



Space Systems Protection

This indicator examines the research, development, testing and deployment of capabilities to better protect space systems from potential negation efforts, particularly detecting, withstanding and recovering from an attack.

TREND 6.1: US and Russia lead in ability to detect rocket launches, while US leads in development of technology to detect direct attacks on satellites — The ability to distinguish space negation attacks from technical failures or environmental disruptions is critical to maintaining international stability in space. Early warning also enables defensive responses, but the type of protection available may be limited. Only the US and Russia can reliably detect rocket launches. US Defense Support Program satellites provide early warning of conventional and nuclear ballistic missile attacks; Russia began rebuilding its aging system in 2001 by upgrading its Oko series satellites. France is developing two missile-launch early-warning satellites — Spirale-1 and -2. Most actors have a basic capability to detect a ground-based electronic attack, such as jamming, by sensing an interference signal or by noticing a loss of communications. It is very difficult to obtain advance warning of directed energy attacks that move at the speed of light.

2008 Development

US faced with potential gaps in missile warning systems

In mid-September 2008 the 23rd US Defense Support Program (DSP) missile-warning satellite launched on 10 November 2007 failed in orbit, opening a potential gap in early-warning data in the future.¹ The newest satellite in an ageing system, the loss of US DPS-23 may reduce the remaining lifespan of the system before the next-generation Space-Based Infrared System (SBIRS) can adequately take over. SBIRS underwent further testing in 2008, but the first dedicated satellite is not expected to be launched until 2010 with others following in 2011, 2014 and 2016 if the program stays on course.² To date, launch of the first satellite has slipped from 2004 to 2010 and the program cost has grown from \$4.2-billion to well over \$11-billion.³ In 2008 the Department of Defense opted to increase the planned constellation from three to five satellites – four are necessary for global coverage – and may add a sixth.⁴ A second SBIRS sensor was launched onboard a classified satellite in Highly Elliptical Orbit on 13 March 2008 and both were to be operational by December 2008.⁵ In the meantime, the US Air Force is moving towards an interim capability to prevent potential gaps in coverage. The Infrared Augmentation Satellite (previously the Geosynchronous Earth Orbit Infrared Gap Filler System) would be launched in 2014 if approved by the US Congress.

But early-warning data is only useful if it can be used to respond defensively to a potential threat. The US Air Force intends to design a new system explicitly to counter anti-satellite missiles and other threats through an upgraded vision of the next phase of the Rapid Attack Identification Detection Reporting System (RAIDRS) Block 20. The new systems would be able to monitor all US military satellites and would collect data from open and classified sources on “space weather; missile-warning alerts...; satellite position and telemetry from space; and intelligence from various sources.”⁶ The intent is to predict when a threat is coming and use the data to make decisions about how to maneuver around a threat. As the

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

system progressing, data from new threats include those in orbit will be added.

Comments?

2008 Development

Japan considers a national early-warning system; Russia upgrades its system

Amid tensions with China and North Korea, Japan is developing a plan to promote the defensive use of rockets and early-warning satellites. Following a change in legislation to allow Japan to deploy military satellites for self-defense in May 2008 (see Laws, Policies and Doctrines Trend 2.4), Japan is now considering plans for its own ballistic missile early-warning satellite. Under a draft plan, Japan's Meteorological Agency will evaluate the possibility of integrating missile defense and early-warning technologies into its preexisting Himawari weather satellites. The Education, Science and Technology Ministry's forthcoming natural disaster detection satellite may also be tasked with the detection of missile launches.⁷

In June 2008, Russia launched the early-warning satellite Cosmos-2440 to enhance its fragile early warning system.⁸ The new Cosmos-2440 may replace the aging US-KMO satellite, Cosoms-2379, that has been working since 2001 and is approaching the end of its lifespan.⁹ On 2 December 2008 Russia launched Cosmos-2446, a US-KS early-warning satellite placed in HEO,¹⁰ bringing the total constellation to five satellites, two in GEO and three in HEO.

The upgrades to the system continue with the construction of a new radar station. Russia terminated an early warning agreement with Ukraine in January 2008, and the Ukrainian radars will be replaced with the new Russian Voronezh-type radar Armavir station.¹¹ Its effective range is 4,000 km and should provide an early warning coverage for the whole country. The station is promised to be operational by the end of the year, as a response to the U.S.-made missile systems in Czech Republic and Poland.¹²

Comments?

2008 Development

US pursues tactical space-based awareness and ASAT attack detection

The US Air Force is pursuing tactical space-based situational awareness via a \$30-million project called Self-Awareness Space Situational Awareness (SASSA) intended to provide data on possible anti-satellite attacks including lasers and radiofrequency jamming, and to evaluate potential threats in the operating environment via a sensor on a host satellite.¹³ The sensory payload will be designed to: 1) provide indications of an attack; 2) identify the source of such an attack; 3) assess any damage to the host satellite; and 4) to identify environmental and potential anti-satellite anomalies in space. There are no plans to include countermeasures or other active defenses in the program.¹⁴ The biggest challenge will be pinpointing the origin of a potential attack. While the program is only in the development stage, it is expected that capabilities will be integrated into future satellites such as the TacSat-5, expected to launch in 2011.¹⁵

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

Comments?

2008 Development

European Space Agency approves space situational awareness program

On November 26 2008, officials from the European Space Agency (ESA) agreed to a \$62.8-million space situational awareness program over three years that includes development of a data security and data-release policy, a study of space weather and near-Earth objects, work on a ground-based tracking radar, and design of space surveillance data centers.¹⁶ Due to disagreement on issues of system management and data security, the approved program is significantly scaled down from earlier proposals that would have launched a full-scale European SSA capability, and even the more modest plan proposed earlier in the year that would have initiated networking and coordination of existing national SSA capabilities.¹⁷ But if successful, the program may be scaled up in the future. In the meantime, member states with national military data from systems such as the French Graves radar will not be contributing significant data to the joint effort.¹⁸ Instead, France announced that it plans to build a national space situational awareness capability by coupling its existing GRAVES radar with the German Tira tracking and imaging radar.¹⁹

A European SSA program would alleviate dependence on foreign data, namely the reliance on the USAF Space Surveillance Network (SSN), which is currently the only maintained catalogue of space objects, and is available publicly. Yet, the development of an independent data collection and tracking capability necessitates the development of rules for access to that data. US and European military authorities have initiated discussion on rules of conduct governing what information is in the public domain and have opened a regular channel for cooperating on space surveillance issues – France in particular has been frustrated that data on its military satellites have been published by the US.²⁰

Comments?

2008 Space Security Impact

Please comment on how events under Trend 6.1 may impact the security of outer space

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

TREND 6.2: Protection of satellite ground stations and satellite communication links — Many space systems lack protection from attacks on ground stations and communications links. The vast majority of commercial space systems have only one operations center and one ground station, leaving them vulnerable to negation efforts. While many actors employ passive electronic protection capabilities, such as shielding and directional antennas, more advanced measures, such as burst transmissions, are generally unique to military systems and the capabilities of more technically advanced states. China and the US have been aggressively pursuing a variety of anti-jamming capabilities.

2008 Development

US Cyber Command put on hold but NATO opens Co-operative Cyber Defense Center

Plans for a US Air Force Cyber Command announced in 2006 to be the dominant service to ‘dominate’ cyberspace was set to become operational on 1 October 2008. Plans were put on hold in August 2008, however, when the Air Force announced that it would not be activated but would instead be transferred to the US Air Force Space Command.²¹ However, plans to have a separate Cyber Command were reconstituted in October 2008 and are intended to include both defense of Defense Department networks and capabilities to launch attacks (see Space Systems Negation Trend 7.1).²² On the defensive side, the Air Force is struggling with how to get ahead of online attackers through efforts to ‘re-write the rules’ of cyberspace in the newly announced Integrated Cyber Defense program of the Air Force Research Laboratory, including “making hostile traffic inoperable on Air Force networks, locating and identifying once-anonymous hackers, [and] enabling Air Force servers to evade or dodge electronic attacks.”²³ It is not clear how this will be made feasible, however. In the mean time, significant activities in cyberspace are done by the Navy’s Network Warfare Command and the Space and Naval Warfare Systems Center.²⁴

On 14 May 2008 seven NATO members (Estonia, Latvia, Lithuania, Germany, Italy, Spain, Slovakia) formally established a Co-operative Cyber Defense Center of Excellence based in Tallin, Estonia.²⁵ The Center is intended to improve the defense of key information systems against cyber attacks and to share best practices. It followed the adoption of a common NATO policy on cyber defense at the NATO summit meeting in April 2008 to develop a coordinated approach to cyber attacks.²⁶ NATO’s focus on cyber security is the result of previous attacks against Estonia in 2007, which crippled strategic network infrastructure including banks.²⁷

Comments?

2008 Development

US improves satellite communication security, tests laser link with Germany

Laser communication links remain an ongoing interest for both increasing data transfer rates and improving security – because they transfer information via line of sight, they are more difficult to intercept or jam. A private German company, Tesat-Spacecom, tested laser communication technology between two satellites over several months beginning in February 2008. The German TerraSAR-X radar satellite and US Near Field Infrared Experiment (NFIRE) satellite exchanged data at speeds of 5.5 gigabits per second, nearly one hundred times faster than conventional radio communication links, but the

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

company claims that the link is capable of achieving speeds of up to 16 gigabits per second.²⁸ The link was maintained for twenty minute increments, at straight-line distances between 2,000 and 8,000 kilometers.²⁹ Future tests are planned between satellites and ground stations in Germany as well as Spain, instead of direct inter-satellite transmissions. These tests will produce a different set of challenges, since laser communications suffer losses due to physical obstacles such as atmospheric particles and clouds.³⁰ Development of the technology has taken over 10 years.

Similar efforts by the US military have faced ongoing technical and budgetary obstacles. The Transformational Communications Satellite (TSAT) intended to provide protected, high-speed communications to the military, including laser communications, is being revised for a scaled-back version known as Block 10, which will lose the satellite-to-satellite laser links.³¹ The program is now 10 years behind schedule, with the first of the reduced capacity satellites not expected to launch until 2019. NASA is also developing a new communications architecture based on optical links.³² Details will be outlined in NASA's 2010 budget request.

The US also continues to improve the security of its existing radio-based satellite communication systems. In February 2007 a new system known as Eagle Sentry was deployed for the purpose of tracking interference with commercial communication systems that are used by the US. Following good performance, a second system was deployed in Europe and was used in 2008 to monitor communications in Afghanistan and Iraq. The system localizes and characterizes interference, allowing it to be identified as a weather event or an enemy attack.³³ The US military has a similar capability with the Rapid Attack Identification and Reporting System (RAIDRS) Block 10, which is currently operating in the Middle East with a prototype system and will begin full operations in 2011.³⁴ The DoD also approved a \$9.2-million contract with General Dynamics for the development of improved satellite encryption methods, which should be completed and ready for production by late 2009.³⁵

Comments?

2008 Space Security Impact

Please comment on how events under Trend 6.2 may impact the security of outer space

TREND 6.3: Protection of satellites against direct attacks — The primary source of protection for satellites comes from the difficulties associated with launching an attack into space. Satellite protection measures also include system redundancy and interoperability, which has become characteristic of satellite navigation systems. Most key US, European, and Russian military satellites are hardened against the effects of a high-altitude nuclear detonation. Nonetheless, if an actor has the ability to overcome these natural defenses, there are few options available for physically protecting a satellite against a direct attack. Consequently, initiatives to prevent the proliferation and use of negation capabilities

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

covered in the chapters on Laws, Policies and Doctrines and Commercial Space are also critical for protection, as is the achievement of collective space security as defined by the Space Security Index.

2008 Development

2008 Development: US pursues space-based satellite protection via guardian nanosatellites

The US continues to develop capabilities to protect satellites against direct attacks through on-orbit space surveillance. In 2008 the US Air Force received \$6.3-million in the FY2009 Defense Authorization budget for an “active and/or passive threat warning sensor for detection of a direct ascent or co-orbital vehicle,” likely part of the Autonomous Nanosatellite Guardian for Evaluating Local Space (ANGELS) under the Spacecraft Protection Technology Project within the Space Technology Program.³⁶ The 2009 request schedules selection of “two technology options that provide defensive capability” for “incorporation” in GEO and LEO satellites.³⁷ In 2007 the USAF awarded a \$29.5-million contract to Orbital Sciences Corporation to upgrade the ANGELS program, which is developing guardian nanosatellites that are capable of identifying and characterizing anomalies that are local to the spacecraft. The nanosatellites will provide some degree of awareness to their host satellite, enabling the satellite to deploy countermeasures or maneuver in the event of a threat.³⁸

The US demonstrated a provisional capability to inspect and characterize satellites and potential abnormalities on-orbit in 2008 using the Microsatellite Technology Experiments (MiTex) satellites following the failure of the US DSP-23 early-warning satellite in GEO in September 2008 (see Space Systems Negation Trend 7.4). There are concerns about its potential use of on-orbit defensive systems to also engage in activities to target other spacecraft.

A slightly different technology capabilities ostensibly aimed at the same goal, however, is the Fast Access Spacecraft Testbed (FAST) under DARPA’s Tactical Technology Office. The goal of the program is to demonstrate a High Power Generation Subsystem (HPGS) that can combined with electric propulsion systems for “light weight, high-power, highly mobile spacecraft.”³⁹ According to DARPA “such a system can form the basis for a paradigm-shift in spacecraft mission design, enabling an affordable launch to LEO with self-transfer to GEO, while retaining sufficient maneuverability in GEO to perform flexible mission scenarios including numerous sorties. The FAST system is intended to enable highly responsive on-orbit servicing architectures, on-orbit space situational awareness capabilities, and remove power constraints from payloads such as ultra wide-bandwidth communications or radar.”⁴⁰ Boeing won a contract to develop the first phase of the program in 2008, which was allocated \$12-million in the defense budget.⁴¹ However, an ability to easily maneuver large distances in space can also provide the basis for negation activities against other satellites.

Comments?

2008 Development

Improvements in satellite hardening against EMP/directed energy attacks

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

Electronics are the foundation of satellite communication networks, and the threat of an Electromagnetic Pulse (EMP) attack, which would involve an “instantaneous, intense energy field that can overload or disrupt at a distance numerous electrical systems and high technology Microcircuits,” through a nuclear explosion or microwaves is a growing concern. Currently, the best protection from a High Altitude EMP (HEMP) event is hardening of those electronics that provide essential services, through a Faraday Cage, in conjunction with surge protectors, which may provide an ability to withstand a HEMP blast.⁴² When combined with redundancy of critical components, however, this type of protection is not inexpensive and may be deemed impractical for all but the most sensitive of military satellites. Given the damage to critical infrastructures that could be incurred from a HEMP, steps are being taken to reduce the duration of the atmospheric ionization. The High Frequency Active Auroral Research Program (HAARP) in Alaska is one of several ionospheric heaters throughout the world. It emits radio waves to mitigate the effects of a high altitude nuclear detonation (HAND). The USAF is also in the midst of developing a coating for critical system components that would offer some kind of protection from directed energy weapons such as lasers.⁴³ While the technology is being developed primarily for ground based assets and missiles, the coating could offer an inexpensive way to protect satellites from energy attacks.

Comments?

2008 Space Security Impact

Please comment on how events under Trend 6.3 may impact the security of outer space

TREND 6.4: US leads in capability to rapidly rebuilt space systems following direct attacks on satellites
— The ability to rapidly rebuild space systems after an attack could reduce vulnerabilities in space and increase the ability to recover from an attack. Although the US and Russia are developing various elements of responsive space systems, no state currently has this capability. The key US responsive launch initiative is the Falcon program, which seeks to develop a rocket capable of placing 100-1,000 kilograms into LEO within 24 hours. It includes the AirLaunch LLC QuickReach air-launch rocket and the SpaceX Falcon-1.

2008 Development

US developing capabilities to rebuild and repair space assets

In 2008 Alliance Spacesystems, the prime contractor for the DARPA/NRL's Front-End Robotics Enabling Near-Term Demonstration (FRIEND) program, completed development, testing, and delivery of the robotic arm to be used for spacecraft servicing⁴⁴ The next phase in the development of the arm will see its used in integrated mission rehearsals, such as an autonomous grappling of objects representative of

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

satellite hardware. The program offers the ability to salvage inoperable space assets via an autonomous rendezvous satellite, as well as reposition operating satellites that do not have the ability to maneuver on their own. However, on-orbit servicing (OOS) technology such as the FRENDS program raises ASAT concerns, should it become possible to approach an enemy satellite and tamper with its hardware. FRENDS was allocated \$10.7-million in the FY 2009 budget.⁴⁵

The US continues to support the development of small satellites to provide passive protection in space. DARPA's Future, Fast, Flexible, Fractionated, Free-Flying Spacecraft United by Information Exchange (System F6) program seeks to research, develop, and test a satellite architecture where the functionality of a single satellite is replaced by a cluster of free-fly subsatellites that wirelessly communicate with each other.⁴⁶ Each subsatellite of the system can perform a separate function or duplicate the function of another module. The use of smaller and smaller satellites to provide operational requirements in outer space, as well as the use of defensive clusters of satellites or the inclusion of space-based backup systems, could contribute to space systems protection strategies, including Operationally Responsive Space for the rapid repair of space systems. A call for proposals was issued in 2007, and in February 2008 DARPA awarded \$38.5-million in contracts for the initial phase to Boeing, Lockheed Martin, Northrop Grumman, and Orbital Sciences.⁴⁷ The initial stage involves testing the technologies needed for a fractionated spacecraft including wireless communication, distributed computing, wireless power transfer, and autonomous cluster navigation, and an econometric analysis to determine value. This is a fairly significant program – in 2007 it received \$21-million in the defense budget, and in 2008 this figure was increased to \$37.3-million.⁴⁸ Although fractionalized satellites could reduce risk, they would also increase costs upfront.

Comments?

2008 Development

US and China developing capabilities to quickly launch spacecraft

The US military Operationally Responsive Space (ORS) office, established in 2007 to develop space systems that can be rapidly launched to provide military applications, lost its first satellite on the third failed Falcon-1 launch by private company SpaceX on 3 August 2008. The launch, called "Jumpstart" was intended to "demonstrate that a spacecraft bus can be built, tested and integrated in a short period of time,"⁴⁹ namely seven months from the ORS office receiving funding, and within four months of the office choosing a contractor for the satellite itself and the launch vehicle. Launch of Tactical Satellite 3 (TacSat-3), a satellite developed by the Air Force Research Laboratory to demonstrate the functionality of small satellites controlled directly by military officers in the field, was also delayed. Initially expected in 2007, then in October 2008, it has been delayed to 2009 following technical issues.⁵⁰ Nonetheless, the ORS office is moving forward with additional plans to develop a rapid launch capability, which includes experiments towards launches with as little as six days notice, and experiments on Tactical Satellite-5, which will feature the Self-Awareness Space Situational Awareness Sensor (SASSA – see Trend 6.2).⁵¹

In other developments, Air Launch, which is under contract from DARPA and NASA, has claimed that its QuickReach rocket is capable of placing a 454 kg satellite into orbit from a C-17 airplane, in less than 24 hours. The cost of such a launch would be approximately \$5-million, compared to \$30-\$100-million for a typical launch. Research on new launch technologies is also taking place. LaunchPoint is working with the

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

US military to research a magnetic ring launcher that would be capable of launching smaller satellites into orbit for approximately \$75,000 per launch and able to deliver satellites at a rate of one per day. The Electromagnetic Systems Division at the University of Austin, Texas, is researching a combination of air launch and magnetic technologies called a railgun for nanosatellites.⁵²

The US is not the only actor interested in being able to rapidly launch low-cost satellites capable of providing responsive needs or reconstituting space assets. China is also working to develop more capable microsatellites for military and other space missions, and a classified “Shenlong air-launched booster designed for drop from a Chinese H-6 badger bomber for smallsat launch operations.”⁵³ Like US air-launch capabilities including the Pegasus and the planned QuickReach, there is a possibility that it could also be used to support the covert deployment of anti-satellite capabilities.

Comments?

2008 Space Security Impact

Please comment on how events under Trend 6.4 may impact the security of outer space

Endnotes

¹ Andrea Shalal-Esa, “U.S. still probing security satellite failure,” Reuters (6 January 2009).

² Staff Writers, “New Missile Warning Satellite Built by Lockheed Martin Progressing in Critical Test Phase,” Space War (28 March 2008), online: http://www.spacewar.com/reports/New_Missile_Warning_Satellite_Built_By_LockMart_Progressing_In_Critical_Test_Phase_999.html; Amy Butler, “Newest DSP Satellite Likely Failing in Orbit,” *Aviation Week* (1 December 2008), online: <http://www.aviationweek.com/aw/generic/story.jsp?id=news/DSP120108.xml&headline=Newest%20DSP%20Likely%20Failing%20in%20Orbit&channel=space>.

³ Andrea Shalal-Esa, “U.S. still probing security satellite failure,” Reuters (6 January 2009).

⁴ Space News, 10 September 2008; US Government Accountability Office, “Space Based Infrared System High Program and its Alternative,” Report to Congress, GAO-07-1088R (12 September 2007); Turner Brinton, “DSP Constellation Health Concerns Prompt Plan for Gap-Filler Satellite,” Space News (24 November 2008).

⁵ Spacedaily.com (6 August 2008); SpaceDaily.com, (24 June 24 2008).

⁶ Amy Butler, “USAF Eyes Counter-ASAT System in 2011,” *Aviation Week* (16 March 2008).

⁷ *Yomiuri Shimbun*, (5 November 2008).

⁸ Stephen Clark, “Russian Proton Rocket Launches Military Satellite,” *Space.com* (30 June 2008), online: <http://www.space.com/missionlaunches/sfn-080630-proton-launch.html>.

⁹ Pavel Podvig, “Lunch of an Early Warning Satellite,” *Russian Strategic Nuclear Forces – Blog* (25 January 2008), online: http://russianforces.org/blog/2008/01/russia_pulls_out_of_an_earlywa.shtml.

¹⁰ Pavel Podvig, “Angara launcher to be ready in 2011,” *Russian Strategic Nuclear Forces – Blog* (2 December 2008), online: http://russianforces.org/blog/2008/12/launch_of_cosmos-2446_a_new_fi.shtml.

¹¹ Pavel Podvig, “Russia pulls out of an early-warning arrangement with Ukraine,” *Russian Strategic Nuclear Forces – Blog* (25 January 2008), online: http://russianforces.org/blog/2008/01/russia_pulls_out_of_an_earlywa.shtml.

¹² “Russia to put new radar station on combat duty by yearend,” *RIA Novosti* (11 April 2008), online: <http://en.rian.ru/russia/20080411/104874373.html>.

¹³ Lockheed Martin, “Lockheed Martin Receives \$30-million Contract for US Air Force SASSA Program,” (4 November 2008), online: PBC007 <http://www.pcb007.com/pages/zone.cgi?a=46237>.

¹⁴ William Mathews, “USAF Seeks Threat Detectors for Satellites,” *Defense News* (9 June 2008), p. 40.

¹⁵ Paul Marks, “Pentagon wants laser attack warnings for satellites,” *New Scientist* (28 May 2008).

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

-
- ¹⁶ Peter B. de Selding, "ESA Space Surveillance Effort of Little Interest to French Military," *Space News* (8 December 2008), p. 11.
- ¹⁷ See Tony Skinner, "Europe pursues space network," *Jane's Defence Weekly* (24 September 2008), p. 18.
- ¹⁸ Peter B. de Selding, "ESA Space Surveillance Effort of Little Interest to French Military," *Space News* (8 December 2008), p. 11.
- ¹⁹ *Space News* 10 Nov 2008, Page A2
- ²⁰ Peter B. de Selding, "ESA Approves Space Situational Awareness Program," *Space News* (19 May 2008), p. 10; Peter B. de Selding, "Despite SSA Collaboration, Europe Leery of U.S. Intentions," *Space News* (16 January 2009).
- ²¹ Bob Brewin, "Air Force Suspends Cyber Command Program," Nextgov (12 August 2008), online: http://www.nextgov.com/nextgov/ng_20080812_7995.php; Erik Holmes, "AFSPC Commander Foresees Smooth Mission Transition," *Defense News* (10 November 2008).
- ²² Bob Brewin, "Air Force pursues Cyber Command again," Nextgov, (7 October 2008), online: http://www.nextgov.com/nextgov/ng_20081007_1366.php.
- ²³ Noah Shachtman, "Air Force Aims to 'Rewrite Laws of Cyberspace,'" *Wired – Blog* (3 November 2008), online: <http://blog.wired.com/defense/2008/11/air-force-aims.html>.
- ²⁴ Phillip Coyle referenced in Bob Brewin, "Air Force Suspends Cyber Command Program," Nextgov (12 August 2008), online: http://www.nextgov.com/nextgov/ng_20080812_7995.php; Erik Holmes, "AFSPC Commander Foresees Smooth Mission Transition," *Defense News* (10 November 2008).
- ²⁵ Denise Hammick, "NATO cyber defence centre established." *Jane's Defence Weekly* (21 May 2008), p. 11.
- ²⁶ <http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377>
- ²⁷ <http://news.bbc.co.uk/2/hi/europe/6665195.stm>
- ²⁸ Staff Writers, "TerraSar-X and NFIRE Fire Up the Pipe With Laser Data Transfer," *Space Mart* (14 May 2008), online: http://www.spacemart.com/reports/TerraSAR_X_And_NFIRE_Fire_Up_The_Pipe_With_Laser_Data_Transfer_999.html.
- ²⁹ Peter B. de Selding, "U.S.-German Laser Intersatellite Link Performs Well on 2 Spacecraft," *Space News* (17 March 2008), p. 1,4.
- ³⁰ Staff Writers, "TerraSar-X and NFIRE Fire Up the Pipe With Laser Data Transfer," *Space Mart* (14 May 2008), online: http://www.spacemart.com/reports/TerraSAR_X_And_NFIRE_Fire_Up_The_Pipe_With_Laser_Data_Transfer_999.html.
- ³¹ Turner Brington, "U.S. Air Force Preparing to Extend T-Sat Design Studies," *Space News* (15 December 2008), p.4.
- ³² Brian Berger, "Griffin: Laser's Key to Space Comms," *Defense News* (6 October 2008).
- ³³ Jeremy Singer, "U.S. Army System Tracking Interference with Communication Satellites," *Space News* (18 February 2008), p. A2.
- ³⁴ Amy Butler, "USAF Eyes Counter-ASAT System in 2011," *Aviation Week* (16 March 2008).
- ³⁵ "Air Force Awards General Dynamics a \$9 million satellite encryption contract," *San Antonio Business Journal* (9 July 2008).
- ³⁶ Beau Rizzo, "Fiscal Year 2009 (FY 09) Defense Budget: Programs of Interest," Center for Defense Information, online: <http://www.cdi.org/pdfs/FY2009ChartFinal.pdf> (date accessed: 20 January 2009).
- ³⁷ Theresa Hitchens and Victoria Sampson, "Space Weapons Spending in the FY 2009 Defense Budget," Center for Defense Information (March 2008), online: <http://www.cdi.org/pdfs/SpaceWeaponsFY09.pdf>.
- ³⁸ CDI Space Security Update #11 (5 December 2007). Originally sourced: *Jane's Defence Weekly* (28 November 2007); Alan Collinson, "Cutting the clutter," *Jane's Defence Weekly* (16 January 2008), p. 30.
- ³⁹ DARPA, Tactical Technology Office, Broad Agency Announcement, "Fast Access Spacecraft Testbed," (20 November 2007), p. 5, online: http://www.darpa.mil/tto/solicit/FAST_BAA_07-65.pdf.
- ⁴⁰ DARPA, Tactical Technology Office, Broad Agency Announcement, "Fast Access Spacecraft Testbed," (20 November 2007), p. 5, online: http://www.darpa.mil/tto/solicit/FAST_BAA_07-65.pdf.
- ⁴¹ Staff Writers, "Boeing Team to Design New Spacecraft Power Generation System," *Space Travel* (4 August 2008), online: http://www.space-travel.com/reports/Boeing_Team_To_Design_New_Spacecraft_Power_Generation_System_999.html; Beau Rizzo, "Fiscal Year 2009 (FY 09) Defense Budget: Programs of Interest," Center for Defense Information, online: <http://www.cdi.org/pdfs/FY2009ChartFinal.pdf> (date accessed: 20 January 2009).
- ⁴² Clay Wilson, Congressional Research Service, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave Devices (HMP): Threat Assessments," CRS Report for Congress (Order Code RL32544) (updated 26 March 2008), online: FAS <http://fas.org/sgp/crs/natsec/RL32544.pdf>.
- ⁴³ Noah Shachtman, "Air Force Looks to Laser Proof Its Weapons," *Wired – Blog* (30 July 2008), online: <http://blog.wired.com/defense/2008/07/spray-on-laser.html>.
- ⁴⁴ Alliance Spacesystems, "Alliance Spacesystems Delivers Robotic Arm for DARPA's 'FRIEND' Technology Demonstration" Press Release (12 September 2008).
- ⁴⁵ Beau Rizzo, "Fiscal Year 2009 (FY 09) Defense Budget: Programs of Interest," Center for Defense Information, online: <http://www.cdi.org/pdfs/FY2009ChartFinal.pdf> (date accessed: 20 January 2009).
- ⁴⁶ Noah Shachtman, "Autonomous' Mini-Spacecraft Team up to Replace Big Sats," *Wired – Blog* (31 July 2007), online: <http://blog.wired.com/defense/2007/07/the-objective-o.html>.
- ⁴⁷ DARPA, Press Release, "DARPA Awards Contracts for Fractionated Spacecraft Program," (26 February 2008), online: <http://www.darpa.mil/news/2008/F6.pdf>. William Mathews, "Cluster Solution," *Defense News* (10 March 2008), p.16.
- ⁴⁸ Beau Rizzo, "Fiscal Year 2009 (FY 09) Defense Budget: Programs of Interest," Center for Defense Information, online: <http://www.cdi.org/pdfs/FY2009ChartFinal.pdf> (date accessed: 20 January 2009); Jeremy Singer, "DARPA Seeks Increase for Space Programs in 2009," *Space News* (25 February 2008), p. 22,30.
- ⁴⁹ Officials from the Operationally Responsive Space office quoted in Caitlin Harrington, "ORS prepares to demo rapid space launch capability," *Jane's Defence Weekly* (4 June 2008), p.5.
- ⁵⁰ Jeremy Singer, "First TacSat Launch Will be No Earlier Than December," *Space News* (30 May 2006); Michael Kleiman, "Technical Issues, More Tests Delay Tactical Satellite-3 Liftoff," *Space War* (3 November 2008), online: http://www.spacewar.com/reports/Technical_Issues_More_Tests_Delay_Tactical_Satellite_3_Liftoff_999.html.

This document is a draft for the upcoming publication *Space Security 2009*. Please send comments on the draft to jwest@ploughshares.ca

⁵¹ Jeremy Singer and Colin Clark, "Budget Puts ORS, Counterspace on Different Funding Trajectories," *Space News* (11 February 2008), p.11.

⁵² William Mathews, "Military Searchers for Faster, Less Expensive Techniques to Lift Payloads," *Defense News* (7 April 2008).

⁵³ Craig Covault, "Size Doesn't Matter," *Aviation Week and Space Technology* (22 December 2008), p. 22.