countries take their space activities. Separately, NASA has more than 300 agreements with over 100 countries for cooperative research in exploration, giving those nations an interest in the health and wellbeing of American space capabilities.[2]

This brings us, of course, to another way in which space contributes to American power: economic activity. The Space Foundation estimates that the global space economy reached $330 billion worldwide in 2014, growing roughly 9% over the prior year.[3] (The overall space economy includes government spending). The Foundation determined that some 76% of that global total was commercial activity, although the figure would change depending on one's definition of "commercial." Typically, analysts approach it in the context of spending on space goods, services, and products. These might range from images of earth taken from space and communications time on a satellite to builders of space infrastructure (launch pads, teleports, etc.) and companies seeking to sell services to the government, such as resupply of the International Space Station. However, one should also keep in mind that space applications are today integrated into the terrestrial economy in ways that cannot be fully accounted. For example, the satellites at the heart of the GPS system are, essentially, very precise orbiting clocks. It is possible to determine one's position by referencing the time difference between the signals received from those clocks. But the precise time function itself has economic applications. Banks, for example, use it to time financial transactions. Imagery taken from space, combined with GPS signals, can be used to improve the performance of everything from transportation networks to farming. Those kinds of applications do not generally fall under the definition of space commerce, but they contribute significantly to U.S. economic growth.

To the degree "leadership" in space signifies the strength of a nation's scientific and industrial enterprises, that strength makes its most forceful appearance in U.S. military capabilities, for space systems also lie at the heart of American military power. Satellites have long been integrated in the U.S. nuclear forces. But, over the last few decades, those systems and capabilities have filtered down into more conventional, and even unconventional, military units. Reconnaissance satellites monitor foreign military capabilities and operations, and now are useful in planning specific tactical operations. During the Cold War, Defense Support Program (DSP) satellites watched for the telltale plume of a missile launch to provide early warning and characterization of a threat. They are being replaced with more modern systems looking at space in greater depth and detail. Communications satellites were critical to the global command and control of nuclear forces deployed around the world. Today,

tactical operators can make use of them to reach back to the United States for information and communications support. Unmanned Aerial Vehicle (UAV) operations overseas, for instance, rely on them to connect with their pilots physically located in the United States. Global Positioning System (GPS) satellites are integral into precisely maneuvering military units on a global scale and turned the "dumb" bombs of World War II, Korea, and Vietnam into the smart bombs of the first Persian Gulf War and virtually every American use of force since.

In addition to dedicated government systems, the military increasingly makes use of civilian capabilities to augment those available from government agencies. By and large, these are commercial systems, generally offering communications and remote sensing capabilities to private customers, but which also sell services to government agencies. Prior to Operation Desert Storm in 1991, for example, U.S. military satellites provided some 80% of the total bandwidth used in theater. By 2009, commercial satellites met roughly 96% of U.S. Central Command's bandwidth needs.[4] Today, a mix of government and commercial space systems "underpin DoD capabilities worldwide at every level of engagement, from humanitarian assistance to all levels of combat… [and remain] a cornerstone of our deterrent strategy."[5]

To understand this, it is useful to think about space systems as a pre-deployed global Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C3ISR) network. Military units deployed in the field draw upon these capabilities as they are required and available. Collectively, space systems represent a huge asymmetric advantage for the United States against less advanced adversaries. With that in mind, the Department of Defense recognizes that it must assure those capabilities can deliver service when needed. Thus, in recent years, it has begun to pay more attention to secure space capabilities in the event of conflict, whereas in prior years it focused most closely on developing and deploying new capabilities, often with inadequate regard to their survivability in a high-intensity conflict.

Vulnerabilities

Space systems consist of three main segments: 1) the space elements, 2) associated ground-based tracking, telemetry, command, and control systems, which are the means by which one controls the satellite, and 3) the links in between. Each of these parts is vulnerable to an adversary's effort to deceive, disrupt, deny, degrade, or destroy them, as summarized below:

- *Deception*. Deception measures are designed to mislead the adversary by manipulation, distortion, or falsification of evidence in order to induce it to react in a manner prejudicial to its interests.
- *Disruption.* Disruption results in the temporary impairment (diminished value or strength) of the utility of space systems, usually without physical damage to the space system. These operations include the delaying of critical, perishable operational data to an adversary.
- *Denial.* Denial seeks the temporary elimination (total removal) of the utility of an adversary's space systems, usually without physical damage. This objective can be accomplished by such measures as interrupting electrical power to the space ground nodes or computer centers where data and information are processed and stored. For example, denying US adversaries position navigation information could significantly inhibit their operations.
- *Degradation*. Permanent partial or total impairment of the utility of space systems, usually with physical damage, is the goal of degradation. This option includes attacking the ground, control, or space segment of any targeted space system. All military options, including special operations, conventional warfare, and information warfare, are available for use against space targets.
- *Destruction.* Destruction seeks the permanent elimination of the utility of space systems. This option includes attack of critical ground nodes; destruction of uplink and downlink facilities, electrical power stations, and telecommunications facilities; and attacks against mobile space elements and on-orbit space assets.[6]

There is some overlap in these categories. An attempt to

destroy a space system, for example, might only result in its degradation. An attempt to degrade a capability might inadvertently result in its destruction. Kinetic weapons might be used in both cases. Similarly, electronic jamming of a spacecraft's antennae or communications transponders (or terrestrial receipt of a signal) might result in disruption sufficient to deny use of the system.

Traditionally, analysts have considered the spacecraft the most critical component of a space system. Ground elements can be defended, duplicated, and repaired while certain capabilities to resist interference with the uplinks and downlinks can be built into a system. This is not always the case; the signal of Global Positioning Satellites, for example, can be jammed or spoofed across a wide area on the receiving end. (Researchers demonstrated the ability to affect ship navigation and unmanned aerial vehicle operations by spoofing the GPS signal in 2011 and 2013 respectively).[7] Once launched, however, satellites cannot currently be physically repaired. They tend to be defenseless and are not easily or quickly replaced. Thus, spacecraft constitute an Achilles heel for any space system. As a result, discussions of space security have often focused on preventing and/or defeating attacks on the space-based elements of any space system.

Threats

Anti-satellite weapons can attack from space or from the ground. As vulnerable as satellites are, building weapons capable of attacking them is no simple task. An attacker must first possess the capability to detect and target the spacecraft. (Some information about orbits, particularly of commercial spacecraft, is easily available, but it may not be sufficient to precisely target an object in space).

Following that, the attacker must be able to reach the target. Often, this has meant launching one's own payload into space, which restricted the number of potential threats to those possessing some space launch capability. A limited ability to precisely target a spacecraft can be overcome by using weapons that do damage over a wide area. These would include nuclear weapons that spread their electromagnetic effects across vast distances and a large number of space targets or weapons that contain multiple small projectiles, which are essentially "fired" like a shotgun into a spacecraft's general area or orbital path. Such weapons might be pre-launched into an orbit from which they would attack. The Soviet Union developed one such co-orbital antisatellite weapon (ASAT) during the Cold War. Others might be launched from the ground to attack their targets directly. Additionally, with improvements in laser technology and more powerful radio transmission capabilities, it is increasingly possible to attack a spacecraft with terrestrially-based energy weapons. While lasers or electromagnetic weapons, such as high-power transmitters, may not destroy their targets in a great cataclysmic explosion, such an affect might not be necessary to disrupt, deny, degrade, or destroy a satellite. For example, a laser attack that blinded a reconnaissance satellite's optics would effectively render it incapable of performing its mission. Jamming transponders similarly interrupts the spacecraft's ability to communicate with the ground, effectively disrupting or denying its utility.

Foreign actors generally recognize the values the United States derives from its space systems. According to Director of National Intelligence (DNI) James R. Clapper, "Foreign military leaders understand the unique advantages that space-based systems provide to the United States."[8] As a result, they are actively developing counter-space capabilities. According to Clapper,

> We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation systems. We assess that this technology will continue to proliferate to new actors and that our more advanced adversaries will continue to develop more sophisticated systems in the next few years.[9]

The examples abound. Since 2000, Iran has jammed satellite broadcasts of the Voice of America and domestic receipt of GPS signals; Indonesia has jammed a Chinese-owned satellite; Iran and Turkey have both jammed broadcasts of domestic dissidents; pre-2011 Libya had jammed mobile satellite communications links; and Iran and Cuba had reportedly colluded to jam satellite broadcasts of the Voice of America.[10]

While jamming a satellite is a relatively undemanding task technologically for a nation-state, the threat to U.S. space systems does not end there. Separately, Clapper notes,

> Russia and China continue to pursue weapons systems capable of destroying satellites on orbit, placing U.S. satellites at greater risk in the next few years. China has probably made progress on the antisatellite missile system that it tested in July 2014. The Russian Duma officials recommended in 2013 that Russia resume research and development of an airborne antisatellite missile to 'be able to intercept absolutely everything that flies from space.'[11]

In fact, Russia inherited a basic co-orbital anti-satellite weapon system from the Soviet Union and China publicly tested a very-capable direct-ascent antisatellite weapon in 2007. The most recent Department of Defense report on Chinese military power notes that "China is also focusing on counter-space, offensive cyber operations, and electronic warfare capabilities meant to deny adversaries the advantages of modern, informationized warfare."[12] In 2014, General William Shelton, then the commander of the Air Force Space Command, told an audience at the Atlantic Council that his chief counter space concerns were jammers, lasers, and tactical space nuclear weapons, confirming the gamut of traditional counter-space weapons.[13]

The Space and Cyber Domains Merge

Even as attention focuses on traditional counter-space weapons, such as those mentioned by Clapper and Shelton, the spread and adoption of digital information technologies represents a new development in the vulnerability of space systems. It has been customary to think of space and cyberspace as separate domains, but in recent years the national security community has begun to talk about space and cyberspace in the same breath. Increasingly, the two are mutually dependent and integrated. As the Commander of Air Force Space Command recently noted, "We have not lost sight of the fact that our space systems are intimately integrated into the cyber mission area. All command and control of space-based systems, and delivery of space-based products, are dependent on operations in cyberspace. Space capabilities, such as position, navigation, and timing and weather are essential to kinetic operations and are delivered through cyberspace."[14] That integration, of course, exposes one domain, space, to the vulnerabilities of the other, cyberspace. Bad actors will be quick to exploit the opportunity.

Josh Hartman, the former Director of the Pentagon's Space and Intelligence Capabilities Office, warned in 2011 that "Cyber vulnerabilities pose the No. 1 counter-space threat to our national capabilities." He drew particular attention to the defense community's penchant for focusing on traditional, kinetic-style attacks on spacecraft, noting that this focus risked taking insufficient care of growing cyber vulnerabilities.[15] Hartman's concerns are well founded.

With the convergence of space and cyberspace, in which a space system connects to the Internet, one might not require sophisticated tools in order to attack a space system. Reasonable hacking skills, knowledge of the target, and access to the Internet might be enough. This convergence of space and cyber systems will make it possible for a larger number of actors to attack space systems.

Cyber weapons help overcome that critical challenge of reaching the target. It may no longer be necessary to penetrate defended territory to strike ground elements or develop advanced space surveillance and targeting capabilities or anti-satellite weapons to disrupt, deny, degrade or destroy space-based elements. Instead, one might simply employ advanced computer code that moves through the Internet, to which a number of space systems are connected. For example, one company which does penetration testing found that a wide range of ground, sea, and air-based satellite terminals could be compromised with malware, enabling a hacker to remotely access the terminal. Such attacks may not compromise the operations of the spacecraft, but could enable an attacker to compromise the reliability and accuracy of the data moving through a space system.[16]

The aerospace sector has long been a target of foreign cyber attacks. For example, between 2003 and 2006, western cyber security experts detected a massive espionage campaign that focused heavily, but not exclusively, on Western defense and aerospace firms. Known as Titan Rain, the campaign was generally attributed to China. Information removed included design schematics for aerospace systems, including space propulsion systems, solar paneling, and fuel tanks for civil space missions.[17] Chinese attention to the U.S. aerospace industry did not begin with Titan Rain, nor did it end with it. According to the National Counterintelligence Executive, in 2010 Dongfan Chung, an engineer with Rockwell and Boeing, "who worked on the B-1 bomber, space shuttle, and other projects, [was] sentenced to 15 years in prison for economic espionage on behalf of the Chinese aviation industry."[18] Digitization of the information that Chung stole made it possible for him to exfiltrate some 250,000 sensitive pages from his employers between 1979 and 2006. More recently, one American cyber security company, Mandiant, released a report on a single Chinese cyber unit, which it dubbed APT 1, in 2013. According to Mandiant, "APT 1 targeted numerous companies that provide fixed satellite services, radar and sensor technology, avionics research and other satellite services."[19] APT 1's purposes certainly include espionage.

The computer security firm Crowdstrike identified an advanced persistent threat it dubbed "Putter Panda," connected to the People's Liberation Army's Unit 61398, that was "conducting intelligence-gathering operations targeting the Government, Defense, Research, and Technology sectors in the United States, with specific targeting of the U.S. Defense and European satellite and aerospace industries." According to Crowdstrike researchers, Putter Panda was affiliated with the PLA's primary signals intelligence collection and analysis agency, which also supports China's space surveillance network.[20]

Discovering corporate secrets is an old practice that many actors follow in order to improve their competitive position. But the increasing government reliance on commercial systems may also give an attacker greater information about foreign states and their activities, and constitute reconnaissance against potential targets in a conflict. For example, intrusions into a system, ostensibly for espionage purposes, also leave open the possibility that damage to the target in some other way that may not be readily apparent. Leaving aside possibilities that such damage might reveal itself at an inopportune time, a successful penetration cannot help but undermine confidence in the system. Consequently, an undetected attack may do real damage, but a defeated cyberattack—one whose immediate consequences have been addressed—may nonetheless lead a defender to lose trust in a necessary space system.

Indeed, there is ample evidence that hackers are not just interested in information about, or that which passes through, a space system. They are also interested in compromising space systems themselves. In one instance, cyber security firm Kaspersky determined that a non-state hacker group known as "Turla" had turned its attention from siphoning information out of its espionage targets to hijacking satellite links among command-and-control servers relying on Linux software.[21] Thus, Turla could "cover its tracks" by corrupting feeds to those command-and-control servers—essentially a deception attack. While space systems were not Turla's primary targets, the episode demonstrates how vulnerabilities in a space system make it possible for a cyber actor to exploit a space system through cyberspace for a different purpose. Thus, deceiving a space system was the means to a different end, but required compromise of the space system itself.

The Chinese have made it clear that they believe it both possible and desirable to attack space systems via computer. The future promises to make cyber counter-space attacks a part of conflict. The U.S.-China Economic and Security Review Commission, which reviews Chinese security and trade practices as they relate to the United States, concluded Chinese hackers were likely responsible for several cyber attacks on U.S. government space systems:

- In October 2007 and July 2008, cyber actors attacked the Landsat-7, a remote sensing satellite operated by the U.S. Geological Survey, resulting in 12 or more minutes of interference on each occasion. The attackers did not achieve the ability to command the satellite.

- In June and October 2008, cyber actors attacked the Terra Earth Observation System satellite, a remote sensing satellite operated by NASA, resulting in two or more minutes of interference on the first occasion and nine or more minutes of interference on the second occasion. In both cases, the responsible parties achieved all steps required to command the satellite but did not issue commands.
- In September 2014, cyber actors hacked into the National Oceanographic and Atmospheric Administration's (NOAA) satellite information and weather service systems, which are used by the U.S. military and a host of U.S. government agencies. NOAA stopped the transmission of satellite images to the National Weather Service for two days while it responded to the intrusion and "sealed off data vital to disaster planning, aviation, shipping, and scores of other crucial uses," according to a U.S. media report citing a discussion with NOAA. The U.S. government has not publicly attributed the attack to any country or actors. However, then-Congressman Frank Wolf stated, "NOAA told me it was a hack and it was China."[22]

Other organizations have identified Chinese attackers in a series of operations aimed at NASA and the aerospace industry. The NASA Inspector General, for example, testified in 2012 that in the 2010-2011 timeframe, there were 5,408 computer security incidents at the agency that resulted in the installation of malicious software and unauthorized access to its systems. Those intrusions disrupted mission operations and were conducted by entities ranging from individuals testing their skills, to criminal enterprises, to likely foreign intelligence services.[23]

These purported attacks show a clear evolution in the nature of counter-space activity *occurring today*. Assuming they are attacks by the Chinese government and/or its agents, they demonstrate how attackers have moved from developing kinetic-style and electromagnetic weapons to cyber weapons.

Implications

As counter-space weapons, cyber weapons have several advantages and disadvantages compared to kinetic or electromagnetic weapons. Only a handful of states can afford to develop some counter-space capabilities, such as co-orbital or direct-ascent ASATs. A somewhat larger number has access to electromagnetic weapons, such as jammers. But an immense number of actors may have access to cyber weapons; they may only require certain coding skills and access to the Internet.

It also can be more difficult to attribute cyber attacks to a specific attacker, particularly given the large number of potential attackers. American satellites continually scan the surface of the earth for signs of missile or rocket launch, while other systems scan earth orbit to track and monitor objects in space. Electromagnetic attacks on a satellite can also usually be attributed to a particular source; they require a satellite dish capable of radiating a sufficient amount of energy to affect the target. Such sources of radiation can generally be detected. Thus, we may be able to deter such attacks by possessing the capability to retaliate and credibly threatening to do so. (The problem is more challenging for the United States when potential adversaries seek to jam communication links, especially low-power links like the GPS signal, across a wide area.)

Knowing an adversary's identity and the general nature of an attack may also make it easier to defend against, or minimize the effects of, an attack. For example, satellites can be maneuvered away from potential threats in many cases. ASAT weapons may, ideally, be engaged themselves on their route to a target. Missile defenses, for example, may be able to shoot down space launch vehicles that appear to be placing weapons in orbit, at least in wartime. Electromagnetic weapons can be struck at their source. In any event, deterrence and defense require attribution, which is one reason the Department of Defense places such a high premium on improving its space surveillance and situational awareness capabilities for space systems.

Cyber attacks present a different problem for the defender; the challenges of attributing them to a specific attacker in particular are very high. Bits, the zeroes and ones that constitute digital data, have no nationality, unlike rockets

and spacecraft. Even if forensic investigation—which often occurs after-the-fact, when it is too late to counter an attack—identifies the source of an attack, such as a particular address on the Internet, it cannot readily identify the nature of the attacker. Are the people that are writing the computer code and employing it hackers? Are they criminals? Or spies? Military units? Or are they rogue actors in a state's security apparatus? In all likelihood, cyber attacks on space systems will involve considerable ambiguity about the attacker and his intentions. That ambiguity, in turn, may make it more difficult for a defender to decide how to respond.

This may give cyber weapons greater appeal than their traditional counterparts in some circumstances, and give a potential attacker a greater number of attack options. A state might choose to use them in the hope or expectation that it can escape attribution entirely, or at least in the belief that the defender's confidence in attribution is so weak as to preclude it from retaliating. Ambiguity about the attacker and/or the nature and purpose of an attack may also enable an attacker to misdirect or confuse a defender while still degrading capabilities. Conversely, ambiguity may not serve an attacker's interests if it seeks to send clear signals. Certainly, cyber weapons provide more options to an attacker and appear to create new avenues of conflict short of crossing an imaginary kinetic redline. This may have a destabilizing affect by leading states to believe they can launch disproportionately effective attacks on space systems with less fear of escalating to a full-blown conflict.

Cyber weapons are often employed stealthily. A defender may not even be aware that it is under cyber attack until the attacker triggers an anomaly. This makes it extraordinarily difficult to characterize an attack or defend against one that is already underway in a timeframe useful to a defender.

Nevertheless, cyber weapons also have certain disadvantages. For a given cyber weapon to work, it must exploit a specific vulnerability in a particular piece of software. Contemporary space systems do not use identical software. Therefore, vulnerabilities to a particular cyber weapon will not be uniform across all space systems. (This may change as space systems trend away from custom software design and towards common software systems or use outdated commercial-off-the-shelf software in order to save money.) Moreover, the vulnerabilities in a space system's software can often be eliminated almost as quickly as they are discovered through periodic software updates. Thus, a cyber weapon is often referred to as "perishable," while the target may be constantly changing. One cannot assemble an arsenal and expect it to be available at will in the future. As a result, the interaction of offense and defense is nearly constant as attackers seek to ensure their weapons retain some capability and must continually conduct cyber reconnaissance of their targets in order to develop new weapons. This is not the case for more traditional counter-space weapons.

Finally, if a cyber attack does no physical damage, it may be possible to "repair" the damage it causes by restoring backed up copies of affected software, developing "work-arounds" for corrupted code, or even developing and installing entirely new software. Thus, while the convergence of space and cyberspace opens up new vulnerabilities in U.S. space systems and increases the number of potential attackers by putting counter-space capabilities in wider hands, the cyber threat is not necessarily the ultimate counter-space weapon that some might fear. Nevertheless, this does not make it any less urgent to address the problem, because the number of potential threats is going to continue to grow at an accelerating rate.

Policy at the Space-Cyberspace Nexus

This cursory examination of space and cyberspace highlights several challenges in U.S. national security. First, the United States depends on space as a critical element in its soft power, economic power, and military power. Second, because space systems are so widely integrated into all three areas, they represent an Achilles heel that potential adversaries might seek to attack for disproportionate gain. Third, established adversaries are aware of this and have actively developed counter-space capabilities for years. Some have even employed them to disrupt space systems. Fourth, the space and cyberspace domains are merging, creating new vulnerabilities in space systems. Worse, because cyber weapons are

more accessible to a wider number of actors, the merger of these two domains will also increase the number of counter-space threats with which the United States must contend. These actors are already shifting from espionage against space-related organizations to interference with space systems themselves. Fifth, cyber weapons in a counter-space role have both advantages and disadvantages compared to their more traditional kinetic or electromagnetic cousins.

The question, of course, is what to do about this new vulnerability. The place to start is, of course, to improve cyber security in space systems. Some in the space community are beginning to acknowledge this need. In 2015, for example, the World Teleport Association issued a report concluding that many in the satellite industry were ill-prepared to deal with cyber attacks.[24] WTA's report highlights increased attention in industry to the problem. Some government space system modernization programs also include additional cyber defense tools. The next generation GPS Operational Control System (OCS), for example, is designed to include some capability to identify and isolate cyber intrusions.[25] Yet the government remains largely focused on traditional counter-space threats, as described by General Shelton in 2014 and DNI Clapper in 2016.

That problem, it should be noted, is not unique in the United States. One analyst writing shortly after the NOAA attacks found a similar lack of urgency about the cyber vulnerabilities in British space systems.[26]

In truth, focusing too narrowly on improving cyber security in space systems would prove inadequate. Because those systems depend on cyberspace at large, they will always be vulnerable to weaknesses in cyberspace. Simply put, they are unlikely to be fully segregated from that domain, if only because the commercial providers upon which the government relies cannot afford to forego the connection. A more holistic approach is needed. The Defense Department's 2015 *Cyber Strategy* offers some insight into how this might be done. It acknowledges that a perfect defense is unlikely and announces an intention "to identify, prioritize, and defend its most vital networks and data so that it can carry out its missions effectively."[27] Because they are critical in so many areas, commercial and government space systems should be high on the list of priorities. In the process of setting its priorities, the Defense Department should consider the non-defense importance of space to American power overall. This may put the Department in the awkward position of more closely committing to defend civilian networks, but the strategy acknowledges a need to work with the private sector.[28] There is no other choice given the integration of the space and cyber domains.

As mentioned earlier, the Department of Defense recognizes the inevitability of attack on the space systems on which it depends. It therefore is seeking to develop a space architecture that is more robust and can continue to operate in a degraded environment.[29] Several concepts present themselves in this regard: disaggregation, hosted payloads, on-board satellite protection, defensive operations, and leveraging commercial capabilities. To these, the Air Force should add the ability to restore and reconstitute software operating systems and other basic concepts from the realm of cyberspace. This will be critical, as commercial systems tend to be less secure than government space systems. Making greater use of the former will require increased attention to securing information that flows across the space and cyber domains. It likewise will be critical to ensure these kinds of capabilities are included in non-military systems, perhaps by subsidizing their affordable development in the private sector and requiring them in government contracts.

When it comes to the security of space systems themselves, a holistic policy approach would treat them less as specific platforms and networks to be defended, and more as part of the country's critical infrastructure. They cannot be defended simply as tactical targets, but must be considered strategic assets. This means elevating their political importance, such that an attack on them—by any means—would be viewed the same as an attack on critical infrastructure or the nation's strategic nuclear forces. Because they provide an asymmetric advantage and represent an asymmetric vulnerability, space systems should be viewed as disproportionately

important assets.

For years, U.S. national space policies have declared that the United States considers the "sustainability, stability, and free access to, and use of, space vital to its national interests," or words to that effect.[30] Yet history raises questions about the sincerity of those statements. The United States has taken little action to impose any meaningful costs on state actors that interfere with its space systems, suggesting that the United States may not view those systems as such a vital national interest after all.

At his confirmation hearings to become Chairman of the Joint Chiefs of Staff, General James Dunford acknowledged that the protection of space assets and space situational awareness did not have the appropriate level of national security priority and needed more attention.[31] The merger of the space and cyber domains only exacerbates the need, not just to pay closer attention to the space mission, but to demonstrate the seriousness with which the United States views attacks on its space infrastructure, regardless of the means used.

An Assessment of Russian and Chinese Offensive Cyber Operations on U.S. Space Assets

By Jennifer McArdle

> *"Control of space means control of the world." – Senator Lyndon B. Johnson, 1958.*

At the height of the Cold War, when the United States and the Soviet Union lived under the shadow of mutually assured destruction, space emerged as a key competitive arena.[1] Indeed, attacks on space systems were perceived as potentially highly escalatory—running the risk of crossing the threshold from a limited conflict to a war between nuclear armed super powers. In large part due to the mutual fragility of U.S. and Soviet Union space-based architectures, there was reticence in some quarters to overly militarize space for fear of injecting a greater degree of instability into the already-fraught global environment.[2]

However, since the collapse of the Soviet Union, a paradigmatic shift has taken place in space. Space assets are no longer considered "unfair game" for fear of escalation. As the former head of U.S. Air Force Space Command, General William Shelton, has stated, space had "been kind of [a] peaceful sanctuary. It is not anymore."[3] Offensive cyber capabilities have allowed conflict to penetrate the exoatmosphere—linking space-based and cyber-assets—without raising the specter of immediate escalation to nuclear war. Meanwhile, cyberspace has blurred the lines between traditional conflict and peace, and states are finding themselves in a state of protracted, low-level conflict in the cyber, and increasingly space, domains.[5] The result is a host of new dangers to U.S. space-based and space-enabling assets.

The Achilles' Heel of U.S. Military and Economic Space Dependency

The 1991 Persian Gulf War—designated by some as the "first space war"—marked the beginning of the near real-time integration of orbital systems into U.S. military operations.[5] Ever since, U.S. weapons platforms have become increasingly dependent on space for their operational effectiveness: precision guided munitions, combat platforms, and missile defense systems, all rely on satellites for targeting and tracking information. Space enables vital intelligence, surveillance, and reconnaissance (ISR) capabilities, providing information that subsequently informs U.S. military force posture and planning.[6] Space assets also provide the bedrock of military connectivity, allowing the U.S. military seamless global communications, regardless of fiber-optic network connectivity and thus reducing the forward deployed footprint of critical information resources.[7]

Yet it is not just the military that has developed a dependency on space-based and space-enabled assets. Space—and its interlinkages to cyberspace—has emerged as

a key enabler for U.S. economic growth. Information communications technology (ICT) is estimated to account for between 9.3% and 19% of U.S. economic gross output growth.[8] Moreover, it is estimated that for every dollar invested in broadband (fixed and wireless), the U.S. economy can expect to see a tenfold return.[9] While these numbers are not exclusive to space-based assets, space—in particular satellites—does play a key role in ICT driven productivity. Indeed, terrestrial network infrastructure is subject to physical limitations, and in some cases cannot meet the requirements of various network activities. Satellites help fill gaps in connectivity and increase network efficiency.[10] At present, about 1,300 active satellites orbit the globe providing worldwide communications and Internet access, navigation, weather forecasting, planetary surveillance, emergency and industrial services, among any number of other activities. Satellites have become a crucial component of economic growth, and investment in the satellite market has rapidly increased. Over the past decade, the global satellite industry's growth has thus increased by about 230%, placing the market value in 2014 at $203 billion. The U.S. market share of the industry is estimated at 43%, or $87.2 billion.[11]

But U.S. dependence on space assets has engendered immense vulnerability. Indeed, space has emerged as a proverbial Achilles' Heel for U.S. economic and national security. The sudden loss of space assets in times of war could prove devastating. As Lt. General Yvan Blondin (retd.), former Commander of the Royal Canadian Air Force (RCAF), mentioned to this author in reference to future air campaigns,

> the loss of satellites would, in the short term, be completely paralyzing to any coalition air war effort, and severely hamper any long term effort to operate effectively in a forward deployment mode.[12]

If that is not sufficient cause for alarm, others have noted that the loss of satellites would entirely disrupt our "current mode of technological existence" in the short-medium- and long-term; entirely wiping various users (particularly those in remote locations) off-line, oversaturating terrestrial connections, disconnecting cellphone connections, and decimating our geo-location and weather forecasting abilities, among other activities. In essence, as futurist Peter Singer has described, it would boot us back to a "pre-digital age."[13]

Cyber Vectors of Attack on Space Systems

Cyberspace and space share a common architecture through mutual networks, systems, and infrastructure. For that reason, space systems are not simply vulnerable to cyber attacks *in* space; every connecting node is a vector for a potential cyber attack. Cyber attacks can target satellites, ground stations, terminals, and end-users. A successful cyber attack in any one vector could be used to launch additional cyber attacks elsewhere. Moreover, given the sheer scale of organizations involved in space programs—universities, contractors, governments agencies, and commercial industry—securing all potential avenues for an offensive space cyber attack is no easy task. As U.S. Air Force Lt. General Brian Arnold (retd.) noted several years ago,

> If you look at things like command and control, [or] on-orbit stationing of assets, you then have to look at the up-link, the down-link, and the ground control station, and then the various nodes that extend out from that… each one requires in-depth cyber protection.[14]

For this reason, cyber security experts have advocated for a systems level, whole of architecture approach to space cyber security.[15]

Cyber attacks to space systems can take many forms. Malicious actors could use jamming devices to overpower satellite signals, degrading communications or rendering them obsolete for a short period of time. Likewise, perpetrators could also subsequently "spoof" satellites into tracking counterfeit GPS signals, causing the satellite to lose its ability to provide accurate geo-location data. Software, hardware, or firmware destined for space systems can be nefariously modified during the design, development, or fabrication phase, later operating as hidden "back doors" in space systems for espionage or sabotage.[16] Counterfeit microelectronics or metals in the global supply chain can find their way into space systems, dramatically decreasing the projected

lifespan of a satellite. Likewise, system upgrades, insider threats, insecure protocols, undocumented protocols, unencrypted data links, and weak password resets all also provide opportunities for subsequent cyber attacks.

Cyber attacks on space-based or space-enabled systems can be exploited for the purposes of espionage, sabotage, or deception. For example, an adversary could gain access to a space system for the purposes of monitoring communication flows or gaining valuable intelligence on sensitive tactical or operational details, such as the capabilities of highly classified weapons platforms or future operational battle plans. More sophisticated attacks could render a satellite defunct or intentionally corrupt the data as its flows through a communication system. The effects of these attacks on U.S. commercial or military satellites could range from local disruptions (for example, the loss of connectivity to a single communication terminal) to much broader and long-lasting losses of communications and connectivity.[17]

Recent history is replete with examples of reported cyber incidents on space assets. In November 2014, a U.S. weather satellite suffered an electronic attack, which resulted in unscheduled maintenance of U.S. National Oceanic and Atmosphere Administration (NOAA) data feed for weather forecasts.[18] In 2011, IntelsatONE, the terrestrial network that connects users to Intelsat's geosynchronous satellites, suffered upwards of 300,000 distributed denial-of-service (DDoS) attacks. In 2007 and 2008, at least four instances of cyber attacks against U.S. government satellites occurred. The more successful of these was against a National Aeronautics and Space Agency (NASA) Terra EOS satellite, and resulted in the perpetrator achieving all required steps to take command of the satellite.[19] In 2009, it was discovered that Iraqi and Afghani insurgents were intercepting live video feeds from U.S. Predator unmanned surveillance aircraft, providing them with the opportunity to evade U.S. targeting or gain useful insight into U.S. military operations. Given that the video feeds were transmitted without encryption, insurgents were able to use $26 commercial-off-the-shelf software to intercept the data.[20]

Yet despite the successful cyber attacks on Terra and other space systems, Bob Vargo, Assistant Director in the Engineering and Space Directorate of NASA's Jet Propulsion Laboratory, has noted that the space community remains in "blissful ignorance" of cyber security for space systems.[21] Cyber security for space assets, particularly commercial space assets, remains woefully under addressed.

U.S. Rivals and the Cyber Threat to U.S. Space Systems

While the peaceful use, and non-weaponization, of outer space has been presented as U.S. policy, U.S. military space systems are perceived by other nations as one of the core technological underpinnings of American primacy. It is only natural that space is increasingly viewed as a domain open to military contestation. As Todd Harrison has noted,

> arguing that military space systems are not weapons is like arguing that the M-16 rifle is not a weapon but merely an enabling capability for the ammunition. Such arguments obscure the military utility of space and the attractive set of targets it presents for potential adversaries.[22]

America's dependence on space-based systems for its economic stability and global military power projection means that counterspace activities will likely figure prominently in the military strategies and operational concepts of U.S. adversaries. Not only could attacks on U.S. space-based capabilities cripple the lethality of U.S. military forces, but attacks on commercial satellites could also raise the economic costs of conflict, with potentially debilitating effects on the morale of the U.S. populace.

From Ukraine to the South China Sea, Moscow and Beijing have been attempting to resurrect age-old spheres of influence, and challenging the existing global order. Both states have become increasingly revisionist and assertive towards their neighbors. They have manifested a predilection for "gray zone" approaches—testing U.S. security commitments and platforms through "salami slicing" or probing tactics that do not in and of themselves amount to a *casus belli*, but nevertheless threaten to create *faits accomplis*.[23] Cyber reconnaissance and attack operations form key aspects of these revisionist

approaches to great power competition. And by virtue of technological connectivity, this competition is now taking place above and over the earth. In short, U.S. spatial architecture is not immune from "gray zone" encroachments.

While the goal of such "gray zone" tactics is to recast geopolitical power dynamics in a gradualist fashion, creeping coercion can occasionally prove dangerously escalatory. Both powers may seek to avoid high-end great power conflict, but—like all states—nevertheless find themselves compelled to prepare for a conventional conflict. It is with this eventuality in mind that both states have actively sought to attain greater space parity with the U.S. Indeed, both Russia and China have ambitious space and counterspace programs of their own.[24] As each country positions more assets in space for communications, reconnaissance, surveillance, or geo-location, their economies and militaries will also become increasingly dependent and at risk. Therefore, while Moscow and Beijing have tested and experimented with the use of certain counterspace capabilities, such as kinetic anti-satellite weapon systems (ASATs), their appeal could hypothetically decrease. In the near- to mid-future, a form of mutual space vulnerability may well emerge that could change the strategic calculus of both states: the use of a kinetic ASAT risks the potential of collision cascading, setting off a torrent of orbital debris that could cause equal, if not greater, damage to Chinese or Russian space constellations.

Cyber attacks on space assets, then, may hold greater appeal for two distinct reasons: not only do they allow challengers to engage in espionage, reconnaissance, sabotage, or deception against the U.S. during peacetime without risking potential vertical or horizontal escalation,[25] but it also allows them to preserve the physical integrity of the space domain—a domain that is becoming increasingly important for their own economic and military advantage.

Cyber Counterspace Operations: The View from Moscow

In recent testimony before the Strategic Forces Subcommittee of the House Armed Services Committee, Lieutenant General David Buck, commander of the Joint Functional Component for Space in U.S. Strategic Command, noted that

> Russia views U.S. dependency on space as an exploitable vulnerability and they are taking deliberate actions to strengthen their counterspace capabilities.[26]

While Russian officials have highlighted the country's accomplishments in ASAT technology,[27] little has been said of its ability to use cyber as a means of attacking space assets—both ground-based and orbital. In order to accurately gauge the mechanisms by which Moscow could employ cyber attacks on U.S. space assets, it is necessary to examine Russia's integration of cyber into their national security architecture from a doctrinal and operational perspective.

An Assessment of Russia's Cyber Doctrine

From a doctrinal level, the Kremlin does not limit the use of cyber attacks to traditional "wartime" hostilities. Russia's use of the cyber domain allows it to actively shape its geopolitical environment, particularly in its near abroad, during times of relative "peace." Indeed, as one Russian officer has noted,

> there is no need to declare war against one's enemies and to actually unleash… military operations using traditional means of armed struggle. This makes plans for "hidden war" considerably more workable and erodes the boundaries of organized violence, which is becoming more acceptable.[28]

As part of the Kremlin's ongoing "hidden war," Russians have displayed a penchant for a concept known as "reflexive control"—a process by which Russia seeks to manipulate and deceive an adversary into reaching an independent decision unfavorable to itself, but advantageous to Moscow. Reflexive control consists of two layers. The first embodies the "eyes, nose, and ears" (or sensors, satellites, and radars)—the technology that allows a state to gather data and information. The second layer, for its part, includes what Timothy Thomas calls the "brain software": the human processing pow-

er upon which state-level and public decision making takes place.[29] Manipulation of the first layer can often cause erroneous or problematic decisionmaking at the second layer, much as Yugoslav tactical deception of NATO forces demonstrated in the Balkans in 1999. It is entirely plausible that Moscow could employ such "reflexive control" techniques against U.S. commercial and governmental space assets, altering data and information in order to mislead U.S. political and military decision-makers and the public.

Yet, peacetime cyber operations extend beyond deception and "reflexive control" techniques. Russian analyst V.I. Tsymbal has noted that the goal of cyber operations in times of relative peace is to conduct adversary espionage and reconnaissance while covertly testing one's own cyber weapons.[30] It is likely that Moscow uses peacetime cyber operations to conduct reconnaissance of U.S. space assets, probing for cyber vulnerabilities across all potential attack vectors from ground control stations, to satellites, and end users. As part of this reconnaissance, Russia could also be covertly planting "combat viruses and other information-related weapons" that could be activated just prior to hostilities in order to gain space and information dominance, while damaging and/or crippling U.S. space-enabled reconnaissance strike complexes.[31] Both the 2010 and 2014 versions of Russia's Military Doctrine point to thinking along such lines.

Indeed, Moscow's *2010 Military Doctrine* notes the importance of information warfare during the initial phases of conflict to weaken the command and control ability of the opponent.[32] The 2014 edition thereafter highlights Russia's development of cyber warfare capabilities for both offensive and defensive purposes.[33] Moreover, according to the Russian media, the country's leadership plans to release a new *Information Security Doctrine* in 2016, which allegedly will propose to develop a specific force structure optimized for information warfare.[34] It is unfortunately conceivable that U.S. space assets, especially less shielded commercial systems, have already fallen prey to malicious Russian cyber activity and are rigged with "hidden backdoors" for future sabotage or espionage. As the Kremlin looks to bolster its offensive cyber forces, such insidious threats will continue to rise.

Operationalizing Cyber: What Can We Learn from Russia's Past Cyber Attacks?

While no evidence yet exists in the open domain of a Russian government sanctioned cyber attack on space assets, Moscow has consistently demonstrated its willingness to to use cyber attacks for political ends. Prior use of cyber attacks by the Kremlin, or its nebulous cloud of proxies, may be indicative of the mechanisms by which Russia may attack U.S. space assets in the future.

The 2007 and 2008 cyber attacks on Estonia and Georgia, were perpetrated by nationalist netizens utilizing botnets and DDoS attacks. The attacks were meant to coerce country-level decision makers into action favorable to Moscow, cause havoc, or act as force multipliers in conflict. While the attacks have not been directly attributed to the Kremlin, in the case of Georgia, an open-source intellectual initiative called Project Grey Goose was able to point to its potential culpability. Project Grey Goose was thus able to trace the origination of the attacks to two Russian hacker forums: stopgeorgia.ru and xakep.ru.[35] The stopgeorgia.ru website's Internet Protocol (IP) address was linked to a hosting firm called Steadyhost, whose offices are believed to be located in the same building as the Russian Ministry of Defense Institute and the Russian Center for Research of Military Strength of Foreign Countries.[36] In both cases, independent analysis confirmed that the attacks were carried out by well organized bodies of individuals with access to key features of command and control—attributes that often require financial and intellectual resources. Estonia and Georgia set the precedent for cyber proxy warfare. It provided the Kremlin with a degree of plausible deniability, while engaging in aggression against neighboring nations. It is likely that if "hidden cyberwarfare" is ongoing against U.S. space-based or space-enabled assets, it is being carried out by patriotic hackers or criminal groups—agents acting on behalf of the Kremlin without the onus of government accountability.

In Ukraine, the Kremlin has actively engaged in a campaign of social engineering, electronic jamming, and reconnaissance for cyber espionage and sabotage.

Moscow combined the use of cyber and information operations with "little green men" in order to annex Crimea. This combination of tactics allowed the Kremlin to manipulate ambiguity, and uncertainty in order to more rapidly create a *fait accompli* on the ground. Of particular note is Russia's use of cyber reconnaissance for espionage and sabotage. Ukraine private sector reports have highlighted the presence of Russia-based advanced persistent threat (APT) cyber espionage tools in Ukraine and North America Treaty Organization (NATO) member states.[37] Furthermore, cybersecurity company Kaspersky has noted that a Russian group of hackers, most likely Turla APT, has been hijacking satellites to mask its command and control operations. While not exclusively focused on Ukraine, the group has been abusing satellite-based Internet connections to siphon off sensitive data from government, military, and academic institutions.[38] It is plausible that these groups are feeding intelligence back to the Kremlin. Moreover, Sandworm Team, a known group of Russian government supported hackers, have reportedly targeted supervisory control and data acquisition (SCADA) equipment, which is used in critical infrastructure settings, with the BlackEnergy toolkit.[39] The victims of the intrusive reconnaissance were production systems, and there would appear to be no immediate, tangible, espionage benefit to targeting the equipment. The attackers were probably scouting for potential weaknesses to exploit in the future.[40] The effects of this type of cyber reconnaissance brutally came to light in January 2016, when a series of coordinated cyber attacks devastated a Ukrainian power grid, causing 225,000 people in Ukraine to be plunged into darkness.[41]

Similar tactics are likely used by the Kremlin, or Russian backed hacker groups, to identify weaknesses in U.S. space assets—both ground and orbital—for espionage or sabotage.

Cyber Warfare in Space with Chinese Characteristics

As far back as 2000, Chinese military analyst Wang Huacheng described the U.S. reliance on ICT and space as its "soft ribs" and a source of "strategic weakness."[42] Under that premise, Beijing has been actively working to develop space and counterspace technologies "to achieve control of low earth orbit in order to defeat the United States on earth."[43] While China is developing "hard-kill" and "soft-kill" counterspace capabilities, recent Chinese military writings have highlighted a preference for "soft-kill" attacks as they provide greater deniability and potentially fewer diplomatic consequences than "hard-kill" attacks, which may generate orbital debris.[44] Given Beijing's well-known penchant for aggressive cyber espionage, it is likely that China will employ cyber as a means to attack U.S. space assets.[45] In order to assess the means by which China—and the People's Liberation Army (PLA)—may employ cyber attacks on U.S. space assets, it is necessary to examine China's integration of cyber into its national security apparatus from both a doctrinal and operational perspective.

The Impact of China's Cyber 'Doctrine' on U.S. Space Assets

China has never officially endorsed a cyber war doctrine. However, it has released official documents that provide some degree of guidance on its conceptualization of the use of cyber attacks for defense policy. In addition to their longstanding concept of waging local wars under informatized condition, China's latest *Defense White Paper* notes that, "Outer space and cyber space have become new commanding heights in strategic competition among all parties."[46] Moreover, one can begin to glean Chinese operational thinking on the use of cyber weapons through various authoritative publications by PLA members.

In 1999, Liberation Army (PLA) colonels Qiao Ling and Wang Xiangsui published a seminal work entitled *Unrestricted Warfare* which argued that modern warfare transcends the "material" of the military domain and includes information, economic and psychological operations.[47] Moreover, unrestricted warfare was not simply a strategy to be operationalized at the onset of active hostilities; it could also be used in peacetime as a subcomponent of a strategy for long-term competition with the United States and other Western countries.[48] PLA Major General Peng Hongqi encouraged the use of "active offense" in peacetime, to provide the weaker power (i.e., China) the ability to deprive a stronger

adversary of the use of information, to include space systems, networked systems, and logistics systems. As part of an "active offense" strategy, Peng believes that the inferior power should conduct information reconnaissance for espionage or sabotage and prepare for confrontation.[49] In line with this thinking, China could be engaging in offensive reconnaissance of U.S. space assets—both terrestrial and orbital. As part of this process, Chinese hackers could be scouring networks for vulnerabilities, siphoning off data, implanting malware or corrupting software to disable space systems at a later time that may be advantageous to Beijing. The attacks in 2007 and 2008, largely attributed to the Chinese, on the Terra EOS earth observation system satellite and the Landsat-7 satellite may be early indicators of this sort of future disruptive attacks.[50]

If such reconnaissance is ongoing, it is likely being done surreptitiously, through hackers or other means. As Peng notes, this would enhance the PLA's plausible deniability if accused of being part of an attack.[51] The 2013 *Science of Military Strategy*, an authoritative PLA publication from the Academy of Military Sciences, highlights the need for a 'whole of nation" approach to conducting cyber war, that includes "external entities" outside the public sector "that can be organized and mobilized for network operations"—an allusion to private sector and patriotic hackers.[52] Previously, the PLA had developed a competition for hackers, the Network Crack Program Hacker group initiative (NCPH), and the winner would receive a monthly stipend from the military.[53] A U.S. branch of VeriSign has accused the NCPH of implanting Trojans on U.S. government agency networks and stealing thousands of unclassified U.S. documents.[54] The use of patriotic hackers may be the Chinese "People's war" of the digital age.

Moreover, the PLA has also examined the means by which deception could be employed on the "digital battlefield." It should be expected that PLA units are prepared to tamper with the order, geo-location, time, flow, and content of information in order to sow confusion.[55] As Lieutenant Colonel Liu Aimin, a staff officer in the General Staff department of the PLA, has stated in reference to the insertion of synthetic information into an enemy's command and control system, the goal is to cause the enemy to conflate fiction and reality, propagating chaos in enemy decision-making.[56] It is likely that Chinese strategists may advocate for the insertion or deletion of information in space assets, helping to fuel the fog of war and generating questions of information integrity.

In the event of conflict against the U.S., the Chinese believe that they must seize "battlefield information dominance" through a blinding first strike.[57] The decisive victory of the United States over Saddam Hussein's regime in Iraq in 1991 was a turning point in Chinese strategic thought. Operation Desert Storm seemed to herald a new era, as it suggested to some that countries which successfully leveraged ICT and space would rapidly acquire overwhelming military superiority. While Beijing ultimately seeks technological symmetry with the U.S., for now preemption provides the PLA a means of countering U.S. information advantages.[58] The *Science of Strategy* advocates a preemptive first strike of information and support systems, followed by weapons systems, ground information facilities, transmission means, and information flow capabilities. The aim of such attacks would be to paralyze the U.S. military and the American will to fight, and "take away the firewood from under the cauldron."[59]

Operationalizing Cyber: What Can We Learn from China's Past Cyber Attacks?

Unlike Russia, China has not been engaged in open hostilities since 1979. Therefore, it is impossible to operationally assess how China may use cyber as a force multiplier in the event of conventional conflict. However, Beijing or PLA proxies have been engaged in a string of cyber espionage incidents that do provide some insight into how China may use cyber weapons to attack U.S. space assets. Furthermore, recent structural reforms to the PLA are also indicative of the primacy that Chinese leadership places on cyber and space operations for future warfare.

Operation Aurora, subsequently attributed to the Chinese, was a six-month penetration of corporate infrastructure in 2009, resulting in the theft of corporate data. During the Aurora campaign, Google, Hotmail, Yahoo,

and Microsoft disclosed that hundreds of its users had fallen victim to spear phishing operations, in which its users had been individually targeted via email and mistakenly downloaded malicious attachments, which in some cases were armed with zero day exploits.[60] Similar to Operation Aurora cyber tactics, a two-year long APT penetration entitled Gh0stNet saw attackers use spear phishing and social engineering to steal data from target systems belonging to the Office of His Holiness the Dali Lama, the Tibetan Government in exile, and affiliated organizations. While the command and control infrastructure of Gh0stNet was located in China, there is no conclusive evidence that the Chinese government was involved. However, researchers at the *Information Warfare Monitor* note that some of the documents appear significant to Sino-Tibetan negotiations, raising suspicion that Beijing or a proxy was involved.[61] Considering how effective a tool spear phishing has been for China and its proxies, it is likely such a tool could be used to gain access into U.S. space assets. Indeed, the sheer number of organizations that are involved in space operations, provide multiple nodes of attack.

Titan Rain was another series of cyber espionage incidents traced broadly to China, which ran from 2003 to 2006 and targeted a diverse list of organizations related to the U.S. federal government, including the Defense Information Systems Agency (DISA), Sandia National Laboratories, the World Bank, Lockheed Martin, and NASA.[62] The attackers were well organized and carried out extensive cyber reconnaissance, using malware to infiltrate target systems for subsequent data exfiltration. While, to our knowledge, Titan Rain was a cyber espionage campaign, the European Union has noted, it is impossible to know whether an intrusion is for espionage or sabotage: "Technically speaking, computer network attack requires computer network espionage to be effective. In other words, what may be preparations for cyberwarfare can well be cyber espionage initially or simply be disguised as such."[63] Chinese penetration of target networks could be reconnaissance missions with the aim of intelligence collection, but they also could be used to spot vulnerabilities and plant logic bombs that could be activated at a future time. As one Chinese proverbs notes, "a victorious army first wins and seeks battle. A defeated army first battles and then seeks victory."[64] The use of reconnaissance to set the stage for a future blinding first strike enables the Chinese to win without fighting.

This past December, President Xi Jinping instituted sweeping reforms of the PLA, restructuring the military services.[65] The Chinese are well aware that the ability of the U.S. to project power into the Asia-Pacific is built on unfettered access to ICT and space. As part of the reforms, China fused its space warfare and cyber warfare units into a new branch entitled the Strategic Support Forces, which is now entrusted with all space, electronic, and network warfare capabilities.[66] This suggests that, on a certain conceptual level, China may be ahead of the U.S., as the Chinese have explicitly linked cyber, space, and electronic operations.

Recommendations

Cyberspace and space are bound within a common architecture through mutual networks, systems, and infrastructure. Space systems, therefore, are not simply vulnerable to cyber attacks in space; rather, every connecting node is a vector for a potential cyber attack. For this reason, space assets require an end-to-end approach to risk management and resilience, whereby every node that is connected to a space system is secured. Preventing cyber attacks requires more than just strong cybersecurity. The U.S. government and commercial space stakeholders can take advantage of Russian and Chinese fears of escalation in order to dissuade future intrusions. The following are four basic recommendations, that should help prevent and/or mitigate potential Russian or Chinese cyber attacks:

1. *Cyber Awareness:* Every space stakeholder, from satellite assembly to the ground-based crew and the end user, must know his or her respective cybersecurity responsibilities. Indeed, as Chinese spear phishing attacks have demonstrated, humans are often the weakest link in cybersecurity. Each person involved with a U.S. space system—commercial or government—should be trained on potential cybersecurity risks. This applies particularly to the commercial cadre of space stakeholders, whose instinct may be to sideline effective cybersecurity risk man-

agement approaches (or to apply minimal efforts) in favor of cutting costs.[67]

2. *Data Encryption*: A basic shielding mechanism against cyber intrusions is to encrypt the signals for tracking and controlling satellites and all data sent to and from space assets. By transforming ordinary data, or plaintext, into code form and then subsequently back into plaintext via an algorithm, encryption can hide the content of the information, prevent undetected modification, and prevent unauthorized use. Moreover, different levels of encryption can be applied based on the sensitivity of the information or mission.
3. *Passive and Active Cyber Defense*: The implementation of passive and active cyber defenses to mitigate known threats will help ensure the security of space-based and space-enabled systems. The application of layered defenses, network segmentation, firewalls, and aggressive patch management should help ensure that systems are protected against previously identified threats. Cyber analytic tools, such as cyber visualization tools or virtualization sandboxes, can help guard against unknown threats.
4. *Raise escalation costs by using foreign satellites:* The U.S. government or commercial satellite providers could make greater use of U.S. partner and allies' government or commercial communications or imagery satellites. From China or Russia's perspective, this would increase the political costs of a cyber attack, given the attack would be on all partner nations in the network, thereby risking horizontal escalation.[68]

While it is impossible to entirely eliminate cyber threats to U.S. space based systems, it may be possible to limit the high costs of unrestrained military competition in space. As Russia and China become increasingly reliant on space, it is possible that a certain parity could emerge in the medium- to long-term. While this parallel situation will not eliminate U.S. concerns about Chinese or Russian counterspace capabilities, it may make it possible for all three governments to pursue strategic restraint on the foundation of mutual vulnerability.

AFPC hosts lunchtime briefing series for Congressional Staff in the House and Senate, featuring presentations by noted subject matter experts focused on a wide array of defense technology issues. If you are a staffer interested in attending future briefings or would like to suggest briefing topics, please contact Defense Technology Programs director Rich Harrison via email at harrison@afpc.org.

Endnotes

Vulnerability and Threat at the Space-Cyber Nexus

1) National Security Council Planning Board, NSC 5814/1, "Preliminary Policy on Outer Space," June 20, 1958, available in Stephanie Feyock, National Security Space Project: Presidential Decisions: NSC Documents (Washington, DC: George C. Marshall Institute, n.d.), 25-26.
2) NASA, "International Partnerships," November 15 2010, http://www.nasa.gov/exploration/dio/partnerships_prt.htm. Many of these involve research or educational activities using NASA-derived data, not the development or operation of flight hardware.
3) The Space Foundation, The Space Report, 2015 (Colorado Springs, CO: Space Foundation, 2015). The Tauri Group, an analytical services firm, estimated the global industry at $323 billion. See The Tauri Group, 2015 State of the Satellite Industry Report (The Tauri Group/Satellite Industry Association, September 2015), 7, http://space.taurigroup.com/reports/SIA_SSIR_2015.pdf.
4) Debra Werner, "Hacking Cases Make Security a Selling Point for Commercial Providers," Space News, March 19, 2012, http://spacenews.com/hacking-cases-make-security-selling-point-commercial-providers/.
5) Douglas Loverro, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, March 25, 2015, 2, http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-LoverroD-20150325.pdf.
6) Maj. Christopher J. King, USAF and MAJ Kenneth G. Kemmerly, USA, "Joint Space Mission Areas," in AU-18, Space Primer (Maxwell Air Force Base, AL: Air University Press, September 2009), 139.
7) Paul G. Kaminski, "America Needs To Stay the Course on GPS Security," Space News, November 19, 2015, http://spacenews.com/op-ed-america-needs-to-stay-the-course-on-gps-security/; James K. Sanborn, "Drone Aircraft Vulnerable to Disruptive GPS 'Spoofing' Technique," Space News, July 16, 2012, http://spacenews.com/drone-aircraft-vulnerable-disruptive-gps-spoofing-technique/.
8) James R. Clapper, Statement before the Senate Select Committee on Intelligence, February 9, 2016, http://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf.
9) Ibid.

10) See Eric Sterner, "Beyond the Stalemate in the Space Commons," in Abraham M. Denmark and Dr. James Mulvenon, eds., Contested Commons: The Future of American Power in a Multipolar World, (Washington, DC: Center for a New American Security, January 2010), 118.
11) Clapper, Statement before the Senate Select Committee on Intelligence.
12) Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015, April 7, 2015, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.
13) Patrick Tucker, "America's Top Threats in Space are Lasers and Nukes," Defense One, July 24, 2014, http://www.defenseone.com/threats/2014/07/americas-top-threats-space-are-lasers-and-nukes/89519/?oref=search_cyber%20attacks%20on%20space%20systems.
14) General John E. Hyten, Presentation to the House Armed Services Committee Subcommittee on Strategic Forces, March 25, 2015, 4, http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-HytenUSAFJ-20150325.pdf.
15) Josh Hartman, "Focus on Cyber Insecurity of Space Systems," Space News, February 16, 2011, http://spacenews.com/focus-cyber-insecurity-space-systems/.
16) Dan Goodin, "Mission-Critical Satellite Communications Wide Open to Malicious Hacking," ars technica, April 17, 2015, http://arstechnica.com/security/2014/04/mission-critical-satellite-communications-wide-open-to-malicious-hacking/.
17) Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies 8, iss. 1, October 1, 2008, 28-29.
18) Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, 2.
19) Mike Gruss, "Aerospace, Telecommunications Companies High on the List for Hackers," Space News, February 20, 2013, http://spacenews.com/33761aerospace-telecommunications-companies-high-on-the-list-for-hackers/. See also, Mandiant, APT: Exposing One of China's Cyber Espionage Units, n.d.
20) Dan Goodin, "Chinese Military Tied to Prolific Hacking Group Targeting US Aerospace Industry," ars technica, June 9, 2014, http://arstechnica.com/security/2014/06/chinese-military-tied-to-prolific-hacking-group-targeting-us-aerospace-industry/.
21) Dan Goodin, "How Highly Advanced Hackers (Ab)Used Satellites to Stay Under the Radar," ars technica, September 9, 2015, http://arstechnica.com/security/2015/09/how-highly-advanced-hackers-abused-satellites-to-stay-under-the-radar/.
22) U.S.-China Economic and Security Review Commissions, 2015 Annual Report to Congress (Washington, DC: U.S.-China Economic and Security Review Commission, November, 2015), 296,http://origin.www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%202%20-%20China%27s%20Space%20and%20Counterspace%20Programs.pdf.
23) Paul K. Martin, Testimony before the House Committee on Science, Space, and Technology Subcommittee on Investigations and Oversight, February 29, 2012, https://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/HHRG-112-SY21-WState-PMartin-20120229.pdf.
24) Juliet Van Wagenen, "WTA Urges Teleport Operators to Improve on Cybersecurity," Via Satellite, August 5, 2015, http://www.satellitetoday.com/technology/2015/08/05/wta-urges-teleport-operators-to-improve-on-cyber-security/.
25) Kaminski, "America Needs To Stay the Course on GPS Security."
26) David Livingstone, "The Intersection of Space and Cyber Security is a Growing Concern," Chatham House, November 25, 2014, https://www.chathamhouse.org/expert/comment/16325.
27) U.S. Department of Defense, The DOD Cyber Strategy, April 2015, 13.
28) Ibid., 24-26.
29) General John Hyten, Presentation to the House Armed Services Committee Subcommittee on Strategic Forces, 14.
30) White House, Office of the Press Secretary, National Space Policy of the United States of America, June 28, 2010, 3. The 2006 policy declared, "The United States considers space capabilities—including ground segments and supporting links—vital to its national interests," and noted, "The United States considers space systems to have the rights of passage through and operations in space without interference. Consistent with this principle, the United States will view purposeful interference with its space systems as an infringement on its rights." White House, Office of the Press Secretary, U.S. National Space Policy, 2006, 2. The 2010 policy considers interference with a space system an infringement on the owning's nation's rights; it is less specific to the United States and more a statement of an international norm.
31) Mike Gruss, "Six Space Questions the Senate Asked Gen. James Dunford," Space News, July 9, 2015, http://spacenews.com/six-space-questions-the-senate-asked-gen-james-dunford/

An Assessment of Russian and Chinese Offensive Cyber Operations on U.S. Space Assets

1) For a historic overview of the Cold War, see John Lewis Gaddis, The Cold War (London: Penguin Groups, 2005).
2) See Von Hardesty and Gene Eisman, Epic Rivalry: The Inside Story of the Soviet and American Space Race (Washington DC: National Geographic, 2007).
3) See General William Shelton's remarks in Elbridge Colby, "From Sanctuary to Battlefield: A Framework for US Defense and Deterrence Strategy for Space," Center for New American Security, January 2016, 8.
4) The author acknowledges the existence of a lively academic debate on whether cyberspace can be characterized as a unique warfighting domain. However, for the purposes of this article, the author has chosen to label cyberspace as a military domain to fit with current U.S. military lexicon. For an alternative view, see Martin Libicki, "Cyberspace is not a Warfighting Domain," I/S: A Journal of Law and Policy for the Information Society 86 (2012).

5) Larry Greenemeir, "GPS and the World's First 'Space War'" Scientific American, February 8, 2016, http://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/.
6) "Space Reconnaissance and the Management of Technical Cooperation," Federation of American Scientists, February 23, 1996, http://fas.org/irp/offdocs/int015.html.
7) Jason Wood, "Strategic Security: Toward an Integrated Nuclear, Space, and Cyber Policy Framework," in "Nuclear Scholars Initiative Project on Nuclear Issues: A Collection of Papers from the 2010 Nuclear Scholars Initiative," Center for Strategic and International Studies, 2010, 95.
8) This estimate is time frame dependent. Between 1997 and 2002, the Hudson Institute estimated that ICT accounted for 19% of economic gross output. More recently, between 2002 and 2007, the Hudson Institute estimated that ICT accounted for 9.3% of economic gross output. See Harold Furchtgott-Roth and Jeffrey Li, "The Contribution of Information, Communications, and Technology Sector to the Growth of U.S. Economy: 1997-2007," The Hudson Institute, 2014.
9) The Committee of Appropriations, "The American Recovery and Reinvestment Act of 2009," January 2009, in the World Economic Forum, "ICT for Economic Growth: A Dynamic Ecosystem Driving the Global Recovery," World Economic Forum, 2009.
10) Ruben Santamarta, "SATCOM Terminals: Hacking by Air, Sea, and Land," IOActive Technical White Paper, 2014, 3.
11) "2015 State of the Satellite Industry Report," Satellite Industry Association, September 2015, http://www.sia.org/wp-content/uploads/2015/06/Mktg15-SSIR-2015-FINAL-Compressed.pdf
12) Author's conversation with Lt. General Yvan Blondin, RCAF (retd.), London, England, March 13, 2016.
13) George Dvorsky, "What Would Happen if All Our Satellites Were Suddenly Destroyed?" iO9: We Come From the Future, June 4, 2015, http://io9.gizmodo.com/what-would-happen-if-all-our-satellites-were-suddenly-d-1709006681. See also Peter Singer and August Cole, Ghost Fleet: A Novel of the Next World War (New York, NY: Houghton Miflin Harcourt Publishing, 2015).
14) Lt. General Brian Arnold, USAF (ret.), Speech to the Air Force Association Global Warfare Symposium, Los Angeles, California, November 19, 2009, in Jason Wood, "Strategic Security: Toward an Integrated Nuclear, Space, and Cyber Policy Framework," in "Nuclear Scholars Initiative Project on Nuclear Issues: A Collection of Papers from the 2010 Nuclear Scholars Initiative," Center for Strategic and International Studies, 2010, 95.
15) See the comments of Sami Saydjari, President of the Cyber Defense Agency, in Hannah Thoreson, "Systems Levels Approach Needed to Secure Space Systems from Cyber Attacks," AIAA Communications, September 2, 2015, http://www.aiaa-space.org/cyberdefense/.
16) Dave Majumdar, "Space Cyber Attacks: A Wake-Up Call," AIAA News, January 14, 2014, https://www.aiaa.org/SecondaryTwoColumn.aspx?id=21097. For more on cyber hardware threats to U.S. weapons systems, see Department of Defense, Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threats," January 2013.
17) Todd Harrison, "The Future of MILSATCOM," Center for Strategic and Budgetary Assessment, 2013, 7.
18) David Livingstone, "Cyberattacks in Space: We Must Defend the Final Frontier," Newsweek, November 26, 2014, http://www.newsweek.com/cyberattacks-space-we-must-defend-final-frontier-287525.
19) Wayne A. Wheeler, "Session 9: Changing Paradigms and Challenges Tools for Space System Cyber Situational Awareness," Presentation at the GSAW 2015, Los Angeles, California, March 2015, and Debra Werner, "Hacking Cases Make Security a Selling Point for Commercial Providers," Space News, March 19, 2012, http://spacenews.com/hacking-cases-make-security-selling-point-commercial-providers/.
20) Siobhan Gorman, Yochi Dreazen, and August Cole, "Insurgents Hack U.S. Drones," Wall Street Journal, December 27, 2009, http://www.wsj.com/articles/SB126102247889095011.
21) Hannah Thoreson, "Systems levels approach needed to secure space systems from cyber attacks," AIAA Communications, September 2, 2015, http://www.aiaa-space.org/cyberdefense/.
22) Harrison, "The Future of MILSATCOM," 1. For more on the weaponization versus militarization of space, see Sean N. Kalic, U.S. Presidents and the Militarization of Space, 1946-1967 (College Station, TX: Texas A&M University Press, 2012).
23) Michael Mazarr, "Mastering the Gray Zone: Understanding A Changing Era of Conflict," Advancing Strategic Thought Series (Carlisle, PA: Army War College, December 2015), 35; Jakub Grygiel and A. Wess Mitchell, The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power (Princeton, NJ: Princeton University Press, 2016), 43.
24) For an excellent overview of Russia and China's developing space and counterspace programs, see Jana Honkova, "The Russian Federation's Approach to Military Space and Its Military Space Capabilities," George C. Marshall Institute Policy Outlook, November 2013, and the United States-China Economic and Security Review Commission's hearing on "China's Space and Counterspace Programs," February 18, 2015.
25) Escalation is defined as an increase in the intensity or scope of a conflict that crosses thresholds considered significant by one or more of the participants. Escalation that involves an increase in the intensity of armed conflict or confrontation, such as the employment of new weapon systems not previously used in the conflict or attacking new categories of targets, is referred to as vertical escalation. Horizontal escalation, in contrast, refers to the expansion of the geographic or cross-domain scope of the conflict. For more information, see Forrest E. Morgan et al., Dangerous Thresholds: Managing Escalation in the 21st Century (Santa Monica, CA: RAND, 2008), 8 and 18.
26) See Lt. General David Buck's remarks to the U.S. House Armed Service Strategic Forces Sub-Committee, as cited in Bill Gertz, "China, Russia Planning Space Attacks on U.S. Satellites," Washington Free Beacon, March 16, 2016, http://freebeacon.com/national-security/china-russia-planning-space-attacks-on-u-s-satellites/.
27) At present, Russia has two air-borne ASAT programs: the Sokol Eschelon (laser) and the Kontakt (kinetic). Moreover, it appears the Kremlin has also developed capacity to approach,

inspect, and potentially sabotage or destroy satellites in orbit. Over the past two years, Moscow has included three mysterious payloads in otherwise innocuous commercial satellite launches. In each case, radar observations by amateur hobbyists and the U.S. Air Force revealed that in each case, an additional small object—dubbed Kosmos -2491, -2499, and -2504—flew away from the jettisoned rocket booster, only to fly back later. It is possible that these objects may be part of a program to refuel aging satellites or it may have more malevolent ASAT intentions. See Honkova, "The Russian Federation's Approach to Military Space and Its Military Space Capabilities," 35-40, and Lee Billings, "War in Space May Be Closer than Ever," Scientific American, August 10, 2015, http://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/.

28) Timothy Thomas, "Russian Views on Information Based Warfare," Airpower Journal Special Edition, 1996, 29.

29) Timothy Thomas, "National State Cyber Strategies: Examples from China and Russia," in Franklin D Kramer and Stuart H Starr, Cyber Power and National Security (Washington DC: Potomac Books, Inc., 2009), 10-11.

30) Professor V.I. Tsymbal, "Kontseptsiya 'informatsionnoy voyny'" (Concept of Information War), paper received at conference with the Russian Academy of Civil Service, Moscow, Russia, September 14, 1995, 2, in Timothy Thomas, "The Russian Understanding of Information Operations and Information Warfare," in David S Alberts and Daniel S. Papp, Information Age Anthology Volume III (Department of Defense: C4ISR Cooperative Research Program, 2001), 800.

31) Thomas, "Russian Views on Information Based Warfare," 29.

32) The 2010 military doctrine also notes the importance of creating a positive view of Russia within the international community during actual battle. See Roland Hickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," FOI: Swedish Defence Research Agency Defense Analysis, 2010, 13.

33) Office of the President of the Russian Federation, "Military Doctrine of the Russian Federation," 2014.

34) "The new doctrine of information security pointed out the danger of destabilization via the Internet," Russian News, October 10, 2015, http://en.news-4-u.ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html.

35) Other examples of the Kremlin's close proximity to hacker groups have generated suspicion about their potential accountability in cyber attacks. One group called the Nashi Youth Group—which is 120,000 members strong—has been linked to Vladislav Surkov, former First Deputy Chief of the Russian Presidential Administration, and there is reason to believe the group may be receiving subsidies from the government. For more information, see Hickerö, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," 38.

36) Grey Logic, "Project Grey Goose Phase II Report: The evolving state of cyber warfare," March 20, 2009), http://fserror.com/pdf/GreyGoose2.pdf

37) With an advanced persistent threat (APT) the hacker seeks to exfiltrate data while maintaining access to the target system over a long period of time. Kenneth Geers, Cyber War in Perspective: Russian Aggression against Ukraine (Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 11.

38) Swati Khandelwal, "Russian Hackers Hijack Satellite Data from Thousands of Hacked Computers," The Hacker News, September 10, 2015, http://thehackernews.com/2015/09/hacking-satellite.html.

39) BlackEnergy is a crimeware toolkit that has been used for years by various criminal outfits. For more on the BlackEnergy toolkit, see Danika Blessman, "Black Energy is Back… and Still Evolving," Solutionary: An NTT Group Security Company, January 18, 2016, https://www.solutionary.com/resource-center/blog/2016/01/black-energy-malware/.

40) Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in Kenneth Geers, Cyber War in Perspective: Russian Aggression against Ukraine (Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 74.

41) Michael J. Assante, "Confirmation of a Coordinated Attack on Ukrainian Power Grid," SANS Industrial Control Systems Security Blog, January 9, 2016, http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/.

42) Wang Huacheng, "The U.S. Military's 'Soft Ribs' and Strategic Weaknesses," Laiowang 27, reprinted in Xinhua Hong Kong Service, July, 5, 2000, in Andrew Krepenevich, "Cyber Warfare: A Nuclear Option," Center for Strategic and Budgetary Assessment, 2012, 29.

43) See Chinese military affairs specialist Rick Fisher in Tara West, "China Prepares for Space Warfare, Creates Space Force to Control LEO with Military Presence," The Inquisitor, January 1, 2016, http://www.inquisitr.com/2673177/china-prepares-for-space-warfare-creates-space-force-to-control-low-earth-orbit-with-military-presence/.

44) Despite a stated preference for "soft-kill" counterspace capabilities, China has been extensively testing kinetic ASAT weapons. In 2007, China destroyed one of its own aging satellites—the Fengyun-1C—via an ASAT weapons test, the result of which was the creation of severe debris clouds. Since 2007, has launched additional tests of ground based ASATs. None of these subsequent launches have destroyed satellites, but Michael Krepon, a space and security expert at the Stimson Center, has noted that China is merely testing to miss, rather than hit. However, China has the same hostile capability as an end result. A May 2013 test propelled a missile 18600 miles into space, approaching the safe haven of 22,236 miles, where US satellites in geosynchronous orbit—including essential early warning and communications—are located. Furthermore, potential exists for China to use a satellite ranging network as an important element in a counterspace "kill chain" providing data of sufficient precision to target satellites with other weapons. This emerged as a concern for the U.S., when one of China's satellite ranging stations, illuminated a U.S. reconnaissance satellite in 2007. For more information, see: Billings, "War in Space May Be Closer than Ever." See also Elbridge Colby, "From Sanctuary to Battlefield: A Framework for US Defense and Deterrence Strategy," Center for New American Security, 2016, 6; Eric Heginbotham et al., "The U.S. –China Military Scorecard:

Forces, Geography, and the Evolving Balance of Power 1996-2017," RAND, 2015, 247-248.
45) For an introductory overview of the use of cyber attacks by China, see Paulo Shakarian, Jana Shakarian, and Andrew Ruef, Introduction to Cyber-Warfare (Waltham, MA: Elsevier, Inc.: 2013), 114-153.
46) "China's Military Strategy," The State Council Information Office of the People's Republic of China, May 2015.
47) Edward Sobiesk, "Redefining the Role of Information Warfare in Chinese Strategy," SANS Institute: InfoSec Reading Room, March 1, 2013.
48) Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," U.S.-China Economic and Security Review Commission, 2009, 4.
49) Peng Hongqi, "A Brief Discussion of Using the Weak to Defeat the Strong under Informatized Conditions," China Military Science 1, 2008, 142-148, in Timothy Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 40-42.
50) U.S. Economic and Security Review Commission, "2011 Report to Congress," November 2011, 216.
51) Hongqi, "A Brief Discussion of Using the Weak to Defeat the Strong under Informatized Conditions," 142-148, in Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force, 40-42.
52) Franz-Stefan Gady, "Why the PLA Revealed its Secret Plans for Cyber War," The Diplomat, March 24, 2015, http://thediplomat.com/2015/03/why-the-pla-revealed-its-secret-plans-for-cyber-war/.
53) Simon Elegant, "Enemies at the Firewall," Time, December 19, 2007, http://content.time.com/time/magazine/article/0,9171,1692063,00.html.
54) Cyber espionage does not necessarily need to be aimed against classified systems to yield national security benefits. Many unclassified systems contain information on technology and innovation that are currently under export control or, in the case of intrusions of software vendors, provide potential insight into latent vulnerabilities that can be leveraged for future purposes. See Jennifer McArdle, "Why the U.S.-China Cyber Spying Ban Will Inevitably Fail," The National Interest, November 1, 2015, http://nationalinterest.org/feature/why-the-us-china-cyber-spying-ban-will-inevitably-fail-14219.
55) Wen T'ao, "PLA Bent on Seizing 'Information Control,'" Hong Kong China Pao, June 1, 2002, in Timothy Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 179.
56) Liu Aimin, "The Characteristics of Informationized War," China Military Science 1, August 2001, 69-72, in Timothy Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 110.
57) Hongqi, "A Brief Discussion of Using the Weak to Defeat the Strong under Informatized Conditions," in Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force, 40-42.
58) Aaron Friedberg, Beyond Air-Sea Battle: The Debate Over US Military Strategy in Asia (London, UK: International Institute for Strategic Studies, 2014), 23-24.
59) Ge Zhenfeng, The Science of Strategy (Beijing: National Defense University, 2001), 366, in Timothy Thomas, The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 178.
60) Gordon Crovitz, "China Goes Phishing: Google Uncovers Beijing's Escalating Cyber Warfare," Wall Street Journal, 6 June 2011, http://www.wsj.com/articles/SB10001424052702303657404576363374283504838.
61) Ronald Deibert et al., "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29, 2009.
62) Nathan Thornburgh, "Inside the Chinese Hack Attack," Time, August 25, 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html.
63) Alexander Klimburg and Heli Tirmaa-Klaar, "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU," European Parliament, April 2011, 7.
64) Sun Tzu, "Formation" in The Art of War, http://web.mit.edu/~dcltdw/AOW/4.html.
65) "Xi's New Model Army," The Economist, January 16, 2016, http://www.economist.com/news/china/21688424-xi-jinping-reforms-chinas-armed-forcesto-his-own-advantage-xis-new-model-army.
66) See Lt. General David Buck's remarks to the U.S. House Armed Service Strategic Forces Sub-Committee, as cited in Bill Gertz, "China, Russia Planning Space Attacks on U.S. Satellites," Washington Free Beacon, March 16, 2016, http://freebeacon.com/national-security/china-russia-planning-space-attacks-on-u-s-satellites/.
67) David Livingstone, "Cyberattacks in Space: We Must Defend the Final Frontier," Newsweek, November 26, 2014, http://www.newsweek.com/cyberattacks-space-we-must-defend-final-frontier-287525.
68) Phillip Saunders, Testimony before the U.S.-China Economic and Security Review Commission, February 18, 2015, http://www.uscc.gov/sites/default/files/Saunders_Testimony2.18.15.pdf.

DEFENSE TECHNOLOGY PROGRAM BRIEF

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AFPC STAFF

Mr. Herman Pirchner, Jr.
President
Mr. Ilan Berman
Vice President
Mrs. Annie Swingen
Director for External Relations
Mr. Jeff M. Smith
Director of South Asia Programs and Kraemer Strategy Fellow
Mr. Richard Harrison
Director of Operations and Defense Technology Programs
Ms. Amanda Azinheira
Research Fellow and Program Officer

BOARD OF ADVISORS

Amb. Paula J. Dobriansky
Hon. Newt Gingrich
Amb. Robert G. Joseph
Sen. Robert Kasten, Jr.
Amb. Richard McCormack
Hon. Robert "Bud" C. McFarlane
Gov. Tom Ridge
Dr. William Schneider, Jr.
Hon. R. James Woolsey
Hon. Dov Zakheim

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org