Promoting Cooperative Solutions for Space Sustainability

Going Blind: Why America is on the Verge of Losing its Situational Awareness in Space and What Can be Done About it

September 10, 2012

By Brian Weeden
Technical Advisor
Secure World Foundation

ABOUT SECURE WORLD FOUNDATION

Secure World Foundation (SWF) is a private operating foundation dedicated to the secure and sustainable use of space for the benefit of Earth and all its peoples. SWF engages with academics, policy makers, scientists and advocates in the space and international affairs communities to support steps that strengthen global space sustainability. It promotes the development of cooperative and effective use of space for the protection of Earth's environment and human security.

ABOUT THE AUTHOR

Brian Weeden is the Technical Advisor for Secure World Foundation and has 14 years of professional experience in the national and international space security arena. His wealth of technical knowledge and expertise has established him as a thought leader for providing critical analysis that supports development of space policy on a global scale.

Prior to joining the Foundation, Mr. Weeden served 9 years on active duty as an officer in the United States Air Force working in space and intercontinental ballistic missile (ICBM) operations. As part of U.S. Strategic Command's Joint Space Operations Center (JSpOC), Captain Weeden directed the orbital analyst training program and developed tactics, techniques and procedures for improving space situational awareness.

In his current role as Technical Advisor, Mr. Weeden conducts research on space debris, global space situational awareness, space traffic management, protection of space assets, and space governance. He also organizes national and international workshops to increase awareness of and facilitate dialogue on space security and sustainability topics. Respected and recognized as an expert, Mr. Weeden's research and analysis have been featured in *The New York Times*, *National Public Radio*, *the BBC*, *Fox News*, *China Radio International*, *The Economist*, academic journals, presentations to the United Nations, and testimony before the U.S. Congress. He is also Co-Chair of the World Economic Forum's Global Agenda Council on Space Security.

Mr. Weeden holds a Bachelor of Science (B.S.) degree in Electrical Engineering from Clarkson University, a Master's of Science (M.S) degree in Space Studies from the University of North Dakota, and is also a graduate of the International Space University Space Studies Program (2007, Beijing). He is currently a Ph.D. student in Science and Technology Public Policy at George Washington University.

CONTENTS

LIST OF ACRONYMS

1 SPCS – 1st Space Control Squadron
AFSPC – Air Force Space Command
AFSPC/A9 – Analyses, Assessments and Lesson Learned branch of Air Force Space Command
ASW – Astrodynamics Support Workstation
C2 – Command and Control
CA – Conjunction Analysis
CAVENet – Correlation, Analysis, and Verification of Ephemerides Network
CCIC2S – Combatant Commanders' Integrated Command and Control System
CCSDS – Consultative Committee for Space Data Systems
CFE – Commercial and Foreign Entities
CIA – U.S. Central Intelligence Agency
COLA – Collision Avoidance
CONUS – Continental United States
COTS – Commercial Off-the-Shelf
CP 0 – Capability Package 0
CPU – Central Processing Unit
CSM – Conjunction Support Messages
CS/SSA COI – Command and Control Space Situational Awareness Community of Interest
DSC – Defensive Space Control
DoD – U.S. Department of Defense
DSP – Defense Support Program
ESA – European Space Agency
FAA – Federal Aviation Administration
GAO – Government Accountability Office
GEO – Geostationary Earth Orbit
GTO – Geosynchronous Transfer Orbit
GOTS – Government Off-the-Shelf
GP – General Perturbations
GPS – Global Positioning System
HAC – High Accuracy Catalog
ICANN – Internet Corporation for Assigned Names and Numbers
ICBM – Intercontinental Ballistic Missile
ISO – International Organization for Standardization
ISON – International Scientific Optical Network
ISR – Intelligence, Surveillance and Reconnaissance
ISRO – Indian Space Research Organization
ISSA – Integrated Space Situational Awareness
IT – Information Technology
JFCC Space – Joint Functional Component Command for Space
JMS – JSpOC Mission System
JSpOC – Joint Space Operations Center
LEO – Low Earth Orbit
MIT – Massachusetts Institute of Technology

MFLOPS – Millions of floating point operations per second
NASA – National Aeronautics and Space Administration
NGO – Non-Governmental Organization
NIST – National Institute for Standards and Technology
NOAA – National Oceanic and Atmospheric Administration
NORAD – North American Aerospace Defense Command
NRO – National Reconnaissance Office
NSA – National Security Agency
NSP – National Space Policy
NSSS – National Security Space Strategy
OIG – Orbital Information Group
OPAF – Other Procurement, Air Force
RAIDRS – Rapid Attack Identification Reporting System
RCS – Radar Cross Section
RDT&E – Research, Development, Test, and Evaluation
SATCAT – Satellite Catalog
SATC – Satellite Catalog (current reference)
SBSS – Space Based Space Surveillance
SCC – Space Control Center
SCOPES – Space Common Operating Picture Exploration System
SDA – Space Data Association
SDC – Space Data Center
SGI – Silicon Graphics, Inc.
SGP – Simplified General Perturbations
SHAC – Space High Accuracy Catalog
SLR – Satellite Laser Ranging
SMC – Space and Missile Systems Center
SP – Special Perturbations
SPADATS – Space Detection and Tracking System
SPADOC – Space Defense Operations Center
SSA – Space Situational Awareness
SSN – Space Surveillance Network
STACS – System Threat Assessment and Characterization
SWF – Secure World Foundation
TLE – Two-Line Elements
USAF – U.S. Air Force
VHF – Very High Frequency
UCS – Union of Concerned Scientists
USNORTHCOM – United States Northern Command
USSTRATCOM – United States Strategic Command

EXECUTIVE SUMMARY

Since the 1960s, outer space has played a critical role in U.S. national security. Satellites provide continuous monitoring of the entire globe to detect ballistic missile launches and early warning of a potential nuclear attack. Other satellites provide valuable intelligence information on adversaries' weapons development and deployment, as well as verification of arms control treaties and agreements. In more recent years, additional space-based capabilities have provided significant benefits to almost all aspects of national security, including precision-guided munitions, command and control of unmanned aircraft, connectivity to remote locations, and an incredible amount of information on military activities in the land, sea, and air domains. Space-based capabilities also play critical roles in global transportation, banking and financial systems, communications, monitoring and utilization of natural resources, and disaster management.

After the fall of the Soviet Union in 1991, a significant number of those within the national security community predicted that the United States would emerge as the single global superpower with unfettered ability to use outer space as it saw fit. Those prognostications could not have been further from reality. Today, outer space is actively used by more than 60 countries and international organizations for an ever-growing number of national security, scientific, and commercial uses. This explosion in use, coupled with legacy issues such as a large amount of space debris, has added to a growing number of challenges facing the continued, sustainable use of space over the long-term. These challenges include the threat of collisions between/among space debris and other satellites, severe solar storms and other forms of space weather, radiofrequency interference, and mishaps, misperceptions or mistrust that could lead to conflict between nations.

A key requirement for successfully tackling these challenges is to improve space situational awareness (SSA), broadly defined as characterizing the space environment and its impact on activities in space. SSA provides crucial information for the United States and all space actors to enable safe and efficient use of space. To meet the aforementioned challenges, the 2010 U.S. National Space Policy states that the United States shall "develop, maintain, and use space situational awareness (SSA) information from commercial, civil, and national security sources to detect, identify, and attribute actions in space that are contrary to responsible use and the long-term sustainability of the space environment." As the primary provider of SSA for both the United States and the world, the Department of Defense (DoD) has also embraced the need for improvements in SSA. The 2011 National Security Space Strategy (NSSS) states that the DoD will continue to improve the quantity and quality of the SSA information it obtains, share data with other space actors, and enhance spaceflight safety for all parties.

However, the U.S. military is a long way from being able to meet these lofty goals. SSA incorporates many elements and functions, but at its core is the maintenance of a catalog of space

objects. The information technology (IT) architecture used to maintain this core and the fundamental approach to SSA taken by the U.S. government are still rooted in a Cold War mindset. The two IT systems at the heart of the U.S. military's SSA capabilities date back to the 1980s and are long past obsolete. Over the last 12 years, multiple procurement programs have failed to replace them, and these failures are in large part a function of the U.S. military procurement culture's inability to develop a solution for a problem with constantly evolving requirements and reliance on modern software and computing hardware. Additionally, the U.S. military's narrow definition of the SSA community of interest and their lack of involvement of key stakeholders in developing astrodynamic standards has created impediments to solving these IT challenges and gaining the trust and buy-in from the global community of space actors.

These materiel, cultural, and bureaucratic shackles are preventing the United States from developing the SSA capabilities it requires to meet its own national security needs and thereby contribute to the long-term sustainability of outer space activities. As long as the U.S. military continues to use these two legacy IT systems, it will face severe restrictions on the number of space objects it can catalog and track, the speed and accuracy of calculations to determine potential on-orbit collisions and warn satellite operators, its capability to share SSA data with partners and allies and ingest outside data, and its ability to take full advantage of the billions of dollars in new SSA sensors that will be coming online in the next few years. Continued use of these outdated systems also puts additional burden on the military and civilian personnel who must still find ways to accomplish their mission of providing SSA, protecting space assets, and ensuring the warfighter in the field has access to the space capabilities they need.

Although the U.S. Air Force has announced recent changes for yet another attempt at solving this issue, it is doubtful these efforts will be successful as they are being developed and implemented under the same mindset and policy framework as the previous attempts. Moreover, they are being formulated and led by the military procurement community that has seldom demonstrated an ability to deliver major defense procurements on time and cost, particularly for software-intensive procurements such as those required for improving the core SSA IT systems.

Recommendation and Challenges

Primary Recommendation: Adopt a more open approach to developing astrodynamic standards and SSA requirements; expand the community of interest to involve all stakeholders, including commercial and foreign entities; and hold public competitions to evaluate and choose new algorithms.

The primary recommendation of this white paper is for the U.S. government to adopt a more open approach to developing astrodynamic standards and SSA capabilities that involves all stakeholders, including commercial and foreign entities and the domestic and international astrodynamics research community. A key part of this more open approach is to hold public

competitions to evaluate and choose new astrodynamics algorithms, similar to the method used to develop and evaluate cryptographic algorithms.

In making this change, there are two key challenges that the U.S. government will need to address, which currently contribute to why the United States cannot meet its SSA goals.

Challenge 1 – The U.S. Military's role as primary provider of American SSA capabilities

In the beginning of the Space Age, it made sense for the military to take the lead role in space surveillance. The military was the dominant player in space, was the only one with the resources and incentive to develop space surveillance capabilities, and the threat of attack from or through space was real. Today, the world has changed. There is a proliferation of national and international civil and commercial actors in space, all of whom need basic information and tools to operate safely in space. Providing such services is not a core military function, and attempting to do so redirects scarce resources from more critical military and intelligence pieces of SSA that are essential to national security. It also burdens the military with a task that requires agile development of IT systems, developing and maintaining a stable cadre of experienced technical and analytical experts, flexibility in dealing with a wide range of customers, and negotiating and cooperating with international entities—all tasks the military is ill-suited to perform.

Recommendation—Shift the core SSA functions necessary for safety of space activities, including management of the satellite catalog and warning of potential collisions, to a non-military entity. Refocus the Department of Defense's efforts on those aspects of SSA that are primarily military and national security missions such as collecting intelligence; determining intent, capabilities, and limitations; and protecting critical national security satellites.

Challenge 2 - The existing U.S. policy to classify and protect the location and existence of a significant number of national security payloads

Since the 1960s, the United States has had a strong tendency to try and protect its military activities in space due to a number of national security and political factors. From the beginning, satellites have played a crucial role in conducting intelligence, surveillance, and reconnaissance that have been a cornerstone of U.S. national security. The desire to protect these capabilities has led the United States to adopt policies that restrict the information available about many national security satellites, including their location in space. Over time, the efficacy of these policies has degraded as other countries, commercial and scientific entities, and even private citizens have developed methods for observing and identifying satellites. At the same time, these policies have increasingly become an obstacle to efforts both to upgrade and replace core IT systems used for SSA and improve collaboration and sharing with commercial and international partners. The classification policy hinders the ability of the United States to improve its SSA capabilities and drive commercial and foreign entities away from reliance on U.S. capabilities and in search of alternatives.

Recommendation—Declassify the orbital existence and location of U.S. national security satellites that are easily discovered and tracked, such as large satellites in low Earth orbit (LEO) or broadcasting satellites in geostationary Earth orbit (GEO), while maintaining the classification of their capabilities and limitations and taking steps to limit the impact of this change to operational security.

Adopting a more open approach and addressing these challenges, through adopting these recommendations or otherwise, is important for enabling the United States to improve its SSA capabilities and meet national policy goals, but they are not sufficient by themselves. The United States still needs to work with other governments and satellite operators on ways to collaborate and share critical SSA data both on active satellites and space debris to ensure that all space actors have the data and analysis tools they need to operate safely and efficiently in space. The U.S. military needs to develop the complementary data sources, analytic tools, and relationships with key partners and allies to ensure that it can detect and characterize attacks against critical U.S. space systems and defend those systems.

The ultimate goal for all stakeholders should be ensuring the long-term sustainability of Earth orbit so that humanity can continue to derive great benefits from space. Improving SSA is the foundation to acting responsibly in space and helps to prevent mishaps, misperceptions, and mistrust. By making space safer and more sustainable, we can ensure that the United States and the world can continue to develop innovative ways to use space through new business models, technological progress, and economic development that will inspire and benefit humanity for generations to come.

INTRODUCTION

The Importance of SSA and Current Shortcomings in the U.S. Military's Approach

The United States, and indeed the world, is increasingly reliant on satellites in orbit around the Earth. The total value of the space economy is currently estimated at $290 billion[1], which does not account for the large number of public goods such as national security, disaster warning and management, and environmental monitoring systems that also rely on satellites. Over the last several years, there has been increased concern about the ability to protect critical satellites from manmade and environmental threats, as well as about the long-term sustainability of the most highly used regions of Earth orbit.

A key enabler for protecting satellites and ensuring the long-term sustainability of Earth orbit is space situational awareness (SSA). SSA is a complex topic that means many things to many people, but can be generally defined as information about the space environment and activities in space that can be used to operate safely and efficiently; avoid physical and electromagnetic interference; detect, characterize and protect against threats; and understand the evolution of the space environment. SSA includes warnings about potential collisions between objects in space, solar storms and other types of space weather that could impact satellites or the Earth, and space-based threats to Earth (including re-entering space debris and nuclear warheads).

The U.S. government considers SSA to be an important national security priority. Top level policy documents highlight the importance of SSA and direct policy goals for improving it. The 2010 U.S. National Space Policy (NSP) states that the United States shall:

> *Develop, maintain, and use space situational awareness information from commercial, civil, and national security sources to detect, identify, and attribute actions in space that are contrary to responsible use and the long-term sustainability of the space environment;*[2]

The 2011 National Security Space Strategy (NSSS) provides further direction and guidance to the U.S. Department of Defense (DoD), which oversees SSA operations for the United States:

> *Shared awareness of spaceflight activity must improve in order to foster global spaceflight safety and help prevent mishaps, misperceptions, and mistrust. The United*

[1] Boucher, M. (2012, April 5) The Space Report 2012: The Authoritative Guide to Global Space Activity Reveals 12.2 Percent Global Space Industry Growth," SpaceRef.com Retrieved from: http://spaceref.com/event/28th-national-space-symposium/the-space-report-2012-the-authoritative-guide-to-global-space-activity-reveals-122-percent-global-sp.html

[2] White House. (2010). United States National Space Policy. Retrieved from www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

States is the leader in space situational awareness (SSA) and can use its knowledge to foster cooperative SSA relationships, support safe space operations, and protect U.S. and allied space capabilities and operations.

DoD will continue to improve the quantity and quality of the SSA information it obtains and expand provision of safety of flight services to U.S. Government agencies, other nations, and commercial firms. DoD will encourage other space operators to share their spaceflight safety data. DoD, in coordination with other government agencies, will seek to establish agreements with other nations and commercial firms to maintain and improve space object databases, pursue common international data standards and data integrity measures, and provide services and disseminate orbital tracking information, including predictions of space object conjunction, to enhance spaceflight safety for all parties.[3]

The U.S. military has responded to this policy guidance by increasing the priority of SSA and dedicating increased resources to the SSA mission. Air Force Space Command's (AFSPC) 2012 list of top space and cyber priorities ranks SSA at number four, behind only nuclear survivable communications, launch detection and missile tracking, and position, navigation, and timing services.[4] The U.S. military has also increased its current and planned spending on SSA. Figure 1 is a summary of spending by the DoD on SSA-related investments between 2008 and 2015. The investments are grouped into spending on new sensors, command and control of SSA sensors and space assets, life extension programs for existing SSA sensors, and other related investments such as research, development, test, and evaluation (RDT&E) of new technologies or risk mitigation programs. In total, the U.S. military plans to spend more than $4 billion on SSA through 2015, two-thirds of it allocated for new sensors.

Despite this recognition of the importance of SSA and the high-level policy guidance directing improvements in SSA capabilities and increased sharing with other actors, there has been little progress over the last decade in solving some of the core problems, and in particular, replacing the two systems at the heart of SSA—the Space Defense Operations Center (SPADOC, pronounced "spay-dock") and the Correlation, Analysis, and Verification of Ephemerides Network (CAVENet). These two systems are used to create much of the data and analysis that form the foundation of the entire SSA effort, including processing observations on objects in orbit around the Earth, maintaining catalogs of space objects, and using these catalogs to perform analyses such

[3] Department of Defense. (2011, January). National security space strategy, unclassified summary. Retrieved from: http://www.dni.gov/reports/2011_nationalsecurityspacestrategy.pdf

[4] Space and Cyberspace Priorities, United States Air Force. (2012) Retrieved from: http://www.airforce-magazine.com/SiteCollectionDocuments/Reports/2012/July%202012/Day17/071612_AFSPC_space_cyber_priorities.pdf

as predicting potential collisions between space objects[5] and detecting threats to U.S. space systems. This data is used by other government entities for a variety of functions.

Figure 1 - U.S. Department of Defense SSA-Related Investments[6]

	Fiscal Year							
	2009	*2010*	*2011*	*2012*	*2013*	*2014*	*2015*	***Total***
New sensor systems	$171.78	$253.34	$437.27	$508.26	$496.98	$495.51	$232.20	$2,595.34
Space command & control	$82.08	$136.27	$132.71	$127.64	$107.97	$159.50	$157.17	$903.34
Life extension for existing sensors	$20.18	$65.85	$50.66	$32.50	$36.88	$81.57	$104.50	$392.14
Other SSA-related investments	$122.44	$145.55	$49.55	$22.08	$22.44	$19.42	$19.74	$401.22
								$4,292.04

Dollars in millions. Fiscal year 2009 is actual funding amount; fiscal years 2010 through 2015 are budget estimates made in 2010.

Over the last twelve years, the U.S. military has proposed and initiated multiple programs to replace SPADOC and CAVENet. All of these acquisition efforts have ended in failure with little or nothing tangible delivered to the operators actually performing the SSA mission. These failures have left the entire SSA enterprise used to help protect the $290 billion space industry reliant on two obsolete computer systems dating back to the 1980s. More importantly, the severe inadequacies of these two systems prevent the U.S. military from implementing its national policy directives and making significant improvements to U.S. SSA capabilities, including incorporating new and different sources, types, and formats of SSA data; integrating SSA data with other sources; and performing high accuracy calculations in a short period of time—all of which are necessary to meet SSA policy goals.

The reliance on these legacy computer systems creates challenges in cooperating with allies, the commercial sector, and other partners, which is essential to SSA. Building a catalog of accurate positional data for space debris requires combining tracking data from a network of radar, optical, and other sensors that are geographically distributed around the Earth and in orbit. Active satellites can also be tracked using the same sensors and procedures. However, in most cases, a satellite owner-operator is able to determine the location of its satellite much more precisely than anyone else. Satellite owner-operators can use a variety of techniques, from their own transponders to on-board global positioning system (GPS) receivers to satellite laser ranging (SLR). Active satellites also present an additional complication in that they maneuver and doing so disrupts the catalog maintenance process. Using a periodic track-and-revisit approach could result in a discrepancy

[5] It is currently unfeasible to determine whether or not two objects will collide in space with certainty. Instead, the standard procedure is to determine the probability that a conjunction (close approach) between two objects could result in a collision, and that probability is used for a risk analysis

[6] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Data compiled from Appendix III. Retrieved from: http://www.gao.gov/assets/320/318942.pdf

between the cataloged location of a satellite that has maneuvered and its position in reality for a period of time, particularly if it is conducting a series of significant maneuvers such as transitioning from a geosynchronous transfer orbit (GTO) to its final slot in the operational geostationary Earth orbit (GEO) belt. Thus, positional data from satellite owner-operators is complementary to that collected by sensor networks and an important part of SSA.

Although it is technically feasible for one State to build the network of sensors required to accomplish tracking debris objects in orbit, the economic cost of doing so is prohibitive. Such a network would also be constrained to geographic locations owned by that State or by States that are amenable to entering into basing or other agreements. It is likely that the political issues stemming from these basing requirements would result in a set of suboptimal choices for sensor locations. Operations at geographically remote sites require complicated logistics, imposing additional costs and complexities. Thus, international cooperation on SSA and data sharing between governments and satellite operators is required to establish the level of SSA necessary to meet national policy objectives.

There are also indications that American SSA capabilities are degrading, in part because of the continued reliance on SPADOC and CAVENet, which are holding back progress and improvements. One indicator is the inaccuracy of the number of active satellites currently in orbit as reported by U.S. officials. In testimony before Congress in 2009, Lieutenant General Larry James, then Commander of Joint Functional Component Command for Space (JFCC Space) and responsible for the Joint Space Operations Center (JSpOC) which oversees all U.S. military SSA activities, stated that the U.S. military was tracking 1,300 active satellites in orbit.[7] This is significantly more payloads than the most accurate open source estimate at the time of just under 900 active satellites.[8] More recent public speeches by U.S. military officials have used an estimate of 1,100 active satellites,[9] a significant change from just a few years previous that cannot be explained by changes in the real satellite population. Meanwhile, the same open source estimate stands at 999 as of April 1, 2012.[10] Another indicator is an annual report by the European Space Agency (ESA) on the geosynchronous region that lists 66 objects that are tracked by non-American telescopes, but do not exist in the U.S. military's satellite catalog.[11] Certain individuals

[7] James, L. (2009, April 28). Statement of Lieutenant General Larry James, Commander Joint Functional Component Command for Space, Before the Subcommittee on Space and Aeronautics, House Committee on Science and Technology. Retrieved from: http://gop.science.house.gov/Media/hearings/space09/april28/james.pdf

[8] Weeden, B. (2009, July 13) "The Numbers Game," *The Space Review*. Retrieved from: http://www.thespacereview.com/article/1417/2

[9] Opall-Rome, B. (2012, February 13) "U.S. Wants a Space Debris Hotline With China Patterned on the One With Russia." *Space News*. Retrieved from: http://www.spacenews.com/policy/120213-space-debris-hotline-china.html

[10] Union of Concerned Scientists. (2012, April, 1). UCS satellite database. Retrieved from http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html

[11] Flohrer, T. (2012, February 17). "Classification of Geosynchronous Objects." European Space Agency, European Space Operations Centre.

with a background in SSA periodically provide the U.S. military with lists of dozens to hundreds of errors in the satellite catalog for correction.

Additional data points have been provided by commercial satellite operators. Over the last few years, major commercial satellite operators such as Intelsat and SES have repeatedly pointed out errors in the U.S. military satellite catalog, such as their satellites being misidentified with other satellites or even pieces of debris (so-called "cross-tags"). The unresponsive or slow responding nature of the U.S. military to correcting these mistakes as well as providing the SSA information commercial satellite operators need for safety of flight prompted three of the largest operators to form the Space Data Association (SDA).[12] The SDA operates its own Space Data Center (SDC) that provides physical and radiofrequency interference warning services to participating satellite operators.

In February 2012, Intelsat announced results from an internal study of the Conjunction Support Messages (CSM) provided by the U.S. military to all satellite operators as part of their SSA Sharing Program.[13] The Intelsat study concluded that the CSMs provided by the U.S. military had nearly a 50 percent false positive rate (half of the warnings were issued when there was not actually a potential collision) and a 50 percent false negative rate (warnings were not issued for half of the actual close approaches).[14] The primary reason for these errors was the U.S. military's lack of information about future planned maneuvers by satellite operators that disrupt conjunction assessment predictions into the future – operators have determined that the positions the JSpOC has on their active satellites are about a week behind in reflecting maneuvers.[15] This lack of information is due to the inability of SPADOC or CAVENet to ingest future planned maneuvers in an automated manner and to the lack of communication between satellite operators and the JSpOC. In response, the U.S. military informed the satellite operators that the CSMs were of an "advisory and informational" nature only and are not actionable.[16]

These shortcomings in the U.S. military's current SSA capabilities have not gone unnoticed. An increasing number of satellite operators, both private and governmental, are joining the SDA largely because they believe the SDA either offers a better product or is more responsive to their needs than the JSpOC. As of Feb. 23, 2012, 22 satellite operators controlling 237 satellites in Geosynchronous Earth Orbit (GEO) and 100 satellites in Low Earth Orbit (LEO) were members

[12] Space Data Association. (2012) Retrieved from: http://www.space-data.org/sda/
[13] Details on the U.S. military's SSA Sharing Program can be found in SWF's SSA Sharing Program Issue Brief, available from http://swfound.org/media/3584/ssa_sharing_program_issue_brief_nov2011.pdf
[14] Morring, F. (2012, February 24). "USAF satellite-conjunction advisories called inaccurate." *Aviation Week & Space Technology*. Retrieved from http://www.aviationweek.com/Article.aspx?id=/article-xml/awx_02_24_2012_p0-429306.xml
[15] Sanders, S. (2012) "SDA Update for WBU-ISOG". Presentation given at the World Broadcasting Unions International Satellite Operations Group (WBU-ISOG) Forum, May 30-31, 2012, New York, New York, USA. Retrieved from: http://www.nabanet.com/wbuarea/library/docs/isog/presentations/2012A/1.4.1%20SES%20(Sanders).pdf
[16] Ibid.

of the SDA.[17] On May 22, 2012, it was announced that the U.S. National Oceanic and Atmospheric Administration (NOAA) had joined the SDA,[18] and on Aug. 8, 2012, the National Aeronautics and Space Administration (NASA) announced it was also joining.[19]

Finally, as we look towards the future, there is a growing role for SSA in helping to ensure the long-term sustainability of space activities and international stability. Ten nations have developed the capability to place objects into Earth orbit and more than 60 nations and international organizations currently operate the nearly 1,000 active satellites.[20] The number of human-created objects in Earth orbit larger than 10 centimeters in diameter currently being tracked has gone from zero in 1956 to more than 21,000.[21] Several hundred thousand additional pieces between 1 and 10 centimeters are largely untracked, yet pose a threat to active satellites.[22]

These numbers will only grow as more countries realize the benefits from space and launch and operate more satellites. Currently, many satellite owner-operators conduct their activities in orbit without knowledge of the objects around them or the space environment. This combination of congestion and lack of information can lead to incidents in space such as the February 2009 collision between the American Iridium 33 and Russian COSMOS 2251 satellites that created nearly 2,000 trackable pieces of debris in orbit.[23] Thus, there is a need to provide all satellite operators with the basic information necessary to operate in a safe and efficient manner, and currently the U.S. military is unable to serve this role largely because of the shortcomings of SPADOC and CAVENet.

Aside from those operating responsibly in space, there is also a concern about irresponsible actors and actions that could have negative consequences for all space activities. Although SSA by itself cannot prevent irresponsible behavior, it can serve as both a deterrent and a way to detect and attribute irresponsible actors and actions. In conjunction with efforts underway to establish best practices and norms of behavior in space, SSA can help responsible space actors pressure others into acting responsibly and provide the evidence necessary to take action when they do not.

[17] DalBello, R. (2012, February 23) "The Space Data Association" Retrieved from: https://acc.dau.mil/adl/en-US/503709/file/63091/SDA.120223.pdf

[18] Space Data Association. (2012, May 22) "Space Data Association: NOAA to Participate in the SDA." Retrieved from: http://www.space-data.org/sda/wp-content/uploads/downloads/2012/05/SDA-release_NOAA_120522.pdf

[19] Space Data Association. (2012, August 8) "Space Data Association: NASA to Participate in the SDA." Retrieved from: http://www.space-data.org/sda/wp-content/uploads/downloads/2012/08/SDA_NASA_PR_8AUG2012_RELEASE.pdf

[20] Union of Concerned Scientists. (2012, April, 1). UCS satellite database. Retrieved from http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html

[21] National Aeronautical and Space Administration. (2012, March) "Orbital Debris Frequently Asked Questions." Retrieved from: http://orbitaldebris.jsc.nasa.gov/faqs.html

[22] Ibid.

[23] Weeden, B. (2010, November 10). "2009 Iridium-Cosmos Collision Fact Sheet" Secure World Foundation. Retrieved from: http://swfound.org/media/6575/2009_iridium-cosmos_factsheet.pdf

SSA will also play an increasingly important role in international security and stability. As more countries rely on space capabilities for national security, there is an increasing chance that mishaps, misperceptions and mistrust could spark or escalate conflict between States. Providing more countries with increased SSA from a reliable and trusted source can help prevent this from happening. Having the U.S. military as the main provider of SSA for the world undermines the credibility of the information it provides, both because of those who do not trust the U.S. military and its penchant for only revealing information when it is in the United States' best interests.

It is important to note that the SDA is also not the ultimate solution to the SSA problem. While the SDA does a very good job of gathering positional information from participating satellite operators and uses strong analytical techniques, it does not have the most accurate information on space debris. That information remains in the hands of the United States and other governments, who likewise do not have the most accurate information on the location of and planned future maneuvers for active satellites other than their own. The SDA has been in negotiations for more than 2 years with the U.S. government about sharing data with no resolution on the horizon, in part because of the shortcomings of SPADOC and CAVENet to accept and process operator data, but also because of national security concerns. As a result, neither party has the full set of information needed to make accurate and reliable decisions regarding safety of spaceflight and in particular avoiding collisions.

The purpose of this report is to provide an overview of the core SSA function of building and maintaining a catalog of space objects and of the legacy systems currently used by the U.S. military to accomplish that task. The report will then provide a summary of 12 years' worth of work to replace those legacy efforts, why they failed, and recommend a new approach to developing core SSA capabilities. In addition, this report discusses two major challenges that will need to be addressed in order to make the changes necessary to develop the SSA capabilities required for the United States to meet its stated national policy goals.

OVERVIEW OF U.S. MILITARY'S SSA EFFORTS

A short history of SSA activities by the U.S. military

Although there are many parts of the U.S. government that perform various SSA functions, the bulk of the SSA mission has been assigned to the military, and the JSpOC at Vandenberg Air Force Base in California is currently the hub. Run by U.S. Strategic Command (USSTRATCOM) and staffed by military members from all services and a few foreign allies, civil servants, and private sector contractors, the JSpOC is responsible for the operational employment of worldwide joint space forces and enables integration of space power into global military operations.[24]

As part of this mission, the JSpOC is responsible for providing SSA for the U.S. military and maintains the U.S. military's satellite catalog of manmade objects in orbit around the Earth and provides portions of the data and analyses to other U.S. government entities and the world. Although there is much more to SSA than just the satellite catalog, it is the catalog that provides the foundation upon which everything else is built.

A satellite catalog is a database that contains a list of objects in orbit, information about those objects such as date and country of launch, and orbital data that describes the position of the object. There are multiple satellite catalogs in use across the world, but the most well-known and publicly available catalog is the one maintained by the U.S. military, traditionally referred to as the SATCAT and more recently as the SATC (military shorthand for satellite catalog). The U.S. military produces the SATC through a process of "cradle to grave" surveillance, meaning that they attempt to maintain an orbital history of an object from the moment it is launched to the moment it re-enters the Earth's atmosphere.

It should be noted that this does not mean every object is continuously tracked all the time. Active satellites under control often provide their owner-operator positional information via telemetry, but for all other objects, the technique employed is one of periodic spot checks to determine an object's position at various points. While continuous tracking of all debris objects in space is desirable, for the time being, it is far beyond anyone's technical and financial capability.

The entire process of building and maintaining a satellite catalog starts with data coming from a network of sensors.[25] The U.S. military operates a worldwide network of optical and radar sensors called the Space Surveillance Network (SSN).[26] Raw data from SSN sensors flows into the JSpOC

[24] United States Air Force. (2008, June 6). "Joint Space Operations Center Fact Sheet." Retrieved from: http://www.vandenberg.af.mil/library/factsheets/factsheet.asp?id=12579

[25] More details on the process of initially detecting a new object and catalog maintenance can be found in the article "The Numbers Game" available at http://www.thespacereview.com/article/1417/2

[26] More information about the SSN and SSA capabilities in other countries can be found in SWF's Space Situational Awareness Fact Sheet, available from http://swfound.org/media/1800/ssa_fact_sheet.pdf, and at the Global Space Situational Awareness Sensor Database at http://globalssasensors.org/

where they are collated and, through a series of calculations, turned into a set of parameters called an element set that describe the locations and movement of an object in orbit. Two commonly used element sets are Two-Line Elements (TLEs), which describe an orbit using the six Keplerian parameters[27], and state vectors, which describe an orbit using an x-y-z coordinate system. Elements sets are useful because they allow the user to propagate an object's position forwards and backwards in time to see where it was in the past or will be in the future.

Once initially detected, a sensor collects a series of observations, called a track, on a space object as it passes through the coverage of that particular sensor. These observations are used to determine an element set describing the object's orbit. However, at this point, the element set is usually very inaccurate since it only has one track of data covering only a small section of the orbit, so subsequent sensors are tasked to collect additional observations on the same object. As more tracks are collected from different points around the object's orbit, it becomes more and more refined. Once this positional accuracy reaches a certain quality, the element set is then ready to be entered into the catalog.

These element sets are constantly updated through a process known as catalog maintenance to make sure that they are as accurate and current as possible. An algorithm incorporates the number of tracks per day needed to maintain the desired accuracy, the priority of various types of objects, the rate of change of their orbits due to natural perturbations, accuracy and capacity of various sensors in the network, and their availability to create a master tasking list for the following day.[28] Each sensor is then given a list of objects to track over the next day and instructions on how many observations to collect. As they collect and send their observations to the central processing hub, the element sets for all the objects are updated and the process repeats. An important piece of this process is the association of new observations with existing objects in the catalog or for detecting potential new objects that need to be added.

The JSpOC uses many computer systems to perform its mission, but there are only two main ones that are used in this process of creating and maintaining a satellite catalog. The first is SPADOC. Development of SPADOC began in the early 1980s by the Ford Aerospace Corporation, with SPADOC version 4C being made operational in the 1990s. SPADOC has many computational and analysis functions, including sending element sets and other data to the SSN, processing observations from the SSN, and updating and maintaining the SATC.

The SPADOC system consists of two IBM 3090-200J mainframes, one active and one backup, that handle all of the processing and a number of client workstations for viewing data and entering

[27] The six classic Keplerian parameters to define the location of an object in orbit around the Earth are: semi-major axis, inclination, eccentricity, right ascension of the ascending node, argument of perigee, and true anomaly. In some cases period, apogee, and perigee are given in place of semi-major axis.

[28] Wilson, B. (2004) "Space Surveillance Network Automated Tasker." Paper presented at the 14th AAS/AIAA Spaceflight Mechanics Meeting, February 8-12, 2004, Maui, United States.

commands.[29] Unveiled in 1985 and in production through 1989, the 3090-200J has two central processing units (CPUs) running at 69 MHz and producing computing power of 276 million floating point operations per second (MFLOPS).[30] For comparison, modern web servers commonly have four multicore processors running at 1.5 to 2 Ghz and delivering a computing power measured in more than 40,000 MFLOPS. Figure 2 summarizes the performance of SPADOC, CAVENet, and a modern commodity web server available in 2006.

Figure 2 - Comparison of SPADOC and CAVENet Servers with Modern Servers

System	Processors	Year Released	Processing Speed (MHz)	Number of Transistors (millions)	Processing Power (MFLOPs)
SPADOC 4C	2 IBM 3090-200	1989	69	not available	276 [31]
SGI Origin 3400	28 R-12000	1998	400	7.5	22,400 [32]
Modern Web Server	4 Intel Dual Core Itanium 2	2006	16,700	592	45,000 [33]

Because of this severely limited processing power, the SATC maintained by SPADOC only contains low accuracy general perturbations (GP) element sets for the 21,000 or more objects contained in it. More accurate element sets can be calculated by SPADOC on an individual basis to support specific analyses such as determining atmospheric re-entry. However, SPADOC is limited to only a few hundred of these element sets at any given time, and the vast majority of the sensors in the SSN cannot process the higher accuracy element sets. In addition to these computational limitations, the SPADOC user interface predates modern graphical user interfaces and is notoriously difficult to learn, requiring the user to memorize numerous three-letter commands.[34]

To address this and other shortcomings with SPADOC, analysts performing the space surveillance mission in Cheyenne Mountain began building a second system known as the Correlation,

[29] Weeden, B. & Cefola, P. (2010, July). Computer systems and algorithms for space situational awareness: History and future development. Paper presented at the 12th International Space Conference of Pacific-basin Societies, Montreal. Retrieved from http://swfound.org/media/15742/computer%20systems%20and%20algorithms%20for%20space%20situational%20awareness%20-%20history%20and%20future%20development.pdf

[30] Longbottom, R. "Computer Speed Claims 1980 to 1996." Retrieved from: http://www.roylongbottom.org.uk/mips.htm#anchorIBM8

[31] Ibid.

[32] SGI. (2001, February 7) "SGI Origin 3000 Series Technical Configuration Owners Guide." Retrieved from: http://techpubs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=hdwr&db=bks&srch=&fname=/SGI_EndUser/Or3000_TCM/sgi_html/ch02.html

[33] "Forthcoming Dual-Core Intel Itanium Processor Achieved Fastest Four-Way Floating Point Benchmark" (2005, July 7). Retrieved from: http://www.intel.com/pressroom/archive/releases/2005/20050707corp.htm

[34] Smith, R. (1999, March 22) "Human Machine Interface Incidents: The SPADOC Story." Retrieved from: http://www.fas.org/spp/military/program/track/spadoc4c.htm

Analysis, and Verification of Ephemerides Network (CAVENet) in 2000.[35] The system consisted of a network of more than 40 Silicon Graphics, Inc. (SGI) workstations and a few Silicon Graphics servers. The servers include SGI Origin 2000s with 8 R-12000 processors and SGI Origin 3400 with 28 R-12000 processors, providing 6,400 MFLOPS and 22,400 MFLOPS, respectively. Although still obsolete by today's standards, CAVENet does offer substantially more computing power than SPADOC. Combined with the flexibility to develop and implement software much faster than on SPADOC, CAVENet quickly became an essential tool for performing orbital analysis.

Since the mid-2000s, CAVENet's role has grown beyond just offline analysis. A number of mission-critical functions have been implemented on CAVENet by a software package known as the Astrodynamic Support Workstation (ASW). This includes updating and maintaining the high accuracy catalog (HAC), which contains special perturbations (SP) state vectors on all objects currently tracked by the U.S. military. The state vectors in the HAC (sometimes also referred to as the space high accuracy catalog or SHAC) are created using the same sensor observations as used in SPADOC but with SP models for atmospheric density and satellite perturbations. Crucially, the HAC also includes covariance information for the state vectors, which provides an assessment of the error in the satellite's location.

The HAC is used to perform more detailed conjunction analysis screening than what is possible with the GP TLEs. In addition to being more accurate, the covariance information allows for a probability of collision to be calculated. The HAC is also used to develop the daily tasking for the SSN using a package known as the SP Tasker.[36] In recent years, maintaining CAVENet has become an increasing challenge. SGI filed for Chapter 11 bankruptcy on April 1, 2009, and many of the replacement parts needed for CAVENet are only available through secondhand sources such as eBay.

For a number of technical and bureaucratic reasons, CAVENET is not allowed to directly communicate with the SSN or many other U.S. government systems that periodically require SSA information. There are also other critical SSA and space control functions that only SPADOC can perform. Thus, both SPADOC and CAVENet are required for the U.S. military to perform its SSA mission. These two obsolete systems form the backbone of protecting nearly $300 billion worth of assets in space and many critical national security functions.

[35] Stringer, M. & Teets, B. (2000, October 23). "Tools and Databases Used to Maintain the Space Catalog at 1 CACS," paper presented at the Fourth US/Russian Space Surveillance Workshop, US Naval Observatory, Washington, DC.

[36] For more details on the historical sensor tasking process and the SP Tasker, see Miller, J. (2007) "A New Sensor Allocation Algorithm for the Space Surveillance Network." Military Operations Research 12(1), 57-70.

SSA Data Sharing Initiatives by the U.S. Government

Since 1958, the U.S. military has shared data on objects in orbit with the world. Initially, this was accomplished through NASA Goddard Space Flight Center's Orbital Information Group (OIG), which took TLEs from the North American Aerospace Defense Command (NORAD) and made them available to the public.[37] In recent years, the U.S. military has started to update, formalize, and expand this data-sharing to address new concerns. The first major shift was the creation of the Commercial and Foreign Entities (CFE) Pilot Program. Established by order of President George W. Bush and authorized by legislation in 2004, the CFE Pilot Program operated with the "overarching goal…to engage the U.S. on the world stage to encourage international cooperation and transparency with foreign nations and/or consortia on space activities that are of mutual benefit." This meant that the United States would "provide SSA information to…mission partners [in order] to protect manned spaceflight, prevent on orbit collisions, and minimize the debris field surrounding the Earth."[38]

On January 3, 2005, U.S. AFSPC launched the CFE Pilot Program website (www.space-track.org), hereafter referred to as Space Track. Space Track took over the role of providing TLEs produced by the SCC to the public from the NASA OIG website.[39] In 2009, after the transfer of the operational SSA mission to USSTRATCOM and the creation of JFCC Space, USSTRATCOM assumed responsibility for the CFE program.[40] This reflected the U.S. government's position that data sharing policy should be set by STRATCOM, not AFSPC, effectively inspiring a transfer of operational control in an overall push by the DoD to consolidate SSA efforts. The name of the program was changed from the CFE Pilot Program to the SSA Sharing Program during this transfer because partners felt the previous title implied they were passively consuming information from the U.S. government. The SSA Sharing Program aims to "create transparency of satellite information" and "promote space flight cooperation and safety" by enhancing the availability of this information to partners.[41]

The Space Track website provides access to TLEs for more than 16,700 cataloged objects on orbit, as well as other information, such as date of launch, launching state, and in some cases the size of object as determined by radar cross section (RCS).[42] Space Track also provides some information on the predicted atmospheric re-entry of space objects in the process of terminal decay.

---

[37] Spillar, C. & Pirtle, M. (2009) "Commercial and Foreign Entities (CFE) Pilot Program Status Update and Way Ahead." Paper presented to Advanced Maui Optical and Space Surveillance Technologies Conference, Sep. 1-4, 2009.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Helms, S. (2010) "Space Situational Awareness." Presentation to the United Nations Committee on Peaceful Uses of Outer Space, June 3, 2010.
[42] Much of the Space Track information is republished at Celestrak (http://www.celestrak.com)

As part of the SSA Sharing Program, the JSpOC also provides a conjunction analysis (CA) service for all satellite operators that provides warning of close approaches between an operational satellite and another object in the catalog. These warnings take the form of a Conjunction Summary Message (CSM), a text message that contains details about the conjunction. Crucially, the CSMs are based on analysis done using the HAC and are much more accurate than analysis done using the TLEs publicly available on Space Track. Organizations that are members of the SSA Sharing Program and have signed a data sharing agreement with USSTRATCOM can also receive more details about the conjunction and additional services to help plan any collision avoidance (COLA) maneuver the satellite operator wishes to conduct.[43]

Although the SSA Sharing Program is useful to satellite operators, it does not fully solve the problem. Providing satellite operators with CSMs instead of sharing the HAC allows the U.S. military to more tightly control the data, but it makes all the satellite operators reliant on the JSpOC for warnings about potential collisions with debris. This in turn increases the workload on the legacy IT systems at the JSpOC that were not designed with these services in mind. The technical limitations of SPADOC and CAVENet, in particular their inability to accept many forms of operator positional data and the lack of computational horsepower, create significant challenges for the operators at the JSpOC in supplying the SSA Sharing Service. This has led to frustration and tensions on both sides.

Efforts to replace SPADOC and CAVENet

Between 1958 and 1960, the tracking of space objects was divided between three organizations: the U.S. Air Force Air Research and Development Command, the Advanced Research Projects Agency, and the U.S. Navy Space Surveillance Network.[44] In 1960, Secretary of Defense Thomas Gates established a single integrated network, the Space Detection and Tracking System (SPADATS) that combined Air Force and Navy efforts under the operational control of NORAD.[45] Eventually, separate centers for space defense and space surveillance were established in Cheyenne Mountain Air Station in Colorado. In 1994, these centers were combined to form the Space Control Center (SCC).[46]

Through the 2000s, Schriever Air Force Base in Colorado was the designated training location for crew members operating SPADOC and CAVENet in the SCC. At that time, the 1st Space Control Squadron (1 SPCS) was responsible for maintaining the satellite catalog and performing other

[43] Bird, D. (2010) Comments given to the conference "Improving Our Vision IV: Linkages and Opportunities," co-hosted by Secure World Foundation, Inmarsat, the Eisenhower Center for Space and Defense Studies, and Intelsat, June 21-22, 2010

[44] Deist, D. (1998) "Cheyenne Mountain Operations Center (CMOC) Space Control Improvement Initiatives." Paper presented at the 16th Annual Lincoln Space Control Conference, Lexington, Massachusetts, U.S.A., April 14-16, 1998.

[45] Ibid.

[46] Ibid.

space surveillance activities in the SCC. Military personnel arriving for training on SPADOC and CAVENet in 2004 were told not to get too comfortable with SPADOC and CAVENet because they were slated to be replaced with a system called Combatant Commanders' Integrated Command and Control System (CCIC2S, pronounced "kicks"). CCIC2S was a program created in 2000 to replace and upgrade many of the critical systems in Cheyenne Mountain across air, missile, and space warning missions. In 2000, SPADOC was processing more than 400,000 observations a day, 167 percent more than it was designed to handle.[47] CCIC2S was slated to replace SPADOC and the first phase of the space portion was due to be deployed in 2006. This never happened.

In a July 2006 report to Congress, the General Accountability Office (GAO) warned that the program was significantly over budget and behind schedule and that "none of the work on CCIC2S's critical space mission capabilities [had] been completed, and estimated completion dates for this work have yet to be determined."[48] Although CCIC2S work for the air and missile warning portions of Cheyenne Mountain operations is proceeding and delivering capabilities, the space portion was soon to be overcome by events.

On July 19, 2006, the Commander of USSTRATCOM signed the Establishing Directive for the Joint Functional Component Command for Space (JFCC Space) at Vandenberg Air Force Base. The Commander JFCC Space serves as the single point of contact for all military space matters to plan, task, direct, and execute space operations.[49] This Directive also created the JSpOC to serve as the primary SSA and Space command and control (C2) entity for the U.S. military, incorporating the functions previously performed by the SCC in Cheyenne Mountain. In September 2007, the JSpOC took operational control of the space surveillance mission from the SCC.

After CCIC2S and with the move of space operations out of Cheyenne Mountain, the U.S. Air Force initiated three separate programs to upgrade the capabilities of SPADOC and CAVENet to fit the new requirements of the JSpOC mission. The Space C2 program was created to provide the ability for the JSpOC to exert command and control over assigned space systems, while the Integrated Space Situational Awareness (ISSA) program was designed to handle the space surveillance catalog maintenance function. The Rapid Attack Identification Reporting System (RAIDRS) Block 20 system was designed to deliver a set of Defensive Space Control (DSC) capabilities, primarily for detecting and geo-locating radiofrequency interference.

[47] Government Accountability Office (2006, July). "Defense Acquisitions: Further Management and Oversight Changes Needed for Efforts to Modernize Cheyenne Mountain Attack Warning Systems," Retrieved from: http://www.gao.gov/assets/260/250753.pdf

[48] Ibid.

[49] Stewart, E. (2006, September 15) "JFCC Space Activates at Vandenberg," Vandenberg Air Force Base website. Retrieved from: http://www.vandenberg.af.mil/news/story.asp?storyID=123028342

In 2010, the U.S. Air Force combined these three programs into a single new program called the JSpOC Mission System (JMS).[50] JMS is being designed to provide Commander JFCC Space with "agile and responsive C2 capabilities to conduct 24/7 world-class space operations," including Space Command and Control, ISSA, and System Threat Assessment and Characterization (STACS).

However, the end result of these 12 years of efforts to replace SPADOC and CAVENet is underwhelming. Past and projected future spending on SSA command and control by the U.S. Air Force (USAF) is summarized in Figure 3. STRATCOM has advertised that JMS Capability Package Zero (CP 0) is now "operational" at the JSpOC and offering a number of benefits.[51] Although technically correct, many of the statements from the U.S. military regarding JMS CP 0 vastly overstate reality. JMS CP 0 consists of a rack of Hewlett-Packard blade servers originally purchased in the mid-2000s and several workstations. The software on the workstations is based on Java and allows operators to update GP element sets, view data pulled from some outside sources, and perform some basic analysis. It is rarely used by operators due to the lack of good procedures and cannot replace any of the critical functions performed by SPADOC or CAVENet for maintaining either the GP or SP catalog, conducting conjunction assessments, or creating the daily tasking. By any objective measure, the JMS CP 0 is a failed effort, spending more than $200 million to deliver an already aging hardware and software package that cannot perform any of the critical parts of the SSA mission.

Figure 3 - SSA Command and Control Investments by the U.S. Air Force since CCIC2S[52]

Cost elements/projects	*Fiscal Year*										
	2006	*2007*	*2008*	*2009*	*2010*	*2011*	*2012*	*2013*	*2014*	*2015*	***Total***
Space command and control											
JMS (RDT&E and OPAF)	0.00	0.00	0.00	0.00	136.27	132.71	127.64	107.97	159.50	157.17	**821.25**
Integrated SSA (RDT&E and OPAF)	0.00	9.76	20.55	52.20	0.00	0.00	0.00	0.00	0.00	0.00	**82.51**
Air Operations Center Weapons System – Space C2 Operations (RDT&E)	0.00	0.00	8.22	23.73	0.00	0.00					**31.95**
RAIDR Block 20 (RDT&E)	0.00	0.79	10.63	6.15	0.00	0.00					**17.57**
Total space command and control	**0.00**	**10.55**	**39.40**	**82.08**	**136.27**	**132.71**	**127.64**	**107.97**	**159.50**	**157.17**	**953.28**

Dollars in Millions. OPAF - Other Procurement, Air Force

[50] Morton, M. & Roberts, T. (2011, September). "Joint Space Operations Center (JSpOC) Mission System (JMS)." Paper presented at the 2011 Advanced Maui Optical and Space Surveillance Technologies Conference, Maui, United States. Retrieved from: http://www.amostech.com/TechnicalPapers/2011/SSA/MORTON.pdf

[51] Ibid.

[52] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Retrieved from: http://www.gao.gov/assets/320/318942.pdf

There have been signs over the last several months that Air Force leadership recognizes the need for a new plan. The Commander of Space and Missile Systems Center (SMC), Lieutenant General Ellen Pawlikowski, announced in April a reboot of the Air Force's acquisitions strategy to replace SPADOC and CAVENet in three phases.[53] Phase 1 in the summer of 2012 would finish rolling out existing work on JMS CP 0 to better "visualize information and to move information around" on monitors while still relying on legacy systems to perform the mission. Phase 2, the JMS Modernization Program, would be complete by the fall of 2014 and involve a combination of government off-the-shelf (GOTS) and commercial off-the-shelf (COTS) software to replace the legacy systems. Phase 3 would involve rolling out "a service orientated architecture" in 2015.

Time is becoming a factor in replacing SPADOC and CAVENet. Several other SSA investments are being brought online over the next few years that will greatly increase the number of objects in the satellite catalog and daily flows of observations to the JSpOC. One such investment is the $800 million Space Based Space Surveillance (SBSS) system. SBSS consists of a satellite in LEO with optical telescopes for tracking other space objects, primarily in geosynchronous orbit. A GAO study concluded in 2011 that replacing SPADOC was necessary to take full advantage of the capabilities SBSS has to offer.[54]

The second program that could potentially be impacted by the failure to replace SPADOC and CAVENet is the Space Fence—a $6.1 billion program to build two or three S-Band tracking radars around the world as a replacement for the legacy very high frequency (VHF) Space Fence built by the U.S. Navy in the early 1960s and transferred to the U.S. Air Force in 2004.[55] The Space Fence will detect, identify, and track objects as small as a few centimeters, resulting in an increase in the satellite catalog to more than 100,000 objects. SPADOC is currently limited to a maximum satellite catalog size of 69,999 objects. In 2005, a study concluded that SPADOC would not be able to handle the increased number of observations predicted to be provided by the Space Fence,[56] a finding confirmed by a 2011 GAO study.[57]

Time is running short to address the challenges between SPADOC and CAVENet and SBSS and the Space Fence. The first SBSS pathfinder satellite was launched in September 2010, with a

---

[53] Werner, D. (2012, April 2). "JSPOC Begins Three-Step Overhaul Starting This Spring." *Space News*. Retrieved from: http://spacenews.com/military/120402-jspoc-overhaul-starting-spring.html

[54] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Retrieved from: http://www.gao.gov/assets/320/318942.pdf

[55] G. Wagner (2004, October 20) "Navy Transfers Space Surveillance Mission to Air Force." Retrieved from: http://www.navy.mil/submit/display.asp?story_id=15597

[56] Government Accountability Office (2006, July). "Defense Acquisitions: Further Management and Oversight Changes Needed for Efforts to Modernize Cheyenne Mountain Attack Warning Systems," Retrieved from: http://www.gao.gov/assets/260/250753.pdf

[57] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Retrieved from: http://www.gao.gov/assets/320/318942.pdf

planned 5.5 year mission.[58] The U.S. military is halfway through this mission time and JMS has not been delivered. Until it is, the military cannot take advantage of the full capabilities of SBSS. Likewise, the first Space Fence site is scheduled to provide initial operating capability by the end of 2015 (a delay of two years from its original IOC date of 2013). In the three years between now and the beginning of the Space Fence, a solution to the SPADOC and CAVENet problem needs to be found and made operational. Otherwise, the Air Force risks its ability to get full value from the billions it is investing in other critical SSA upgrades and jeopardizing the ability of the United States to perform the SSA mission in the future.

[58] 30th Space Wing Public Affairs. (2010, September 25) "Vandenberg Launches Minotaur IV." Retrieved from: http://www.vandenberg.af.mil/news/story.asp?id=123223753

RECOMMENDATION AND CHALLENGES

The previous discussion of the catalog maintenance process and the legacy systems used to create and maintain the satellite catalog has a direct impact on both current U.S. SSA capabilities and improving them to meet stated policy goals. As long as the U.S. military is reliant on SPADOC and CAVENet, it will have significant technical limitations to its SSA capabilities.

This is not news to the U.S. military. As discussed, there have been a number of efforts over the last 12 years aimed at replacing SPADOC and CAVENet, all of which have failed. At the strategic level, these failures can be traced back to the overall approach taken by the U.S. military. It has treated the SPADOC and CAVENet replacement as traditional military acquisitions programs, which have a long track record of delivering complex software on-time and on-budget. Furthermore, all of these previous acquisitions programs have only involved a limited number of stakeholders, primarily the U.S. Air Force, in developing both requirements and technical solutions.

The second phase of the new JMS plan outlined by Lt. Gen. Pawlikowski – using a combination of GOTS and COTS to replace SPADOC and CAVENet in the short term – represents a significant shift in approach from the first iteration of JMS. Instead of previous efforts to create from scratch the hardware and software systems needed to replace SPADOC and CAVENet, this new approach will rely on taking existing government and commercial software and adapting it to the military's needs. Chief among these is a government software program known as Space Common Operating Picture Exploration System (SCOPES) and currently called ISSA.[59] ISSA is primarily a tool to visualize satellite orbits and scenarios and perform a variety of analyses. Historically, it has not had a catalog maintenance component, but that could be added by using code from other government software such as ASW. These broad strokes appear to be a feasible short-term solution to replacing SPADOC and CAVENet.

However, the third phase of the plan – developing a full-fledged service-orientated architecture by 2015 – does not appear to be a workable solution. By all accounts, it appears to be yet another attempt to accomplish the same goals as the previous failed programs without addressing any of the shortcomings of the general approach.

Chief among these shortcomings is the lack of involvement of stakeholders in the process. SSA has evolved from a function performed by the U.S. Air Force for primarily military and national security needs, to a function performed by the U.S. Air Force on behalf of the global space community for a wide variety of needs, including safety and national security. However, the

[59] This is a completely separate piece of software from the previous mention of ISSA. The first instance of ISSA was a formal acquisitions program from 2007-2010 as part of the effort to replace SPADOC, and was merged into JMS in 2010. The second instance of ISSA was a GOTS software suite called SCOPES that was renamed ISSA.

conversation about the SSA requirements, capabilities, and best way to develop those capabilities that feeds into the acquisition process remains almost entirely constrained to the U.S. Air Force.

At the centerpiece of this conversation is the discussion of astrodynamic standards and development of the core mathematical techniques used to build and maintain the satellite catalog. Astrodynamic standards are an important foundation for SSA, although there has been a difference of opinion over what is meant by the term "standard." One perspective is the development of a standard set of algorithms used to generate an element set from observations and the mathematical techniques and force models used to propagate the element set forward and backward in time. The standards ensure that such algorithms produce results at the required level of accuracy and precision and that results generated by different users are comparable. Another perspective is that standards are used to define interfaces between organizations, such as a standardized message or data format. These standards make it easier to exchange data between different systems and develop automated routines for exporting and importing data.

Since the beginning of the U.S. military's involvement in SSA, they have tended to prefer the former approach of standards as specifying a particular approach or set of tools. Currently, the Analyses, Assessments and Lessons Learned branch of Air Force Space Command Air Staff (AFSPC/A9) is responsible for creating and establishing the astrodynamics standards used in the JSpOC.[60] Per its mission, AFSPC/A9 focuses primarily on the needs of Air Force Space Command in establishing these standards. It also has a bias towards how things have been done in the past. As the SSA customer base has been expanded beyond just NORAD and Space Command to the rest of the U.S. government and now the world, the limited vision and mission of AFSPC/A9 has posed an even greater obstacle to improving SSA. Standards that meet Space Command's criteria may not be sufficient for other parts of the U.S. government, let alone the commercial and foreign operators using the JSpOC's services. Combined with the reluctance to accept new and alternative approaches to astrodynamics standards, this creates a barrier to enhancing and improving SSA sharing with other parts of the U.S. government as well as commercial and foreign entities.

More recently, a significant amount of work has taken place in international bodies such as the Consultative Committee for Space Data Systems (CCSDS) and the International Organization for Standardization (ISO) on developing standards related to SSA. These efforts have largely taken the second approach of defining interfaces and formats rather than specifying techniques, although there are differences between the two. CCSDS is comprised of space agencies, and as such has tended to push the existing U.S. Air Force standards for adoption.[61] ISO is fundamentally an industrial organization that is focused on developing commerce and commercial opportunities, and

[60] "AFSPC Astrodynamic Standard Software" (2011, March 29). Retrieved from: http://www.astrodynamicstandards.com/Resources/Astro_Stds_List.pdf

[61] Finkleman, D. (2007) "TLE or not TLE? That is the Question." Paper presented at the 17th AAS/AIAA Spaceflight Mechanics Meeting, Sedona, Arizona, United States, January 28-February 1, 2007.

as such tends to approach the astrodynamics standards problem from a more open and collaborative perspective.

Astrodynamic standards form the foundation of the software suite used to produce and maintain the satellite catalog and are driven in large part by the requirements of the end user. The astrodynamic standards currently in use by the JSpOC and planned for use in JMS do not reflect the requirements of all the end users the JSpOC desires to serve, nor do they represent the best and only method of delivering those requirements.

Main recommendation— Adopt a more open approach to developing astrodynamic standards and SSA requirements; expand the community of interest to involve all stakeholders, including commercial and foreign entities; and hold public competitions to evaluate and choose new algorithms.

Rationale for expanding the SSA community

The U.S. Air Force is not the only organization in the world with SSA capabilities, a need for SSA systems or with expertise in astrodynamics. However, the historical and current U.S. military approach to developing its astrodynamic standards and SSA algorithms is to involve only a limited pool of astrodynamics expertise from a small group of government employees and defense contractors. This has led to a narrow perspective of the problem and the pursuit of only a few techniques for solving it. For example, in the 1960s, the Soviets developed a rigorous mathematical technique for updating the orbit of a satellite in LEO from a single radar track, a technique that was relatively unknown in the United States for 30 years.[62] In contrast, the paradigm adopted by the U.S. Air Force focused on all the observations being sent to a central processing hub that updated element sets using a batch least squares method.

Likewise, the algorithms used by the U.S Air Force to propagate orbits focus on specific implementations of either analytic theory, such as the Simplified General Perturbations or SGP, or numerical theory, such as that used to produce the SP state vectors.[63] Meanwhile, an entire other class of algorithms known as semi-analytic theory were developed and used by the Russians as well as Draper Laboratory at the Massachusetts Institute of Technology (MIT).[64] Each of these approaches has various advantages and disadvantages and might be better in different situations. Yet the inclusion of only a small group of people among those who determined the astrodynamic standards for the U.S. Air Force, and thus the bulk of the U.S. military's SSA efforts, artificially

[62] Khutorovsky, Z. (2004) "Techniques and algorithms for determination of orbits of LEO satellites using measurements acquired during one penetration to the field of view of detection radar."
[63] Vallado, D. (2001) "A Summary of Astrodynamic Standards." Paper presented at the 2001 AAS/AIAA Astrodynamics Specialists Conference, Quebec City, Quebec, Canada, July 30 – August 2, 2001.
[64] Ibid.

narrowed the solution set to a limited number of possibilities and based the entire SSA effort by the U.S. military on a single approach.

As an alternative, the U.S. military should adopt a similar approach to that used to develop cryptographic standards and algorithms. The National Institute for Standards and Technology (NIST) works actively with other government and industry organizations to develop standards and guidelines for cost-effective uses of cryptography. In particular, it uses open competitions involving academia, government agencies, and the private sector to choose its cryptographic standards and algorithms. In doing so, NIST ensures that it is drawing on the largest pool of talent and innovation possible to propose standards, scrutinize them, and compare them in a competitive manner. This creates buy-in among all the stakeholders; furthermore, making the details of the winning standard publicly accessible enables cross-compatibility between different implantations. Other government organizations, such as the National Security Agency (NSA), then use the algorithms and standards developed by NIST as the foundation for U.S. government implementation.

The importance of broad and open scrutiny and evaluation of standards cannot be understated. Volumes of scientific research, economics theory on free markets, and real world business models of internet giants such as Google, Facebook, Amazon, and Wikipedia have definitively shown the power of crowdsourcing and the advantages of leveraging the wisdom of the crowd when solving large and complex problems. Few aspects of national security are more important than the strength of cryptographic algorithms, and it serves to reason that if such open competitions are used to develop cryptography, they would be useful in developing astrodynamic algorithms.

Figure 4 shows the stakeholders involved in SSA as determined by the GAO. There are at least two important groups missing from this chart. One is the U.S. Navy, which has played a significant role in American SSA since the 1960s and whose center at Dahlgren, VA, currently serves as the backup for SPADOC. A second group that is missing from this chart is the astrodynamics research community, which should be considered an important stakeholder as they play an extremely important role in developing the mathematical theories used for orbit determination and modeling.

The most important takeaway is that for the United States to have the level of SSA it requires, it must work with and exchange data with satellite operators and foreign governments, and especially those that are close allies and partners. Yet, these stakeholders have not been seriously involved in astrodynamics standards efforts to date. Thus, the "standards" that need to be developed for SSA algorithms should have input from all the stakeholders, not just those within the U.S. government.

Figure 4: Stakeholders Involved in SSA[65]

DOD

Office of the Secretary of Defense
Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Under Secretary of Defense for Policy
Assistant Secretary of Defense, Networks and Information Integration
Defense Advanced Research Projects Agency
Defense Special Missile and Astronautics Center
Director of Cost Assessment and Program Evaluation
Director of Operational Test and Evaluation
Joint Chiefs of Staff
Office of the Secretary of the Air Force
U.S. Strategic Command
Joint Functional Component Command for Space
Joint Forces Command
Pacific Command
Office of the Chief of Naval Operations
14th Air Force
Air Force Materiel Command
Air Force Intelligence, Surveillance and Reconnaissance Agency
Air Force Program Executive Officer
for Command and Control, and Combat Support
Air Force Program Executive Officer for Space
Air Force Research Laboratory
Air Force Space Command
Air Force Technical Applications Center
Electronics Systems Center, 850th Electronic Systems Group
Missile Defense Agency
National Security Space Office
Army Space and Missile Defense Command
Space and Missile Systems Center
Space Protection Office
US Marine Corp, Plans, Policies and Operations

Intelligence community

Office of the Director of National Intelligence
Central Intelligence Agency
National Air and Space Intelligence Center
Defense Intelligence Agency
National Geospatial-Intelligence Agency
National Reconnaissance Office
National Security Agency

Civil government

Department of Commerce
Department of Energy
Department of State
Department of Transportation
National Oceanic and Atmospheric Administration
National Aeronautics and Space Administration
Lawrence Livermore Laboratory
Los Alamos National Laboratory
Massachusetts Institute of Technology, Lincoln Laboratory
Sandia National Laboratory

Commercial and foreign entities

Satellite operators
Satellite developers
Foreign government space agencies

Likewise, collaboration is also critical to success. One key to the success of modern Internet companies developing and maintaining massively complex software platforms and services is community collaboration on solving challenges that everyone faces, even if they are competitors. Often this collaboration is done through open source software. In traditional closed source software, the source code that forms the basis of the software is a tightly held secret only available to a specific number of programmers officially working on the project. Open source software makes the source code freely available to anyone to view, adapt, or even suggest improvements. The open source approach greatly expands the number of people that can examine code for bugs, supply programming time to write code, and offer ideas and creative solutions for solving problems.[66]

[65] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Retrieved from: http://www.gao.gov/assets/320/318942.pdf

[66] More details about how open source could play a role in SSA is explored in Cefola, P., Weeden, B., Levit, C., "Open Source Software Suite for Space Situational Awareness and Space Object Catalog Work," 4th International Conference on Astrodynamics Tools Techniques, Madrid, Spain, 3-6 May 2010. Retrieved from: http://swfound.org/media/15745/open%20source%20software%20suite%20for%20space%20situational%20awareness%20and%20space%20object%20catalog%20work.pdf

An example of this collaboration is the work on developing database systems capable of handling billions of items across distributed architectures such as the Cassandra Project or Apache Hadoop. These databases were developed by engineers from many different companies, some of whom were even rivals. This collaboration allowed these companies to pool resources and talent to solve the problem in a more efficient and cost-effective manner than each one working alone. Another example is MySQL, a very common, extensively used open source database language. Twitter relies on MySQL heavily and contributes its own internal improvements in MySQL back into the community.[67] Twitter has also created 16 open source technologies from its own development work.[68]

Some may note that the U.S. Air Force already has a Command and Control Space Situational Awareness Community of Interest (C2/SSA COI), which on the surface appears to be a more open approach. However, it is not nearly as open as it needs to be. The official website for the C2/SSA COI is private and accessible only by those possessing U.S. government common access cards. It appears as though the "community" involved in the C2/SSA COI is only that within the United States government.

Although holding an open competition to develop new astrodynamics standards is sorely needed, it is a process that would take years to conclude. In the meantime, it is possible to shortcut the process by holding an open competition between the many existing astrodynamics algorithms to determine which one(s) is (are) best suited for various SSA tasks and thus should be incorporated into an initial short-term solution to replace SPADOC and CAVENet.

[67] "MySQL at Twitter" (2012, April 9) Twitter Engineering Blog. Retrieved from: http://engineering.twitter.com/2012/04/mysql-at-twitter.html

[68] Harris, D. "The clarity and mystery behind what makes Twitter run." (2012, August 22) Gigaom.com Retrieved from: http://gigaom.com/cloud/the-clarity-and-mystery-behind-what-makes-twitter-run/

Challenges in Implementing a More Open Approach to SSA

Implementing this primary recommendation of expanding the SSA community of interest to include all stakeholders will be difficult to accomplish due to the cultural and bureaucratic challenges that current exist with the U.S. government's approach to SSA. Two of these challenges should take priority as they drive a number of other hurdles.

Challenge 1 – The U.S. Military's role as primary provider of American SSA capabilities

Recommendation—Shift the core SSA functions necessary for safety of space activities, including management of the satellite catalog and warning of potential collisions, to a non-military entity and refocus the Department of Defense's efforts on those aspects of SSA that are primarily military and national security missions such as collecting intelligence; determining intent, capabilities, and limitations; and protecting critical national security satellites.

Background

As is the case with most new domains, SSA was primarily a military endeavor in the beginning. During the 1950s and 1960s, nuclear attack via ballistic missiles whose warheads traveled through space or even nuclear warheads deorbiting to strike targets on the ground was a possibility. The vast majority of initial SSA investments were a direct result of the military investing in missile and attack warning and many SSA sensors still serve a dual purpose for both SSA and missile warning.

While the United States and Russia still maintain large nuclear arsenals and other countries such as China have created smaller arsenals, the threat of nuclear attack today is greatly diminished. However, largely because it has always performed the mission, the U.S. military continues to be the hub for all SSA activities, even those that do not serve a military function, lie outside the common sense mission of the military, and for which the military is neither equipped nor staffed to handle. SSA to support civil and commercial safety of flight, including providing warnings of potential collisions to all the satellite operators in the world, is an example of such a function.

The expansion of the SSA customer base and an increase in the need for public safety services indicates that the military should step back from its current role and delegate the core functions of tracking objects and maintaining the satellite catalog to a non-military entity. This would require the new non-military entity to have access to at least three data sets: metric tracking data on space debris, owner-operator element sets for active satellites, and data on space weather.

Making this change would not mean eliminating the JSpOC or the U.S. military's role in SSA. Clearly, there are specific SSA activities and analyses that are necessary to support national security objectives, such as determining potential threats from space and to space assets and protecting critical national security satellites. The JSpOC should still be responsible for

performing these activities, but should do so by adding additional data sources and layers of analysis to the core satellite catalog maintained by the new non-military entity.

A reasonable analogy in this case is air traffic over the continental United States (CONUS). Day-to-day situational awareness of air traffic is managed by civil authorities under the control of the Federal Aviation Administration (FAA). U.S. Northern Command (USNORTHCOM) has responsibility for providing warning of all threats within U.S. airspace. It uses air traffic awareness data from the FAA, along with additional military resources, to accomplish this mission. Should the need arise due to changes in threat posture or indications of attack, this relationship can change to allow USNORTHCOM to respond as needed

Such a change does not mean that all military and national security satellites would be forced to reveal themselves. Under the Chicago Convention of 1944, which established the international air traffic control system, government aircraft are exempted from the air traffic regulations, but are required to operate with "due regard to the safety of civil aviation."[69] Although the vast majority of the time military and other state aircraft do follow international regulations, this exemption was critical in getting government support for the international air traffic system.

These same two principles can be adopted for SSA. Transferring the basic situational awareness responsibility to a non-military entity allows the military to focus its limited resources on those aspects of SSA necessary for national security and out of the realm of a non-military entity, such as using classified intelligence, surveillance, and reconnaissance (ISR) capabilities to characterize activities in the space domain and determine potential threats. Additionally, an exemption can be made for those national security satellites that need to operate with due regard.

Rationale for transferring core functions to a non-military entity

There are several significant reasons for shifting these core SSA responsibilities to a non-military entity. The first reason for doing so is that replacing SPADOC and CAVENet involves creating a new computer and software system, and the U.S. military has a long track record of failing IT projects. Commander of AFSPC, General William Shelton, was recently quoted in *Space News* that

> *"If you look across the entire Department of Defense, I'm not aware of a single software-based program that has gone extremely well. We do not have the recipe yet for software development - an extensive software development program that is on schedule, on budget, that produces the same capability that we originally sought."*[70]

[69] "Convention on International Civil Aviation, Signed at Chicago, on 7 December 1944 (Chicago Convention." Retrieved from: http://www.mcgill.ca/files/iasl/chicago1944a.pdf

[70] Shelton, William. (2012, April 23) *Space News* .

One reason why the DoD has this track record is because modern IT projects, and software development in particular, require a mindset and culture that is at odds with typical military procurement. The DoD tends to take a top-down approach, also known as a waterfall model,[71] to developing software that usually starts with the end user elaborating all the requirements that the final system needs to provide.[72] Only when this process is complete does the software writing begin and the customer often only sees the end result when it is finally delivered. This can be years later, at a time when some of the requirements are no longer valid or new ones have emerged. Changing requirements during the process leads to increased costs and delivery times. The lack of constant interaction and feedback between the developers and end users and the infrequency of iterations leads to failure.

Another drawback of the traditional government acquisitions approach to IT projects is to select a single prime contractor to develop proprietary software that delivers the capabilities. This locks the government into using a single service provider and provides significant economic incentives for the contractor to build inflexible, stovepiped solutions that only they can maintain.

In contrast, successful complex modern software is developed by large teams of engineers working collaboratively with extensive testing and frequent updates, typically employing iterative and incremental software development models.[73] For example, Facebook engineers are continuously writing code to fix bugs and add new features and pushing changes to the production platform every day. Netflix has developed a software tool called Chaos Monkey that randomly disables parts of its actual production servers in order to test reliability and force engineers to improve resiliency.[74] More cutting edge development teams even employ agile software development methods such as scrum that are designed to deal with situations where it is difficult to plan ahead.[75]

Such practices are part of what allows these companies to provide a staggering level of service. Facebook has more than 900 million users that add more than 500 terabytes of data every day and its total disk space is more than 100 petabytes.[76] During peak hours, Netflix accounts for more than 30 percent of all Internet downstream bandwidth in North America.[77]

---

[71] For an overview of the waterfall model see http://en.wikipedia.org/wiki/Waterfall_model

[72] A classic text on this issue, "Developing Software to Government Standards" by William H. Roetzhein (Prentice Hall, 1991), discusses how the preparation of a system or segment specification assumes that the requirements are static.

[73] For an overview of iterative and incremental software development, see http://en.wikipedia.org/wiki/Iterative_and_incremental_development

[74] Izrailevsky, Y. (2011, July 19). "The Netflix Simian Army." The Netflix Tech Blog. Retrieved from: http://techblog.netflix.com/2011/07/netflix-simian-army.html

[75] For an overview of agile scrum software development, see http://en.wikipedia.org/wiki/Scrum_(development)

[76] Kern, E. (2012, August 22). "Facebook is collection your data – 500 terabytes a day." Gigaom.com Retrieved from: http://gigaom.com/data/facebook-is-collecting-your-data-500-terabytes-a-day/

[77] Sandvine (2012) "Global Internet Phenomena Report." Retrieved from: http://www.sandvine.com/downloads/documents/Phenomena_1H_2012/Sandvine_Global_Internet_Phenomena_Report_1H_2012.pdf

The software and hardware needed to replace SPADOC and CAVENet is not especially complicated and is overall lower in complexity and scale than those problems faced, and solved, by Amazon, Facebook, Google, and many hundreds of other companies building businesses based around the Internet. A set of observations on a space object taken by a sensor is no more than a string of text, in many ways similar to an email, and the initial processing done to determine which object in the catalog those observations belong to is not especially different from modern email spam filtering. While SPADOC struggles to handle the several hundred thousand observations it receives a day, it is trivial for a fairly low-cost email server to handle the same amount of email traffic each day. Similarly, while CAVENet takes many hours to perform a conjunction analysis of all active satellites in space versus all other objects, a modern laptop can perform the same analysis in a much shorter time.

The more than a decade spent by the military in trying to replace SPADOC and CAVENet with little success is a direct indicator of how ill-suited military acquisitions programs are to deal with this sort of problem. Shifting the core SSA functions to a non-military entity would remove the cultural and bureaucratic barriers to developing successful IT systems in the military and greatly increase chances of success in replacing them. It would also free the military to focus on the aspects of SSA that are difficult and have a true national security focus, such as characterization and determining threats.

The second reason for shifting some SSA responsibilities to a non-military entity is that it would have more flexibility to hire, train, and retain experienced personnel to perform the SSA mission. Currently, the operators at the JSpOC performing the SSA mission are a mix of mostly active duty military with civil service civilians and contractors in both operational and support roles. The training and experience of these personnel is a direct limiting factor in both the quality of the satellite catalog and the ability to provide services such as conjunction warning to satellite operators. While the computers do all the heavy calculations, it is up to the human analyst to determine if the answer makes sense and is correct. Intimate knowledge of the numerical and analytical techniques behind this process is required, along with considerable experience with both conjunction analysis specifically and SSA in general.

With rare exceptions, active duty military personnel are not given the opportunity to develop the skills to perform this task well. At most, they will be in a particular location for a 3- or 4-year tour and, during that tour are likely to have multiple jobs. The military promotions system demands incremental moves within a tour to various leadership, instructor, or evaluator positions to demonstrate suitability for promotion. Staying in the same job for an entire tour is considered evidence of someone who doesn't have "the right stuff" and is a potential death knell for any career. There is also a strong prejudice against analysts in the officer rank.[78]

[78] Weeden, B. (2009, February 23) "Billiards in space." The Space Review. Retrieved from http://www.thespacereview.com/article/1314/1

It should be noted that these jobs are not done solely by officers – enlisted personnel are also assigned to these positions. And often there is no shortage of diligent and intelligent analysts coming from the enlisted ranks. That is a testament to the quality of personnel that the Air Force is able to attract and retain.

However, even if a dedicated and competent military professional is willing to sacrifice their career to spend an entire tour doing just one job, they are unlikely to have the required mathematical or analytic background for conjunction analysis. The vast majority of space operators, the career field that provides personnel to these billets, are trained to follow set procedures and given only a few months of background training before being certified. Many come from jobs other than orbital analysis and will never have to do orbital analysis again in their careers. Thus, they have neither the tools nor incentive to develop the vital mathematical and analytical skills needed for this job. Shifting the core SSA mission away from the U.S. military to an entity that can hire, train, and retain exactly the personnel needed to perform this highly technical and analytical position would go a long way toward improving the quality of services offered and SSA in general.

A third major reason to transfer some SSA responsibilities to a non-military entity is that it would be much easier to incorporate SSA data from new sensors and non-traditional sources and cooperate with commercial and foreign entities. In several other countries, SSA is either handled entirely by a civil agency or has significant portions handled by non-military agencies. For example, the development of the new European SSA Programme is led by ESA, while SSA efforts in India are led by the Indian Space Research Organization (ISRO), both civil agencies. The SSA Sharing Program's current requirement for external entities to sign a legal agreement with the military entity that also oversees America's nuclear weapons arsenal, USSTRATCOM, presents significant legal and political challenges for several commercial and foreign entities.

A fourth major reason is that there is no longer a significant cause for the U.S. military to be performing core SSA functions, such as maintaining a satellite catalog or providing collision warnings to satellite operators. Performing its core mission of defending the United States requires use of a satellite catalog and other SSA data, but does not require creating that data. In the early days of the use of space, the U.S. military was the only entity with both the need and capabilities to collect SSA data, but today that has changed. The growth of the commercial and non-military space activities has led to an increase in other entities aside from the U.S. military that are both SSA data providers and consumers. Just as it makes no sense for the military to be running the entire air traffic control network, it no longer makes sense to have the military run the entire SSA enterprise.

The creation of the SDC by the SDA is a concrete example of a non-military approach to solving at least some of these issues. The initial contract award to develop the SDC was made in the spring

of 2010, and the system achieved initial operating capability in July 2010.[79] Full operational capability, including web services, flexible software architecture, and state-of-the-art security and reliability, was achieved in September 2011.[80] In total, these efforts required fewer than a dozen highly qualified people and a relatively small investment of capital and delivered several of the improvements planned for JMS, including the ability to accept data from a variety of sources and in a variety of formats, customized warning thresholds for each user, protection of proprietary information from competitors and third parties, and greatly enhanced speed and flexibility.

Of course, it must be understood that the SDC development drew directly on all the software resources that the primary developer, AGI, was working on for a number of years such as the SOCRATES web service. Additionally, the SDC codebase is still closed-source proprietary code, which does not address some of the concerns with independent verification and transparency. Thus, while the SDC is a good example of an alternative approach to developing SSA software, it may not be the approach best suited to solving the SSA problems faced by the U.S. government.

Implementation options

Implementing this recommendation will be challenging, particularly in dealing with the tasking of the SSN, much of which is operated by the military. This is where the analogy with the air traffic system breaks down, as the FAA operates many of its own air traffic control radars. It is not practical in the short term for this new non-military SSA entity to build and operate its own sensors to replace the existing SSN. However, one possible solution would be to keep the tasking of the SSN at the JSpOC and route the observations through the existing communications channels to the new non-military entity, which would be tasked with maintaining the satellite catalog and performing conjunction assessments. Some level of screening or modification could take place to conceal sources, methods, and capabilities, but the bulk of the observations can be passed to the new entity for use in updating the catalog. Initial detection and tracking of new space launches would need to remain with the JSpOC, but once an initial orbit is determined, the new object can be handed off to the non-military entity for cataloging. Sensor tasking for catalog maintenance purposes would be done by the new entity, and passed to the JSpOC, which can then add any tasking related to military and intelligence needs before passing to the sensor network. Protocols for real-time tasking to support events such as breakups or emergencies would also need to be developed. Although there may be growing pains, none of these challenges appear to be insurmountable.

Perhaps the most challenging part of implementing this recommendation would be deciding which non-military entity these SSA responsibilities should be transferred to. From a security perspective, transferring them to another U.S. government agency is likely the preferred choice.

[79] Finkleman, D. (2012) "Commercial Collaboration for Collision Avoidance and Flight Operations." Paper presented at the 2012 SpaceOps Conference, Stockholm, Sweden, June 11-15, 2012.
[80] Ibid.

However, at the moment no other U.S. agency stands out as a good fit, including the two most likely candidates: NASA and the FAA. NASA has the operational, technical, and scientific expertise to handle the SSA mission, but comes with its own bureaucratic and budgetary challenges. Deciding which NASA center takes the SSA mission would be difficult given the existing rivalry between centers, and it is likely that the politically acceptable solution would involve splitting the SSA mission set between more than one center. That would invite disaster.

The FAA has experience and credibility in performing its duties for air traffic management, which does have some similarities to what is needed for SSA operations. However, the space divisions at the FAA are policy-centric and do not have operational or technical expertise in SSA. Giving the FAA a portion of the SSA mission would require a significant infusion of experienced personnel and a change in the current makeup of the space division.

A potential third option is to create a new entity, and a model that deserves consideration is the U.S. Coast Guard. Although technically a uniformed branch of the military, the Coast Guard has a fundamentally different mission from the rest of the U.S. military in that it has both security and safety missions. Officially, the Coast Guard fulfills three basic roles: maritime safety, maritime security, and maritime stewardship that are further divided into 11 statutory missions.[81] This maps well to the required mission set for an SSA entity, particularly if future responsibilities for space traffic management are envisioned. Creation of a "Space Guard" modeled on the Coast Guard would have the advantage of a more safety-focused mission but also not be completely severed from the U.S. military's security infrastructure.[82] However, these existing military links and the possibility of being subsumed by the military in times of war means that a "Space Guard" would pose more challenges for international cooperation and trust than a purely non-military entity.

Finally, an option that should be seriously considered is creation of a non-governmental entity to oversee these core SSA functions, and in particular, a non-governmental organization (NGO). Although some elements of the U.S. government would be uncomfortable with such an entity handling data and performing analyses with national security implications, there are benefits. An NGO is more likely to be trusted by other organizations and governments and seen as impartial. This is an important factor in using SSA for discovering irresponsible behavior in space. Other NGOs that are deeply involved in multi-stakeholder governance of critical infrastructure, such as the non-profit corporation Internet Corporation for Assigned Names and Numbers (ICANN) that runs major parts of the governance of the Internet, could serve as useful models for such entities in the SSA domain.

Challenge 2 – The existing U.S. policy to classify and protect the location and existence of a

[81] 6 U.S.C. § 468 Retrieved from: http://www.law.cornell.edu/uscode/text/6/468

[82] McKinley, C. (2000) "The Guardians of Space: Organizing America's Space Assets for the Twenty-First Century." *Aerospace Power Journal*, Spring 2000. Retrieved from: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/spr00/mckinley.htm

significant number of national security payloads

Recommendation—Declassify the orbital existence and location of U.S. national security satellites that are easily discovered and tracked, such as large satellite in LEO or broadcasting satellites in GEO, while maintaining the classification of their capabilities and limitations and taking steps to limit the impact of this change to operational security.

Background

Like space activities in general, classification of national security space activities evolved during the Cold War. At their conception under the Eisenhower Administration, the initial U.S. satellite reconnaissance efforts by the Air Force were openly acknowledged and only the specific operational details and intelligence products were classified.[83] However, there were concerns within the military and intelligence community as to whether President Dwight Eisenhower would be forced to exclude satellite reconnaissance from the definition of "peaceful activities" in order to get international acceptance of the concept.[84] At the same time, there existed a covert satellite reconnaissance program code-named CORONA managed initially by the U.S Central intelligence Agency (CIA) and later as a combined CIA-Air Force effort.

The inability of the Soviets to prevent U.S. surveillance satellites from peering deep into the Soviet Union was a significant area of tension, and the Kennedy Administration decided to make all space reconnaissance activities covert so as to give both sides plausible deniability and reduce Soviet incentives to go after these systems militarily or diplomatically.[85] Ultimately, all these factors led to the classification of the very existence of U.S. space reconnaissance efforts in September 1961 with the creation of the National Reconnaissance Office (NRO), the organization that oversees all U.S. overflight activities.[86] Additionally, the challenges in protecting certain military space programs while continuing an open launch policy led the Kennedy Administration to release DoD Directive S-5200.13 in 1962 mandating a "blackout" of all military space programs.[87]

Since the Kennedy Administration, these two policies have provided the basis for much of the approach to U.S. military activities in space, with varying impacts on the classification and release

[83] Richelson, J. T. (1998). "Out of the black: The disclosure and declassification of the national reconnaissance office." International Journal of intelligence and Counterintelligence, 11(1), 1-25. Retrieved from: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB257/index.htm

[84] Perry, R. (1969) "A History of Satellite Reconnaissance, Volume 5: Management of the National Reconnaissance Program" NRO, Washington, DC, p. 3-4

[85] Sylvester, A. (1960, August 9) "Probable Reactions to US Reconnaissance Satellite Programs." Memorandum for the President, The White House, Subject: SAMOS II Launch, 26 January 1961; Director of Central Intelligence, SNIE 100-6-60.

[86] Gilpatric, R. (1961, September 6) "Management of the National Reconnaissance Program." Letter to Allen Dulles. Retrieved from: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/05-01.htm

[87] Gilpatric, R. (1962, March 23). "Security and Public Information Policy for Military Space Programs." Department of Defense Directive S-5200.13 Retrieved from: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB225/doc14.pdf

of information about the location of U.S. national security satellites in orbit around Earth. Up until 1983, the U.S. military released positional information on all but a few U.S. satellites in highly inclined or geostationary orbits.[88] After 1983, this policy was modified to restrict the distribution of positional information on many more U.S. national security satellites across all orbital regimes; the new policy continued even after the NRO became "overt" in 1992. From 1999 to 2003, this policy even extended to the GPS satellites operated by the U.S. Air Force, which broadcast their location to anyone with a GPS receiver.[89] Today the policy of not publishing the location of many national security satellites continues, even for large, transmitting satellites in the GEO belt.

It is likely that these restrictions have been the result of policy inertia and the continuation of a number of arguments made since the beginning of military space activities to protect satellite reconnaissance.[90] It was acknowledged early on that effective reconnaissance requires surprise and secrecy, including protecting the types of sensors used and the timing of reconnaissance activities. Increasing the number of U.S. satellites in orbit whose purpose was unknown and restricting precise data on their orbital location were seen as effective strategies against countermeasures.[91]

The current policy requires that the existence of certain satellites performing specific national security functions be protected by placing them on what is known as the exclusion list. Although the U.S. government does announce all space launches in accordance with international agreements, for these protected satellites on the exclusion list it withholds the name of the satellite, its function, and any information about its eventual location in orbit. After launch, these satellites are given the designation "USA XXX" in the U.S. military's catalog of space objects,[92] where XXX is a unique, sequential number. In addition, the U.S. military does not publish orbital data indicating the location of these satellites after launch nor any of the other objects that it placed into orbit on the same launch, such as spent rocket stages or additional payloads, even if the latter are unclassified.

Rationale for modifying the classification policy

The primary reason for modifying this policy is that it has had a negative impact on the United States' ability to improve the SSA systems in use by its military. In order to attempt to enforce the secrecy policy, the U.S. military needs to be in a position to control and filter SSA data to try and prevent the existence and location of classified satellites from being disclosed. To meet this need, the United States has made the military the central hub for all SSA activities in the United

[88] Personal conversations with early satellite observers.
[89] Langley, R.B. (1999, March 30). U.S.SPACECOM stops publishing 2-line element sets for GPS satellites. Seesat-L mailing list. Retrieved from http://satobs.org/seesat/Mar-1999/0451.html
[90] Policy paper, "National Policy on Satellite Reconnaissance," April 10, 1962. Retrieved from: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB225/doc15.pdf
[91] Ibid.
[92] The public catalog of space objects maintained by the U.S. military can be found at http://space-track.org

States, including those activities related to civil and commercial safety of spaceflight that are not part of its traditional mission. It has also led the United States to try and make the U.S. military the central SSA authority for all space actors so as to discourage them from developing their own SSA capabilities. After the 2009 Iridium-Cosmos collision, the U.S. government decided to provide a free collision warning service to all space actors[93] instead of publishing the SSA data so satellite operators could perform their own analysis.[94] This program has greatly increased the SSA workload on the U.S. military by giving it a function for which it is not equipped nor staffed to handle and is a contributing factor to resource shortages and significant problems with warning accuracy.

The secrecy policy also hinders cooperation with key partners and allies. For the last decade, the U.S. military has run a set of exercises called the Schriever Wargame series to examine potential future space conflicts. Recent wargames have involved allies and commercial partners, and a key lesson has been the need for integrating these non-military entities into situational awareness and planning to take full advantage of the capabilities available to coalition partners.[95] The current classification policy is a barrier to such collaboration.

Furthermore, the current classification policy places a multi-level security requirement on all IT systems used to generate and handle SSA. Historically, this requirement has been a significant driver of increased costs and development time for SPADOC and CAVENet.[96] It remains a significant cost driver and hurdle for JMS as well. A recent GAO report stated that Air Force officials informed the GAO that they are not aware of any Air Force information technology systems that provide information at as many classification levels as JMS is intended to provide, although no direct attribution or evidence was provided.[97]

It is possible that the secrecy policy as it currently exists gives the United States an incentive to undermine other SSA efforts that could provide an alternative data source to the one it controls. An element of the previously mentioned policy of making the U.S. military the central hub for all SSA activities is not only offering free services to all space actors, but also in discouraging or even actively undermining alternatives. Although there is no public evidence of explicit efforts towards this end, the U.S. government stance on alternatives such as the SDA, the International Scientific Optical Network (ISON), and the bilateral agreements it is signing with other countries hint that

[93] Chow, T. (2011, September, 22). Space situational awareness sharing program: An SWF issue brief. Secure World Foundation. Retrieved from http://swfound.org/media/3584/ssa_sharing_program_issue_brief_nov2011.pdf

[94] Weeden, B. (2009, February 23) "Billiards in space." *The Space Review*. Retrieved from http://www.thespacereview.com/article/1314/1

[95] James, L. (2010, November) "The Challenge of Integration: Lessons from Schriever Wargame 2010." *High Frontier*,7(1), 9-11. Retrieved from: http://www.afspc.af.mil/shared/media/document/AFD-101116-028.pdf

[96] Smith, R. (1999, March 22) "Human Machine Interface Incidents: The SPADOC Story." Retrieved from: http://www.fas.org/spp/military/program/track/spadoc4c.htm

[97] Government Accountability Office (2011, May) "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities." Retrieved from: http://www.gao.gov/assets/320/318942.pdf

this may be the case. This policy could also play a role in the reticence of certain U.S. European allies to participate in the proposed European SSA system. While the United States is completely within its sovereign rights to undertake such efforts, the prioritization of the secrecy policy over improving SSA raises the question of whether or not the United States is serious about its stated national policy goals of improving SSA and the long-term sustainability of space. Increasing the amount of accurate and precise SSA available to all space actors, regardless of the source, will benefit the United States.

This detrimental impact on SSA is not new and has long been characterized as an unfortunate cost of achieving the benefit of helping protect the existence and location of many of the U.S. national security satellites. However, there is evidence that this benefit is diminishing. As the main target of such satellites during the Cold War, the Soviet Union was well aware of the existence and locations of these satellites through their own satellite tracking capabilities, espionage activities, and unauthorized and inadvertent disclosures by U.S. officials.[98] A notable example occurred in 1986 when William Burrows published his now infamous book "Deep Black," which discussed the history of classified U.S. activities in space at length and revealed details of many classified satellite programs.[99]

Since the end of the Cold War, the challenges in keeping these satellites hidden have only increased. The mere fact that the U.S. government is trying to protect the identity and location of these objects leads to more curiosity, publicity and eventual discovery (a phenomenon known in the popular culture as "The Streisand Effect"). Each launch of a U.S. military payload is accompanied by reams of press reports and discussions among communities of amateur observers on the Internet, who often can deduce what is being launched and its function. Many of these amateur observers have sophisticated tools for non-cooperative tracking of space objects, including custom-made telescopes, automated tracking software, imaging capabilities, and radiofrequency detection equipment.[100] These amateur observers and other experts are then quoted in the press, leading to more dissemination of the secret data.[101] These amateur activities are in addition to the SSA capabilities possessed by other states, both allies and potential adversaries.

The strategy put forward in 1962 of increasing the number of satellites in orbit whose purpose is unknown to obfuscate which satellites are performing sensitive missions is not as viable as it once may have been. Over the last 50 years of space activity, it has become publicly known which

[98] Richelson, J.T. (2002). Restructuring the NRO: From the Cold War's end to the 21st century. International Journal of Intelligence and Counterintelligence, 15(4), 496-539. DOI:10.1080/08850600290101749

[99] Burrows, W.E. (1986). Deep black: Space espionage and national security. Random House: New York.

[100] Wilson, T. (2001). Threats to United States space capabilities. Prepared for the Commission to Assess United States National Security Space Management and Organization. Retrieved from http://www.fas.org/spp/eprint/article05.html

[101] Nash, J. (2012, May 1) "Spy-High: Amateur Astronomers Scour the Sky for Government Secrets." *Scientific American*. Retrieved from: http://www.scientificamerican.com/article.cfm?id=amateur-astronomers-spy-satellite

orbits are most useful for which purposes and patterns of behavior of reconnaissance activities have been identified.

The large amount of attention these classified objects receive in large part because of the attempts to keep them secret has led to a functional failure of the secrecy policy. Of the approximately 180 objects listed as USA objects without TLEs in the public satellite catalog as of April 2012,[102] nearly all are found in the public satellite database maintained by the Union of Concerned Scientists (UCS), which lists name, function, and mission in addition to their USA identifier.[103] For many, amateur observers regularly provide positional data and occasionally even imagery of satellites in LEO and GEO that are USA objects in the public satellite catalog. Even more details for many of these protected satellites in GEO are provided in the annual "Classification of the Geosynchronous Objects" report by the European Space Agency.[104] Based on tracking data from ESA and ISON, the report provides both the name and orbital location of 46 active U.S. satellites and 105 dead satellites and pieces of debris that are listed as USA objects without TLEs in the public satellite catalog.[105]

One of the more recent and well-publicized failures of this policy concerns the launch of two orbital test vehicles for the Air Force's X-37B program in 2010 and 2011.[106] When the first orbital test vehicle was launched in April 2010, the U.S. military rolled out a very public campaign to discuss the program and made a point of indicating they were being more "open" by telling the world they were launching the vehicle into orbit. However, they refused to provide details on the contents of the payload bay, the purpose of the payload, or on the test vehicle's orbit.[107] On May 22, 2010, amateur satellite observers reported the test vehicle's orbit[108] and did so again after it maneuvered that August,[109] demonstrating the failure of the secrecy policy to protect its existence and location. These and other incidents led General James Cartwright, then Vice Chairman of the

[102] As determined by a search of the SATCAT at http://www.celestrak.com
[103] Union of Concerned Scientists. (2012, April, 1). UCS satellite database. Retrieved from http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html
[104] Flohrer, T. (2012, February 17). "Classification of Geosynchronous Objects." European Space Agency, European Space Operations Centre.
[105] Based on a comparison of the UCS database with the public satellite catalog available at http://www.celestrak.com
[106] Weeden, B. (2010, May 19). X-7B orbital test vehicle fact sheet. Secure World Foundation. Retrieved from http://swfound.org/media/1791/x-37b_factsheet.pdf
[107] Payton, G. (2010, April 20). Transcript of media teleconference. Retrieved from http://www.defense.gov/Blog_files/Blog_assets/PaytonX-37.pdf
[108] Broad, W.J. (2010, May 22). Surveillance suspected as spacecraft's main role. *New York Times*. Retrieved from http://www.nytimes.com/2010/05/23/science/space/23secret.html?_r=1&hp
[109] David, L. (2010, August 24). Secret X-37B space plane has changed orbit. Space.com Retrieved from http://www.space.com/9000-secret-37b-space-plane-changed-orbit.html

Joint Chiefs of Staff, to conclude it was no longer possible for the United States and other countries to keep vast numbers of orbiting satellites a secret.[110]

The current classification policy also has a negative impact on the safety of space activities. Recently, the U.S. military began a program to launch non-military payloads along with their classified payloads to help provide opportunities for academic and scientific entities to place small satellites in orbit without needing to pay expensive launch costs. Because of the classification policy, the orbital information for these additional payloads is protected so as to not provide clues about the orbit of the classified payload. This makes it difficult for scientists or students to communicate with these satellites to retrieve data, especially if the satellite stops broadcasting due to a malfunction. It also increases the number of objects in space for which there is no public positional information, which can present navigation hazards in congested orbits. In addition to the 180 or so active classified U.S. satellites, the positional information for another nearly 300 non-classified objects (secondary payloads, debris, or rocket bodies) is being withheld because they were part of the same launch as one of the classified satellites. The lack of positional information on these objects makes it very difficult for the many satellite owner-operators who lack access to their own SSA systems to detect and avoid possible collisions with them.

Another example concerns a failed Defense Support Program (DSP) early warning satellite, DSP-23. The satellite experienced a malfunction in 2008, causing a change in its orbital behavior that was detected by amateur observers but never acknowledged by the U.S. government.[111] This malfunction left the satellite drifting through the geostationary belt and posing a potential collision hazard to other operational satellites, including a cluster of commercial communications satellites.[112] Even though it is no longer functional, the secrecy policy is still in effect for the satellite and its orbital location is not published in the public satellite catalog. Amateur observers are still tracking it, however, and monitoring it for potential collisions with other satellites.[113]

This practice by the United States of trying to protect specific satellites has also led to copycat policies by other countries. In 2007, French military officials stated in an interview that they would use their tracking data on classified U.S. satellites to pressure the United States into applying the same protections to certain French satellites.[114] In December 2009, the U.S. military stopped publishing positional data for several French military satellites.[115] The U.S. military has adopted similar policies for several Japanese, Israeli, and German military satellites. Although the total

[110] AFP. (2010, May 13) "Chaotic space traffic needs rules: US general". Retrieved from: http://www.google.com/hostednews/afp/article/ALeqM5iXC0gGbQ1dF3navsVE-QkRB3MY9w
[111] Weeden, B. (2009, January 19). The ongoing saga of DSP Flight 23. The Space Review. Retrieved from http://www.thespacereview.com/article/1290/1
[112] David, L. (2009, February 25). Wandering U.S. spy satellite prompts continuing concerns. Space.com. Retrieved from http://www.space.com/3036-wandering-spy-satellite-prompts-continuing-concerns.html
[113] Ibid.
[114] de Selding, P. (2007, June 8). French say 'non' to U.S. disclosure of secret satellites. Space.com Retrieved from http://www.space.com/3913-french-disclosure-secret-satellites.html
[115] Space Security Index. (2010). Retrieved from http://www.spacesecurity.org/space.security.2010.reduced.pdf

number of satellites removed in such a manner is small, it does present a growing trend that could have safety implications. While the United States does have information, tools, and procedures to help prevent collisions between its classified and other trackable objects in orbit, much less is known about the ability of these other states to do the same.

Implementation options

The most obvious satellites to apply a relaxed classification policy to are those that are easily detected and tracked. These include large satellites operating from fixed locations in GEO, especially those that broadcast communications data, and large satellites in LEO.

As many of these classified satellites are used to gather intelligence, the most significant national security concern is their ability to do so. For those whose existence is already publicly known, changing the secrecy policy and publishing the orbits of these currently classified satellites does no additional harm. The modified policy should still protect their program name or designation, mission, function, capabilities, and limitations because it is these details that are truly militarily useful to an adversary. These details are also easier to protect because they are not easily determined by a remote observer.

As for publishing the location of LEO satellites used for reconnaissance, some will argue that doing so allows an adversary to predict when they will overfly a particular location and thus hide or modify activities and hinder the ability to perform reconnaissance. This is not necessarily the case. Changes in orbit have a short shelf-life – several of these potential adversaries maintain their own satellite tracking facilities that will detect the new orbit as soon as the maneuvered satellite overflies their territory, making the maneuver tactic only useful for the first pass after the maneuver.

Thus, the position of these LEO reconnaissance satellites can be made public in a way that still protects their advantage by reducing the frequency of public updates to the orbit of these satellites. An update of these satellites' position once-per-day or even every 12 hours would allow plenty of time to maintain the element of surprise for the first pass after a maneuver while still providing public information to aid safety and transparency efforts.

Finally, not all U.S. national security satellites needed to have their locations revealed. If the U.S. military has technology or operational procedures to avoid detection, it does not need to preemptively announce the location of national security assets performing a particularly important or sensitive mission. However, it should do so with full acknowledgement of the potential safety hazards/risks/dangers and accept the responsibility to operate such classified objects in a responsible manner.

CONCLUSIONS

Given its increased reliance on space capabilities for national security and economic might, the United States must meet the challenges of an increasingly contested, congested, and competitive space domain. SSA lies at the heart of meeting those challenges. At the highest levels, the United States has recognized the need for improving SSA and for putting specific policy guidance in place to meet that need. However, there are technical limitations of the legacy IT systems at the core of the U.S. military's current SSA capabilities that prevent it from making the changes necessary to realize its policy and security goals.

The Air Force may be able to execute the three phase strategy outlined by Lt. Gen. Pawlikowski and deliver JMS to replace SPADOC and CAVENet by 2015. However, this is only part of solving the problem. A much bigger question is whether JMS can deliver the capabilities that are needed by all stakeholders and whether the JSpOC, as currently conceived, can achieve the policy goals the President and Department of Defense have set out. Replacing SPADOC and CAVENet with JMS might enable the JSpOC to ingest owner-operator data and perform conjunction analyses faster, but it will not solve the manpower, expertise or training issues within the U.S military. Nor will simply replacing the hardware address bureaucratic, cultural and political barriers that are currently hindering SSA sharing and cooperation efforts.

This report has argued that adopting a more open approach to SSA and developing astrodynamic standards that includes all stakeholders is crucial to providing a solution that addresses the problems faced by all space actors. Making a more open approach feasible also means addressing the challenges of the central role of the U.S. military in providing SSA services and the current classification policy for national security assets. The common thread among the recommendation and the challenges is the recognition of fundamental changes in the users and uses of the space domain that prompt a re-examination of the traditional approach to SSA.

Overcoming these challenges will likely require policy action at the highest levels, putting to rest some long-held beliefs about U.S. power in space, and re-evaluating the prioritization of secrecy over transparency and public services. It will not be easy. However, it is in the realm of the possible. If these challenges are addressed, resolving the technical problems with maintaining an improved catalog of space objects and providing better conjunction warnings to all satellite operators will be relatively simple and straightforward.

If American SSA capabilities are not improved in the near future, the consequences could be significant for the United States and its goals and objectives. In addition to the increasing chances of another satellite collision in orbit, perhaps this time involving a national security asset of the United States or another country, failure to improve SSA will almost certainly drive other space actors to seek and develop alternative sources of SSA information other than the U.S. military. While ultimately these alternative sources would improve SSA for all, they would certainly run

counter to the U.S. government's desire to protect national security assets in orbit by controlling the data on their location. If these alternative sources of SSA were developed in a stove-piped fashion without involving astrodynamic standards, such a scenario could also run the risk of multiple, competing, and non-interoperable approaches to SSA that wastes valuable resources and could actually worsen the situation by providing inaccurate information. A scenario where the U.S. government takes the lead in working with all stakeholders to develop the underlying astrodynamic standards and interoperable systems that provide the services everyone needs is a much more desirable solution for all.

Secure World Foundation—Headquarters
525 Zang Street, Suite D
Broomfield, CO 80021
United States of America
***tel* +1.303.554.1560**
fax +1.303.554.1562

Secure World Foundation—Washington
1779 Massachusetts Ave., NW
Washington, DC 20036
United States of America
***tel* +1.202.568.6212**
***fax* +1.202.462.1843**

To learn more about Secure World Foundation
please visit *www.swfound.org*