SATCOM for Net-Centric Warfare

MilsatMagazine

MAY 2018

U.S.A.F. General Raymond's Keynote

Counterspace Capabilities &
Space Sustainability

The New Warfighting Domain

Overcoming Threats to Military Satellites

Cybersecurity Without Limits

Information Assurance

Dispatches

Photo of the U.S.A.F.'s AFSPC-11 launch
is courtesy of United Launch Alliance

PUBLISHING OPERATIONS

Silvano Payne, Publisher + Executive Writer
Hartley G. Lesser, Editorial Director
Pattie Lesser, Executive Editor
Jill Durfee, Sales Director, Associate Editor
Simon Payne, Development Director
Donald McGee, Production Manager
Dan Makinster, Technical Advisor
Sean Payne, Industry Writer

SENIOR CONTRIBUTORS

Tony Bardo, Hughes
Richard Dutchik, Dutchik Communications
Chris Forrester, Broadgate Publications
Karl Fuchs, iDirect Government Services
Bob Gough, Carrick Communications
Rebecca M. Cowen-Hirsch, Inmarsat
Giles Peeters, Track24 Defence
Koen Willems, Newtec

AUTHORS

Major Chris Bradley
Charlie Kawasaki
General John “Jay” Raymond
Victoria Samson
Ryan Schradin
Lance Smith
Senior Airman Arielle Vasquez
Dr. Brian Weeden

FEATURES

ADVERTISER INDEX

A United Launch Alliance Atlas V rocket launches two military satellites for the AFSPC-11 mission. Photo is courtesy of United Launch Alliance.

MilsatMagazine is published 11 times a year by Satnews Publishers, 800 Siesta Way, Sonoma, CA — 95476 — USA.
Phone: (707) 939-9306,
Fax: (707) 939-9235

We reserve the right to edit all submitted materials to meet publication content guidelines, as well as for grammar and spelling errors, or to move articles to an alternative issue to accommodate publication space requirements, or remove content due to space restrictions. Submission of content does not constitute acceptance of said material by Satnews Publishers. Edited materials may, or may not, be returned to author and/or company for review prior to publication — article review PDFs must be returned with corrections within 72 hours of receipt by the author. The views expressed in Satnews Publishers’ various print, online and PDF publications do not necessarily reflect the views or opinions of Satnews Publishers. All rights reserved. All included imagery is courtesy of, and copyright to, the respective companies and/or named individuals.

AvL
AvL

An EAGLE and a CBAS for the U.S.A.F. are launched by ULA

A ULA Atlas V rocket carrying the AFSPC-11 mission for the U.S. Air Force lifted off from Space Launch Complex-41 at 7:13 p.m. ET on April 14. Photo is courtesy of United Launch Alliance.

This was a smooth ULA launch occurring on a spring evening as the company's Atlas V 551 configuration — the most powerful Atlas V variant that has flown to date — lifted off from Space Launch Complex 41 at Cape Canaveral Air Force Station, Florida, on a crucial, multi-payload mission for the U.S. Air Force.

The forward payload is referred to as CBAS (Continuous Broadcast Augmenting SATCOM) and the aft spacecraft is EAGLE (EELV Secondary Payload Adapter [ESPA] Augmented Geosynchronous Experiment).

"*Today's launch is a testament to why the ULA team continually serves as our nation's most reliable and successful launch provider for our nation's most critical space assets*," said *Gary Wentz*, ULA Vice President of Government and Commercial Programs.

He added, "*I want to thank the entire ULA team, and the phenomenal teamwork of our mission partners*."

The Atlas V Evolved Expendable Launch Vehicle (EELV) 551 configured vehicle included a large, five meter Payload Fairing (PLF). The Atlas booster for this mission was powered by the RD AMROSS RD-180 engine. Aerojet Rocketdyne provided the five AJ-60A solid rocket boosters (SRBs) and RL10C-1 engine for the Centaur's upper stage.

"*Congratulations to the AFSPC-11 integrated team and all mission partners on a successful launch. This is testament to the dedicated government and contractor professionals who work tirelessly mission-by-mission to achieve 100 percent mission success.*" said Lt. Gen. *John F. Thompson*, Space and Missile Systems Center commander and Air Force program Executive Officer for space.

Launch services for the Atlas V 551 vehicle were acquired by the Space and Missile Systems Center. First used in 2006, this Atlas vehicle configuration successfully launched the **New Horizons** satellite, the **Juno** satellite and five Navy communications **MUOS** missions.

Managed by the Military Satellite Communications Directorate of the U.S. Air Force's Space and Missile Systems Center, CBAS is a military satellite communications spacecraft destined for geosynchronous orbit to provide communications relay capabilities to support senior leaders and combatant commanders.

CBAS will augment existing military satellite communications capabilities and broadcast military data continuously through space-based, satellite communications relay links.

The Air Force Research Laboratory (AFRL) EAGLE payload's primary mission objective is to demonstrate a maneuverable ESPA based on a space vehicle design which can accommodate up to six hosted or deployable payloads in geosynchronous orbit.

SMC is the U.S. Air Force's center for acquiring and developing military space systems. Its portfolio includes GPS, military satellite communications, defense meteorological satellites, space launch and range systems, satellite control networks, space-based infrared systems and space situational awareness capabilities.

This is the 77th launch of the Atlas V rocket, ULA's fourth launch in 2018 and the 127th successful launch since the company was formed in December 2006.

www.ulalaunch.com/

Advantech Wireless | SMARTER SOLUTIONS, GLOBAL REACH.

GOVERNMENT & MILITARY SOLUTIONS

ENABLING FASTER & MORE SECURE COMMUNICATONS FOR MILITARY & GOVERNMENT LEADERS

WGS CERTIFIED

- Complete Military SATCOM Solutions
- Advanced GaN for Radar Applications
- Second Generation GaN Troposcatter Amplifiers

Multi Services
VSAT Solution

At Advantech Wireless, we have over 25 years of experience in helping military special forces and government agencies by delivering cutting-edge innovations in communications that solve mission critical communications challenges.

We understand the challenges that government & military forces face and our technologies bring them the freedom to communicate beyond line of sight quickly, reliably and securely.

Second Generation
GaN based SSPAs/SSPBs

TROPOSCATTER Modular
Solid State GaN Power Amplifiers

Higher Power and higher Information rates for Mission Critical Operations

sales@advantechwireless.com

www.advantechwireless.com/gov

U.S. Cyber Command commander named

In response to the changing face of warfare, U.S. Cyber Command has been elevated to a combatant command, this according to chief Pentagon spokesperson Dana W. White.

She said that the cyber domain will define the next century of warfare.

White added that, just as the U.S. military must be prepared to defend the nation against hostile acts from land, air and sea, the U.S. must also be equipped to deter and, if necessary, respond to hostile acts in cyberspace.

CYBERCOM Commander, U.S. Army Lt. Gen. Paul M. Nakasone.

Army Lt. Gen. *Paul M. Nakasone*, most recently commander of Army Cyber Command, will receive his fourth star as he succeeds retiring Navy Adm. Michael S. Rogers as Cybercom commander.

Nakasone will play a critical role in tasks that include training cyber warriors, advocating for more cybersecurity resources, and planning and conducting cyber operations.

This change of command is noteworthy because it signifies the elevation of Cyber Command as our 10th combatant command. Last year, Defense Secretary *James N. Mattis* announced the elevation of Cyber Command, acknowledging that a new warfighting domain has come of age.

U.S. Cyber Command, which has been a sub-unified command under U.S. Strategic Command, was established in 2009 in response to the rapidly evolving threats with adversaries seeking to exploit the cyber domain to attack the United States and its allies.

The elevation of the command raises the stature of the commander to a peer level with other unified combatant command commanders, allowing the Cybercom commander to report directly to the secretary of defense, *Kenneth P. Rapuano*, who is the assistant secretary of defense for homeland defense and global security.

twitter.com/uscommandcyber?lang=en

Second of five evaluations for a DARPA and AFRL SSA mission completed by Ball Aerospace

Ball Aerospace has successfully completed the second of five evaluations of the Space Evaluation and Analysis Capability (SEAC) testbed the company is developing for the Air Force Research Laboratory (AFRL) and Defense Advanced Research Projects Agency's (DARPA's) Hallmark program, demonstrating an open-architecture, open development and developer-community driven approach — the program is advancing technologies that deliver real-time space-domain awareness to command and control and protect space assets.

The role of the Hallmark program SEAC testbed is to support multiple tools and technologies developed by various companies and academic institutions that will make up the system's technical capabilities and include operator interfaces, simulation and scenario playback capabilities to stimulate these tools.

Ball is embracing DARPA's "zero-integrator" approach to the SEAC testbed design, which eliminates the single-contractor integration bottleneck in traditional acquisition models, and is implementing modern DevOps software development practices that empower external tool developers to deliver new capabilities faster without risking system security or stability by developing and testing in an operations-like environment.

Tool developers independently identified areas for improvement and delivered software updates in less than three hours. Then within an hour, Ball engineers deployed the updates and were able to show that the additional functionality was available in the system.

Steve Smith, VP, Systems Engineering Solutions (SES) business, Ball Aerospace, said that as the SEAC provider, Ball is leveraging the firm's heritage with operational system development to innovate new technologies with open-source software. His open-architecture model will lend itself to tool developers and help create efficiencies in the government environment, ultimately protecting vital space assets.

Carl Fischer, Chief Technologist, Advanced ISR Solutions, Ball Aerospace, added that to assess the effectiveness of the testbed and tools during the recent evaluation event, Ball simulated three different government-provided scenarios that required a timely analysis and response. Leveraging the company's development environment and simulated operation floor, Ball demonstrated the speed at which the system can be updated.

www.ball.com/aerospace/

Intelsat General's 15 year tradition continues for AFN

Intelsat General, a wholly owned subsidiary of Intelsat (NYSE: I) will distribute television and radio programing to U.S. servicemen and women stationed around the world, working with the support of three other satellite and ground service providers.

Intelsat General has been carrying the global satellite feed for the American Forces Network (AFN) for more than 15 years, bringing U.S. troops on land and at sea a wide variety of television and radio programming.

The new one-year contract with four renewable option years will involve six satellites and five teleports at various locations around the globe, as well as the IntelsatOne terrestrial fiber network.

The additional partners involved in providing the service are SES Government Solutions, Korea Telecom and Allen Communications.

The AFN will provide Intelsat General with three data streams for distribution globally, using uplink teleports in California and Maryland in the United States as well as South Korea and Germany.

Intelsat will distribute the AFN programming to ships at sea and fixed military bases in the Atlantic Ocean Region, the Indian Ocean Region, and the Continental U.S., Greenland, Central America and Cuba.

The American Forces Network, based at Fort Meade in Maryland, traces its origins to a single Army radio station established in Kodiak, Alaska, to entertain isolated soldiers at the beginning of World War II.

AFN has since grown to provide a wide range of around-the-clock radio and television programming from a variety of commercial sources, giving U.S. troops worldwide the same access to news, sports and entertainment that they might enjoy at home.

Rick Henry, VP of Sales and Marketing for Intelsat General, stated that the company has been supporting the American Forces Network for a number of years and this new contract will allow Intelsat General to continue to distribute programming that is so important to the morale of the troops at home, at sea and abroad. This globalized network enables AFN programming to reach more than one million service men and women stationed in the most remote areas of the globe, allowing them to feel closer to home whether they are watching an NFL football game or an episode of a television series.

www.intelsatgeneral.com/

myafn.dodmedia.osd.mil/

Blockchain-based cyber security report published by ABI Research

ABI Research recently published their *Hot Tech Innovators: Blockchain-Based Cybersecurity* report, which is part of the firm's Digital Security research service, that includes research data and analyst insights.

Blockchain technology is most often associated with cryptocurrencies and financial services applications. But, it's the very decentralized nature and cryptographic anchor of blockchain that makes it a prime foundation for cybersecurity solutions, particularly considering the continued mass-scale data breaches and identity theft happening on a worldwide scale and within the most well-guarded corporate perimeters.

The race is on for blockchain-based cybersecurity. ABI Research has identified the 15 startups in the blockchain-based cybersecurity space who are driving these unprecedented security solutions.

These startups, according to ABI Research, are the hot tech innovators who are aiming to harness the transformative features of blockchain and transform existing security models around identity, authentication, and data protection.

By leveraging digital signatures, cryptographic hashing, and consensus mechanisms in a distributed ledger format, these innovators hope to provide long-awaited solutions to the problems of data theft and loss.

"*The blockchain infrastructure can enable a strengthening of traditional cybersecurity practices, such as identity management and access control for example, by finding new applications for existing technologies, such as decentralized DDoS protection, or distributed PKI*," said *Michela Menting*, Research Director at ABI Research.

Menting added, "*Going forward, we will see increasing interest in using blockchain to protect all types of data (identity, corporate, financial) in transit and at rest. Most importantly, these technologies will be just as easily available to individuals wanting to regain control and protect their personal information, as well as to large organizations managing terabytes of business data.*"

The ABI Research Hot Tech Innovators in Blockchain-Based Cybersecurity are:

- ***Block Armour** is an India-based startup founded in 2016. The startup is developing an enterprise identity, authentication and access control management platform for critical / corporate systems, powered by Blockchain technology. The platform leverages digital signature-based identity and authentication for people, devices, and data. (**www.blockarmour.com/**)*

- ***Cambridge Blockchain** is a U.S.-based startup that was founded in 2015. It is focusing on offering software for enterprise digital identity, and notably facilitating KYC and AML for financial institutions. (**www.cambridge-blockchain.com/**)*

- ***Civic** is a U.S.-based IDV and management startup founded in 2016. It offers the Civic Secure Identity Platform (SIP) which runs on a mobile application that stores PII and can leverage the encryption and biometrics features of smartphones and tablets. The Civic App allows users to share and manage their fully verified identity data. (**www.civic.com/**)*

- ***Datum** is a Swiss-based startup that was founded in 2017. The startup plans on offering a decentralized and distributed high performance NoSQL database for the secure, private, and anonymous backup of structured data, including social network data and data from wearables, smart home, and other IoT devices. (**datum.org/**)*

- *Founded in 2013, **Evernym** is a U.S.-based startup that is developing a sovereign identity distributed ledger platform. Evernym is banking on SaaS services and applications built on the Sovrin Network, an attribute-based global identity network for self-sovereign identity. (**www.evernym.com/**)*

- ***Gem** is a U.S.-based startup that was founded in 2013. The startup focuses on developing enterprise blockchain for clients to build, deploy, and manage distributed applications. Gem is targeting the healthcare sector with its Gem Health Network (powered by Ethereum) as well as the supply chain sector. (**enterprise.gem.co/**)*

- ***Gladius** is a U.S.-based startup that was founded in April 2017 which focuses on providing an automated marketplace where users can rent out spare bandwidth and storage as well as purchase content delivery and DDoS protection services, all based on the Ethereum blockchain. (**gladius.io**)*

- *Founded in 2016, **Gospel** is a U.K.-based startup offering a secure enterprise data distribution platform for internal and external sharing of critical data across decentralized ecosystems. (**gospel.tech/**)*

- ***Guardtime** is an Estonian-based company focusing on data security and is currently headquartered in the Netherlands. Founded in the pre-bitcoin era in 2007, the firm developed a proprietary, subscription-based permissioned system for protecting government systems and data. (**guardtime.com/**)*

- *Based in France and founded in 2014,* ***Ledger*** *specializes in security solutions for cryptocurrency and blockchain applications through the offer of hardware security devices. For enterprises and corporations, Ledger offers the Vault: a managed SaaS solution to safeguard ledgers for large amounts and/or multiple cryptocurrencies.(****www.ledger.fr/****)*

- *Based in the U.K.,* ***MaidSafe*** *is a B2B2C company focusing on the provision of IaaS and PaaS services, notably through an open source, decentralized data storage and communication platform, known as the SAFE Network. (****maidsafe.net/****)*

- *Based in the U.S. and founded in 2015,* ***NuCypher*** *offers a security and encryption platform for distributed systems, including blockchain, big data, cloud, and the IoT. (****www.nucypher.com****)*

- ***Nuggets*** *is a U.K.-based startup that was founded in 2016. It focuses on enabling secure login, payment, and ID verification for consumers using biometric technologies. The idea is to eliminate the need to share or store personal data. The current blockchain is hosted on an Ethereum-pegged private blockchain (sidechain) distributed to a set of independent partners in the Nuggets ecosystem. (****nuggets.life)***

- *U.K.-based* ***Obsidian Platform****, which was founded in 2014 and incorporated in 2017, aims to offer private communication by combining a secure messenger application with a cryptographic coin that enables a decentralized communication network. (****icobench.com/ico/obsidian****)*

- **REMME** *is a Ukraine-based company that was founded in 2015. The startup aims to eliminate passwords and provide better authentication for users and for devices, based on a distributed PKI system. The current focus is on enterprise, the IoT, financial and critical infrastructure, medical technology, and cryptocurrency sectors. (****remme.io****)*

ABIresearch for visionaries

For additional info regarding ABI Research's Hot Tech Innovators reports, **please access this direct link.**

Hughes multi-modem prototype selected by DoD

Hughes Network Systems, LLC (HUGHES) has been awarded a follow-on contract to continue the second phase of a pilot study program to assess the feasibility of interoperability across multiple satellite communication (SATCOM) systems for the Department of Defense (DoD).

Under this award, Hughes will be responsible for prototyping a Flexible Modem Interface (FMI) for military terminals that will enable various military and commercial systems and services to interoperate in the field.

The new study — the second over the course of several years — builds on the growing commercial partnership with the DoD to assess what the ideal military SATCOM architecture would look like and how diverse systems could work together.

The assessment and prototype deliverables have the potential to create a more resilient, cost-effective, and flexible SATCOM architecture for DoD.

In Phase 2, Hughes will build on their recommendations from the first study and explore how an interoperable system solution could be effectively implemented by developing and producing the new FMI for demonstration and evaluation.

In 2017, Hughes participated in two different studies within the first phase of this project. In that first phase, Hughes recommended that the Defense Department pursue a SATCOM strategy that supports interoperability for wideband government applications, which would significantly enhance DoD's communications infrastructure and reduce acquisition and operations costs.

Dr. Rajeev Gopal, Senior Technical Director, Advanced Systems for Hughes says in Phase Two of this program, Hughes is being asked to develop, demonstrate and deliver a hardware and architecture prototype solution to support interoperable SATCOM capabilities for the military, which will help fortify satellite communications in contested environments.

The delivered solution will increase the resiliency and interoperability of various commercial and military SATCOM systems and services used by the DoD, including over High-Throughput Satellites (HTS).

As part of the overall assessment, Hughes will be evaluating the needs and capabilities that DoD will require in the future, including a secure and affordable wideband communications architecture (WCA) that can facilitate varied and redundant space and ground transports.

The FMI prototype will be demonstrated within the context of a mission management architecture that supports wide-beam, spot-beam, and on-board processing satellites, including new GEO HTS and Low Earth Orbit (LEO) satellite constellations.

Rick Lober, vice president and general manager of defense and intelligence systems at Hughes added that the overall goal for Hughes is to help the Defense Department produce a solution that expands the capabilities of the U.S. government's satellite communications.

To do that, Rick said, they will examine how to create an interoperable system that is flexible and resilient, allowing DoD's various global applications to operate over its own satellite network as well as leveraging commercial satellites, management systems, gateways, waveforms, and modems for DoD terminals to increase mission assurance.

www.hughes.com

iDirect Government unveils a new, ruggedized satellite router

Direct Government (iDirectGov) has unveiled their 9050 OM ruggedized satellite router — the 9050 OM features enhanced security, military environmental standards and improved functionality in a ruggedized form factor for operation in harsh outdoor environments.

A 950mp integrated satellite router board resides at the heart of the 9050 OM, which protects the board from the elements including blowing rain or dusty conditions. Powered by Evolution® 4.2 software, the 9050 OM can operate in harsh environments in temperatures ranging from -40 degrees F to +131 degrees F.

While en route to a mission, the 9050 OM can survive a parachute jump from 25,000 feet or be submerged in water, and still be able to operate once it reaches its final destination.

The 9050 OM features are as follow:

- *Transmit Key Line, to lower battery consumption and extend the mission as needed*
- *Blackout switch to turn off all LEDs for discrete operations*
- *Single data connector to support two LAN ports, console, GPS input, and Transmit Key Line*
- *Antenna pointing meter to ensure the satellite terminal is properly peaked*
- *Passively cooled – no powered fans required to cool down the product while in operation*
- *External power supply designed for outdoor use along with the product*
- *Federal Information Processing Standards (FIPS) 140-2 Level 3 certified*
- *Wideband Global SATCOM (WGS) certification ready*

John Ratigan, President of iDirect Government, said this is going to drastically change the way operators work in the field. Gone are the days of lugging around heavy transit cases in inclement weather and remote locations — this 9050 OM is durable, compact and powerful, enabling iDirectGov's 950mp satellite router board to send critical information over the airwaves without overheating or experiencing a failure in the field. The company's engineers designed and tested this solution so that the men and women who defend our nation can communicate seamlessly in order to complete their mission and keep us safe.

www.idirectgov.com

U.S. military cyber ops students "Game On..."

CYBERWAR:2025
DotEvil

Two students at the Naval Postgraduate School here have created a way to bridge a training gap in U.S. military cyber operations — through a game.

For their master's thesis, Army Master Sgt. *David Long* and Army Capt. *Chris Mulch* designed and developed ***CyberWar 2025***, a computer-based strategy war game that challenges players to navigate through the core concepts of the cyber realm.

"*The goal of CyberWar: 2025 is to stimulate and increase players' knowledge and experience of cyberspace operations*," Mulch said. "*The basic idea is to learn as you play.*"

In approximately 30 to 60 minutes of turn-based, 'sandbox' gameplay, players employ a range of the basic concepts laid out in **Joint Publications 3-12(R) Cyberspace Operations**. A deft combination of offensive cyber operations, defensive cyber operations and computer network exploitation can lead a player to victory, even if in a relatively weak position.

"*Everybody starts out on a level playing field*," Mulch explained. "*Players utilize resources in a way they see fit, whether those resources are put into offense, defense or reconnaissance.*"

A sense of urgency has burgeoned in the United States over the last decade as adversaries — state and non-state actors alike — have increasingly turned to the cyber domain to actively work against U.S. national security interests.

In a recent speech at J**ohn Hopkins University**, Defense Secretary *James N. Mattis* reiterated that the Defense Department absolutely must "*invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Our competitive edge has eroded in every domain of warfare — air, land, sea, space, and cyberspace — and it is continually eroding.*"

President *Donald J. Trump* echoed this in his fiscal year 2019 budget request to Congress, calling for a 4.2 percent increase in the Pentagon's cyber funding to US$8.5 billion as **U.S. Cyber Command** approaches full operational capability as a newly-unified combatant command.

"*What's going on in cyber policy is a big question right now in DoD*," Mulch said. *"What does our competitive balance look like? Should we be strong? Should we be putting time and resources into defense, reconnaissance or research?*"

Yet, there remains a critical gap in how DoD goes about preparing the military to engage in this domain. Several educational courses and training exercises have been developed to prepare leaders to plan and execute cyberspace-based effects to support operations, but there are no virtual simulations used by the military to train and educate service members in the basic concepts of cyberspace operations.

Filling a Gap

When Long, a cyberwarfare practitioner at Fort Meade, Maryland, and Mulch, an information operations officer, arrived at the **Naval Postgraduate School** in June 2016 to begin their graduate work in information strategy and political warfare, it didn't take them long to turn to solving this.

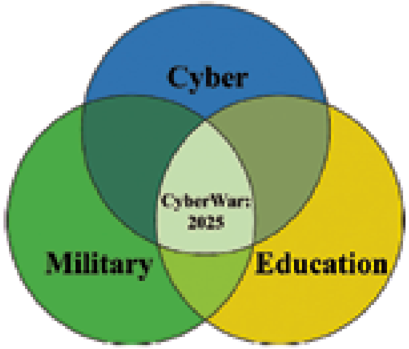
"*People would say I'm the cyber guy, even though I really don't like that term*," Long said. "*When I came to NPS, my promise to myself was to [impact] the Army cyber mission; I had a lot of ideas about how we can educate people about cyber operations, and how we could do it correctly.*"

Attending a game theory course, they encountered an article exploring the strengths and weaknesses of American cyber capabilities vis-a-vis Russia and China. Over spirited arguments over how much emphasis the U.S. should be placing on offense, defense or reconnaissance, the kernel of CyberWar: 2025 was formed.

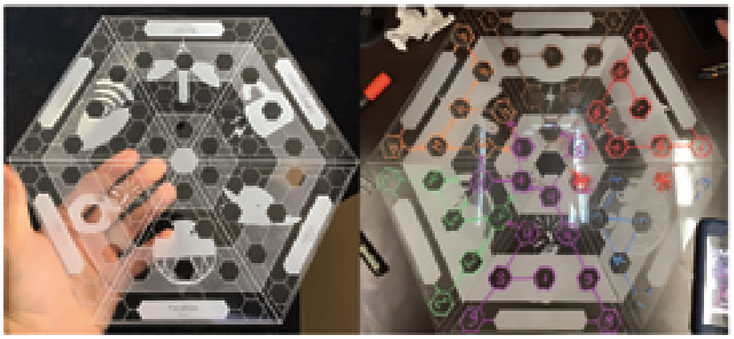
"*We used game theory to explore that, but that was the basis of 'hey, I think we have a question here that we could look into*,'" Mulch said.

Army War-Gaming

Coming up with a game was not too far of a stretch: the U.S. military has a long history of using games to prepare, understand and even plan for war. The earliest use of war gaming in the U.S. dates back to 1883, when Maj. *William R. Livermore* used topographical maps to practice the art of war. Livermore's work was itself based on **Kriegsspiel**, a tabletop game the Prussian military had used since 1812 to train their officers.



Three Core Elements that Make Up CyberWar: 2025



Initial Table Top Development and Testing

However, such gaming is not just "beer and pretzels," Long stressed. Serious games, which academic literature refers to as "gamification", are played to stimulate creative thinking, decision making and problem solving to learn. Good gamification allows players to synthesize new knowledge and make critical judgments.

"*With CyberWar: 2025, what we're really looking at, other than reinforcing terminology, is letting people learn through discovery what the relationship between cyber effects is*," Mulch said.

For example, if a player has developed strong defensive capabilities but weak offensive capabilities, what would a potential conflict look like with an adversary with strong offensive capabilities?

"*In a nutshell, that's what CyberWar: 2025 provides: An interactive experience for you to reinforce concepts and potentially look at other ways to solve a problem*," Mulch said.

Game Play

The game, he said, is intended to feel like **Diplomacy**, a classic 1954 strategy board game that relies as much on player interaction as moving pieces around a board.

At the start of CyberWar: 2025, six players are randomized for anonymity, so you could be sitting next to somebody, but not necessarily be located next to them on the board.
Play then proceeds simultaneously by round, with each player submitting their orders, which are resolved all at once before the next round.

"*The players communicate with each other and maneuver around the map, which consists of 48 interconnected 'server nodes' that are represented by hexagons*," Mulch explained.

As players capture new server nodes, they gain points which they then use to either conduct an action or research three tiers of new, more advanced effects for these actions.

"The more points you have, the more you can put into effects, and then you can use these to launch attacks against your adversaries and so forth," Mulch said.

The game play is simple and intuitive, but there's a lot going on under the hood. When all players have submitted their orders, the software engine running the game sorts their input, calculates each of their actions, analyzes the results and then broadcasts these back to the players within a split second.

Training Applications

"*What we accomplished over a tight nine-month time frame was to effectively pack ten pounds of product into a five-pound product bag,"* Long said. *"You learn by making mistakes: you can explore multiple paths and if you make a mistake, that doesn't mean you lose the game."*

From inception, Long and Mulch designed the game to be applicable for all branches of DoD and their subordinate cyber fields, as well as an educational tool for decision makers and leaders on cyber policy.

As their thesis was published in December, CyberWar: 2025 has been successfully adopted in cyber courses at NPS, though Long and Mulch would like to see it become more widely available.

"*The way forward is to have it incorporated into cyber education courses across the services*," Mulch said.

The simulation also has great potential as refresher training, the duo said. For service members who've already received cyber training, yet haven't practiced it for some time, CyberWar: 2025 serves as an efficient tool to get them back up to speed prior to deployment or a training event.

"*Whether they're about to go out to the National Training Center at Fort Irwin, California, the Joint Readiness Training Center at Fort Polk, Louisiana, or anywhere else, CyberWar: 2025 could be implemented as a reinforcement tool at the home station pre train-up before they go into an actual exercise*," Long said.

CyberWar: 2025 has been effectively used in the classroom at NPS, but the students hope to soon see the application available to a broader DoD audience. With further development, incorporating computer-controlled players, Long and Mulch see the opportunity for a DoD-wide training tool.

Commands and NPS students interested in this project should contact:

SFC David "Ty" Long, Student, Department of Defense Analysis, GSOIS

CPT Chris Mulch, Student, Department of Defense Analysis, GSOIS

Dr. Michael Freeman, Associate Professor, Department of Defense Analysis, GSOIS

Dr. Robert Burks, Associate Professor, Department of Defense Analysis, GSOIS

GSOIS = Graduate School of Operations and Information Science at the Naval Postgraduate School, Monterey, California

https://www.nps.edu/web/gsois/

A boost for soldier communications

The days of simple radio communication seem to be over for the soldiers of the 173rd Airborne Brigade Combat Team.

In the place of radios comes a sophisticated yet intuitive communication system that allows leaders at the squad level and higher to rapidly share information across the military network. This new platform, called the **Integrated Tactical Network**, revolutionizes the way tactical leaders are able to communicate, improving the lethality of small units, while at the same time increasing safety and situational awareness for soldiers.

“*Besides each of us having access to the mission graphics, we will be able to battle track each other*,” said Army 1st. Lieutenant *Michael Austin*, a platoon leader in Attack Company, 1st Battalion, 503rd Infantry Regiment. “*If we're in a movement to contact and we take chance contact, we can use this to very accurately shift fires, and have more fires on the enemy while being very safe because we know our exact front-line trace*.”

The benefits for soldiers in the field are extensive. With the platform, leaders are able to track the positions of the units all around the battlefield, as well as share text messages, voice communication and even pictures.

Crystal-Clear Communications

The equipment was fielded to the battalion two days prior to executing company-level combined arms live-fire exercises in Germany that were conducted from May 1 to 5. After a one-day class, the radio telephone operators and the platoon leaders understood the process for using the devices and were able to use them for the actual exercise.

“*We had crystal-clear communications the entire time and that's the first time we've had that*,” Austin said. “*Our scouts were able to take photos directly from their hide site, so we had eyes on the objective in real-time*.”

The new system uses equipment that soldiers are already familiar with, including the multi-band, inter/intra team radio to project data as well as a modern smartphone for the actual interface.

U.S. Army 1st. Lt. Michael Austin, a platoon leader for Attack Co., 1st Battalion, 503rd Infantry Regiment, uses an end-user device to report information to his company commander through the Integrated Tactical Network during a live-fire exercise in Grafenwoehr, Germany.
Army photo by Spc. Joshua Cofield

“*This system is simple to field and use*,” said Army Capt. *Michael Belina*, the signals officer for 1st Battalion, 503rd Infantry Regiment. “*We were able to learn it at the [operator] level in one day. The software is really intuitive since most soldiers know how to use smart phones as a second nature, [so] there's no issue with them picking up the features and figuring it out*.”

Platoon leaders, fire support officers and company commanders have the devices now, but squad leaders will have the same devices soon.

“*When the platform is fully implemented, paratroopers will have an additional quality radio and access to the same common operating picture as their leadership*,” Belina said. “*The common soldier will have a better idea of what's going on around him, and it will basically cut out some of the talk that is required to build that picture. It will be more immediate*.”

Another benefit of the new equipment is that it simplifies the communications package for the soldier on the ground.

“*It makes it so you don't have to have a truck with a [Joint Capabilities Release] on it, with a vehicle and power to it. It takes away all that equipment and simplifies it*,” said Army Sgt. *Alex Jones*, a retransmission team noncommissioned officer with the 1st Battalion, 503rd Infantry Regiment's communications section.

On a less tangible level, this system empowers junior leaders to know their mission and react quickly as the situation on the ground changes.

“*As an airborne unit, we already do a good job of going down to the lowest level to ensure everyone knows the plan*,” Austin said. “*But it's typically just the platoon leaders and platoon sergeants and up that have the finer details. This ensures even lower levels know the plan*.”

By improving communication across the formation, empowering junior leaders and ensuring soldier lethality on the battlefield, this new system shows just how the 173rd Airborne Brigade Combat Team soldiers continue to lead the force not just as fighters but also as modern, adaptable communicators on today's battlefield.

Story by U.S. Army Major Chris Bradley,
173rd Airborne Brigade Combat Team

Preparing warfighters today for the future...

On the far southwest end of Schriever Air Force Base is an operations warehouse known as ‘the Barn,’ where members replicate live GPS and satellite communication electronic attacks for training service members across the world.

This is the home of the 527th Space Aggressor Squadron which relies on its total force integration to get the mission done, which includes 26th Space Aggressor Squadron Reserve personnel. The 527th SAS stood up as the first space aggressor unit in 2000, while the 26th SAS activated in 2003. The history of the space aggressors traces back to the Vietnam War, when they were established to address aircrew training deficiencies.

“*During that time, there were unsatisfactory kill rates in the air domain*,” said Capt. *Brian Goodman*, training flight commander, 527th SAS. “*Adversaries were shooting down too many aircraft, especially compared to past successes. They realized they were executing so poorly in air-to-air combat because pilots were not exposed to adversaries’ techniques and capabilities*.”

Thus, the evolution of the air aggressors. As the U.S. Air Force’s mission portfolio grew, the aggressor program grew toward space, which is now known as the space aggressors.

“*We narrow our mission down to ‘know, teach, replicate*,” said Maj. *Sheri Lattemore*, a Canadian service member and director of operations, 527th SAS. “*We know and understand all the realistic and relevant threats and we teach those threats to different training audiences*.”

“*The 527th SAS has three mission sets which involve GPS electronic attack, satellite communications electronic attack and orbital engagement systems*,” she added. “*GPS electronic attack is when we put noise over the GPS signal so nobody can receive the signal on their receivers. We do the same thing for satellite communications; however, we will send our signal to the satellite itself so communication on the satellite is no longer possible. For orbital engagement systems, we play the role of the adversary against satellites*.”

These tactics are engaged as part of military training exercises isolated to controlled environments. At no time do aggressors use these tactics outside of coordinated and approved exercises.

To best prepare for the challenges they may face, the aggressors have an intelligence flight whose entire function is to research adversaries’ capabilities, weapons systems, limitations and how they’re going to employ those systems. The flight coordinates with the intelligence community to gather information.

The 527th SAS then conducts the teaching and replication part of their mission with the warfighters, including the Air Force, sister services, allies and coalition partners.

“*In the summer of 2016, we created a memorandum of agreement with the U.S. Army, then followed by the U.S. Navy*,” Lattemore said. “*We train them to do our mission, with the intent of creating their own aggressor units*.

“*We plan to have Canadians visit us to absorb as much information as they possibly can start their own GPS electronic attack unit*,” she added. “*Over the years I have been here, I’ve learned a lot about the policies and procedures, but also how to create an aggressor unit. We want to show them they can provide this training in Canada too*.”

On a year-round basis, the squadron participates in various exercises. The 527th SAS gathers intelligence and provides relevant and realistic training for the warfighters that helps enhance their situational awareness regarding adversary space systems. The space aggressors also participate in RED FLAG at Nellis Air Force Base, Nevada.

During those exercises, the 527th SAS conducts adversarial tactics including jamming satellite communications and GPS receivers in an attempt to teach warfighters the effects of the adversaries’ weapon systems. The friendly forces then attempt to identify and mitigate the problems associated with these effects.

“*For exercises, we work closely with the 26th SAS*,” Lattemore said. “*We support three RED FLAGS a year as well as weapons school integration, which is twice a year*.”

According to Capt. *Nathaniel Lee*, assistant to the flight commander for aggressor weapons and tactics, 527th SAS, the squadron is developing a threat replication program from the ground up, to be finalized this April. He explained the need for space aggressors is increasing because adversaries are always developing new capabilities. Lee reflected on what it means to be a part of the squadron.

“*We hear a lot in Air Force Space Command about the looming threat of combat in space,” he said. “Understanding the threats and developing tactics are centered on the aggressors. Knowing the space community is getting that out of this small organization is something we take a lot of pride in*.”

Story and photo by Senior Airman Arielle Vasquez
50th Space Wing Public Affairs. U.S.A.F.

NATIONAL SPACE SYMPOSIUM 2018

Keynote address—U.S.A.F. General John “Jay” Raymond

General Raymond’s presentation courtesy of Air Force Space Command

Good morning… I tell you, what a great morning… it’s great to be here (at the Space Symposium)… *General Shelton*, thank you for the kind remarks, the kind introduction, and thank you more importantly for your leadership, mentorship, and your friendship. I really value your counsel and I appreciate your being here and all you do for us.

Hats off to the Space Foundation for yet another great Space Symposium. Every year I say, “how are they going to do it, how are they going to raise the bar?” And every year they do, and it’s pretty easy to do so when you start off with the Vice President of the United States.

I was preparing for this talk and I found out that the Space Symposium and I have something in common — the first Space Symposium was held in 1984, the same year I began my Air Force career.

In 1984, only 250 people attended this symposium, and today I heard that a couple of weeks ago, the registration was cut off at about 14,000 attendees. I doubt for those who were here at the beginning that if you took a break and then came back today, you would not recognize the symposium as it is today. Congratulations once again to the Space Symposium for aging much more gracefully than me and thanks to the Broadmoor, as well. As I mentioned last year, if you are going to host an event, do it at the Broadmoor because it’s really hard to mess it up in a place like this.

Today is a really important day in the space business — 48 years ago today, Apollo 13 landed. As you all know that’s the famous mission carrying *Jim Lovell*, *Fred Haise* and *Jack Swigert*, in which Swigert reported, “***Houston, we’ve had a problem***.”

In between the 11th and 17th of April, NASA pulled together their tremendous team and, under the watchful eye of the entire American public, turned potential tragedy into triumph. I was just two weeks shy of my 8th birthday, and I remember very vividly being glued to my television set, not just for that but the entire Apollo program.

Although this past year may not have had the intensity of the week long Apollo 13 mission, especially for those Astronauts who were on board, I am convinced that when historians look back at 2017 and 2018, they will look back on this as one of the most critical times in our national security space history. It will be seen, in my opinion, as a strategic inflection point for national security space and a bold shift towards warfighting and space superiority.

So here we are at a Symposium that is not recognizable from when it started, with a speaker that may not be recognizable as well, and I am here to talk about national security space. If you haven’t been in the national security space business for the last year, then you don’t recognize it either. We have made historic advances this past year and I often say it’s an extremely exciting time to be in the space business.

In my opinion, there are three big reasons for this historic shift and advances that have been made.

First is a strategic alignment of vision, strategy, leadership, and resources. You have heard that throughout the beginning of this symposium.

Our partnerships with the National Reconnaissance Office, with our allies and commercial industry are extremely important and growing. There is a clear and better understanding of the potential threat and the implications of that threat to our national and the joint force.

First, that strategic alignment begins with the National Security and Defense Strategies. Our National Security Strategy states that the United States considers "unfettered access to and freedom to operate in space as a vital national interest."

It goes on to further state "any harmful interference with or an attack upon critical components of our space architecture that directly affect that vital U.S. interests, will be met with a deliberate response at a time, place, manner, and domain of our choosing."

The National Defense Strategy recognizes space as a warfighting domain and outlines the central challenges to U.S. prosperity and security as the reemergence of long term strategic competitors. The bold steps that we have taken over this past year enable us to compete, deter, and to win today and into the future.

Let me put this in Airmen's terms, I will say we have done a 9G turn towards space superiority. This 9G turn has been enabled by the strong leadership of our Secretary of the Air Force and out Chief of Staff of the Air Force. I first met Secretary Wilson 11 months ago and I took that picture on the left at the river entrance of the Pentagon when she was sworn in by the Secretary of Defense as our Secretary of the Air Force.

Less than 24 hours later, an official senate photographer took that picture on the right, it is a much less comfortable setting than the river entrance… but this picture again was taken less than 24 hours later when we testified to the Senate Armed Services Strategic Forces Subcommittee on Space. I will tell you from day one, Secretary Wilson has been a strong advocate and leader for our Air Force and for space. If you have an opportunity the Secretary of the Air Force is here for the next for days, shake her hand and say thank you.

The second half of this incredible leadership team is our Chief of Staff, I think he is landing at Peterson Air Force Base as we speak, he will be here the rest of the day and tomorrow. He is an Airmen's Chief, I call him a big 10 Chief, he is here for all airmen. He speaks very fluently about multi-domain operations and space. He has spoken many times on future warfare, specifically on the need to normalize and treat space as any other domain.

Let me read a quote from the Chief that he said at AFA in Orlando, "It's time for us as a service, regardless of specialty badge, to embrace space superiority with the same passion and sense of ownership that we apply to air superiority today."

We have a great Chief, for those who have the privilege of hearing him speak this afternoon I highly recommend you do so.

Last year when I spoke from this stage I had only have been in the job for the few months, so I did not have a lot of accomplishments yet, so I focused on history… it was the 70th anniversary of our Air Force and the 35th anniversary of Air Force Space Command.

I broke the history of the command into three distinct eras, the first was building the command in the first 9 years when we build and consolidated missions under Air Force Space Command just in time for Desert Storm.

Post Desert Storm we focused on integrating space capability to great effect, all the way up until I picked the demarcation of 2007 when China shot down their own weather satellite. I deemed that as a shift more toward space superiority.

I also talked about a Space Warfighting construct which stared with a CONOPS, having the ability to command and control, having space situational awareness, being able to go fast to develop the capabilities that we need to defend our constellations and critical partnerships.

Today I am not going to talk about a Space Warfighting Construct, because it does not exist anymore, it is a reality. Over the past year we have turned a construct into reality, and it all boils down to its just warfighting.

Let me say upfront I could spend hours talking about all the things we have done over the last year. But what I would like to do is highlight a few of the major accomplishments. Most were significantly enabled by a budget that was very friendly to space.

This year with the support of our Chief and Secretary and the Department of Defense, the President's budget submission includes almost 7 billion more for space.

We start with a concept of operations early on, I think this is the most significant accomplishment that we made. We wrote this concept of operations with the National Reconnaissance Office. This provided us the sheet music on how we are going to fight a fight that extends into space, and let me be very clear, we don't want to fight this fight. One way we are going to not fight it is to be ready to fight and win if deterrence should fail.

The NRO is the best partner we could ever have and I will tell you Betty Sapp is my best friend.

Next we wrote a C2 CONOPS and a Space Situational Awareness and Indications and Warning CONOPS, and presented those to General Hyten, our combatant commander, for approval. Those CONOPS have provided the sheet music for how we operate and have had great effect for both us and the National Reconnaissance Office.

Let's start with command and control, probably the most significant, on 1 December, General Hyten as part of a larger, broader STRATCOM C2 reorganization, stood up a four star space component command, dual-hatted me in that command and we stood down JFCC space. That elevation from a three-star to a four-star operational component has been significant.

It is more than just adding a letter to the name of an organization, it is significant in being able to integrate within U.S. Strategic Command andmaybeevenmoreimportantlyithasbeenextremelyvaluablebeing able to integrate with the geographic combatant commands around the world.

Last time when I spoke here we had something called the National Space Defense Center… it was still experimental. Today it is operational. We now have an operational space control center here in Colorado Springs that enables me to do the Joint Force Space Component job.

The JSpOC continues to mature, as well. We have focused the JSpOC on being able to provide those critical space capabilities to our joint warfighters and our allies. It is really clear today, just like any other domain, if we were to get into a conflict, we will do so with our allies.

We have worked very hard to strengthen our allied partnership at the JSpOC and, as General Hyten has directed, this summer we will transition the JSpOC to a Combined Space Operations Center, a CSpOC, that will further the integration of our critical allies into our capabilities.

If you have centers, you also have to have a system that can command and control, so this year we transitioned away from what we call the JSpOC Mission System Increment 3, a C2 system, and entered into a partnership with the Air Force Rapid Capabilities Office, Air Force Research Lab and Space and Missile System Center and we developed a program called Enterprise Space Battle Management Command and Control.

It is a system that is open architected, fueled by industry consortium, built to enable speed and innovation and multi-domain integration that will be absolutely critical going forward. The progress on this system to date has been nothing short of remarkable and I am extremely excited for the transformational capabilities it will deliver.

Stemming from the work that we did with the NRO in developing the CONOPS for Space Situational Awareness, we also focused significantly on Space Situational Awareness.

I just spoke about command and control — from that CONOPS we then canceled a program because it was not going to meet our mission needs and we entered into a partnership with the NRO on a joint Space Situational Awareness program which will provide better capability that meets our mission needs at a cheaper cost than what we have had in the past.

Moving to defensible architectures, as part of this 9G turn toward space superiority, you have to have architectures that are dependable. We have taken several bold steps over the course of this last year to move in that direction.

First and probably most importantly, in missile warning we recognize that the current OPIR was robust and affords us the opportunity to stake a step forward and that's what we have done.

We have taken a significant leap in this President's Budget to getting to a next-generation missile warning capability which will provide us with critical missile warning capability for our nation, but will also be dependable.

On SATCOM, we have done the same thing; we have re-architected the SATCOM architectures to be more defendable. I would like to highlight one aspect of that, which is a partnership that we have entered into with Norway to host payloads on their satellites and will provide us the ability to get satellites into orbit two to three years earlier than what we could have done if we had built our own satellites.

Rapid acquisition, Lt. Gen. J. T. Thompson, the Space and Missile Systems Center Commander, will talk later on this week, but we have made great strides in moving fast, as well. Consistent with the National Defense Authorization Act of this past year, we have renamed the Operationally Responsive space Office into a Space RCO, Rapid Capabilities Office.

Renaming is good, but is not sufficient. Now we are in the process of building that capability to be an exact clone of the RCO, Rapid Capabilities Office that we have in other domains. We are going to build this clone with the same level of leadership, authorities, and resources that are necessary to deliver on the timeline that we need.

I mentioned, as well, that partnerships are absolutely critical to us. To be honest, when space was a benign domain, they were not all that important, because you did not have to worry about something on orbit once it successfully survived launch.

Today's partnerships are vital in the contested space environment — partnerships strengthen our advantage and complicate potential adversary decision making.

I have already highlighted a couple of partnerships thought this speech but let me move forward and highlight a few more. I can't emphasize enough about the strong partnership we enjoy with the National Reconnaissance office, it has never been stronger and it's a source of great strength to both organizations.

We have made significant advances that would not have been possible even just a few years ago. On the commercial front, we are not only working internal to the government, but we have several partnership opportunities that we are partnering with commercial. Those range from launch to re-entry and everything in between.

Let me highlight launch — the commercial launch industry is going to enable us to fundamentally transform how we do launch and range operations in the future.

This year, the 45th Space Wing down at Patrick Air Force Base has a goal of reaching 48 launches in one year. To put that into perspective, 48 launches is more than half of the 90 launches accomplished worldwide this year. We couldn't do this without transitioning to autonomous launch operations.

Historically, when we conducted launches, we had radars and telemetry dishes and optical capabilities and command destruct capabilities to protect public safety. We would bring in a crew to operate those capabilities and we had individuals on the consoles to blow up a rocket if it went astray.

The commercial industry moved in a different direction and are moving us towards autonomy, which will reduce manpower and cost significantly and allow us to go faster and have more opportunities to access space.

We have chartered a team that is currently building the future launch and range vision and the goal is to get to all autonomous ranges in the near future. This will pay significant dividends not just for us, but the entire space industry.

I have mentioned our efforts to pattern in operations and development with our international coalition of allies and partners, we also do this in training.

One example is the Schriever Wargames. It's an annual exercise and in that exercise are our Five Eye partners. Over the last few years, we have added France and Germany, and this year we have expanded it even further and Japan will be participating in the Schriever Wargames.

Just like in the F-22, that 9G turn for us is not possible without the Airmen to pilot it. We are investing in the development of our space workforce accordingly. In the FY19 budget submittal we have added approximately 175 million dollars to training infrastructure which directly enhances our warfighting readiness.

This includes increasing exercise and training opportunities for space operations teams as well as funding the development of space training simulators that will mirror where the broader Air Force is going in live, virtual and constructive environments.

One of the critical things we have developed is something called Space Flag. I know you all have heard of Red Flag and understand the importance of Red Flag in developing our Airmen before they get into a fight — Space Flag is the same thing for the Space Domain.

We did two last year and this year Space Flag is going on as I speak here in Colorado Springs — we will do two this year and next year we will do three. They have already provided significant dividends.

The Secretary and Chief have also tasked Air Force Space Command to do a review of space professional development and the space force structure. We have a team that has been built to accomplish that study, we will out brief the Chief and Secretary here in a few months.

Over the last year we have already made some pretty significant strides in developing the space leaders that we need to operate in a contested environment.

That takes me to the wrap up point, I have just taken a whirlwind tour through the efforts that have gone on over the past year. Any one of those would have made a big year, I could write another book on things we are also doing that I have not talked about. Focusing on C2, defendable architectures, Space Situational Awareness, partnerships and developing our Airmen.

The reason we dominate as an Air Force is because of our Airmen. What I would like to do is highlight a few of our Airmen I am privileged to lead as part of Air Force Space Command and Joint Force Space Component Command.

Airmen who are selfless and courageous, such as 1st Lt. *Dominic Vicino*, please stand up. Dom, thank you. Dom was a water polo player at the Air Force Academy, he is stationed down at Eglin… he was at the beach, he knows the currents are really bad and he notices two people that are drowning and he jumps in to save them. While he is doing that, a life guard jumps in but starts to drown, as well. So Dominic pulls three people out of the water, saves three lives and earns the Airman's Medal. Dominic, thanks for being here.

Just as swimming on the beach is not a spectator sport, neither is space superiority — as our Chief says, it has to be trained for and fought for. Our Airmen are doing just that. As I talked about Space Flag and the advanced training that we have been doing, there is an Airman who has been the principle architect of that, Major *Kenny Grosselin*. Kenny, please stand up. Kenny is a graduate weapons officer and is now transforming our weapons school to better train operators for the environment that they face today. He has also been a principal architect of the advanced training we have done and the Space Flag exercises I just spoke about. Kenny I really appreciate all of your hard work and expertise, thanks you.

The other thing is that if you are going to have space superiority, you can't do it from home, you have to deploy. Our Airmen in Air Force Space Command answer the call to deliver space superiority to our nation and our allies, TSgt Pat Thompson please stand.

Pat deployed in support of Operation Inherent Resolve proving critical space effects to the CENTCOM AOR and then redeployed again to Afghanistan in support of Operation Freedom Sentinel and Operation Resolute Support. Pat I can't thank you enough for your selfless service making sure that our joint warfighters and allies they Another Airman that I brought with me today is part of that ground breaking organization I spoke about earlier, the National Space Defense Center, SSgt Adam Swift, please stand.

Adam's full time job is focusing on space superiority, he was the first pick to help stand up the National Space Defense Center, he has been there since the beginning. It's kind of like kids and they are growing up and people have not seen them for a while, they come over and say "look how tall they have gotten," — same thing with the National Space Defense Center. If you have not been there in a while and you go, you will say "look at all the advances we have made." It's because of Airmen like Airman Swift, so thank you for all you have done, we appreciate your expertise.

Finally, our last Airman is a civilian airman, Dr. *Mark Eddings*… Mark is a principle architect of something we call the space TTX, a tabletop exercise that our Chief and Secretary asked us to put together and provide to the entire senior leadership of the Air Force… we have given it to every level of our government including the Vice President, Secretary of Defense, Deputy Secretary of Defense, Chairman of the Joint Chiefs, STRATCOM commander, other joint force commanders and congress. It has had a huge impact, so Mark thank you for your expertise and the work you did on that is nothing short of heroic and we really appreciate that.

Just I have highlighted the five amazing Airmen, I wish I could highlight all 35,000 of them, because I am privileged to lead a group of people that are all equally impressive. I do have one more person to recognize, but he is not an Airman. Under my new joint hat for U.S. Strategic Command, I have a growing joint team to help me with my joint role.

One of those is Army Major *Jerry Micka*. He is a former engineer branch officer who is now an Army space operator, he is stationed at Vandenberg as a chief of current operations at the JSpOC, he was our lead for tracking the reentry of the Chinese space station. That was a heroic effort pulling in partners from all over the world. I appreciate your support, thank you for what you do out at Vandenberg.

So space superiority is a core mission of the United States Air Force. As I mentioned throughout this speech, we are making a 9G turn with very bold steps to get there. The need to gain and maintain space superiority is not just an Air Force requirement, it is a joint requirement and in the future the entire joint force will be called upon for its full spectrum of capabilities, not just to gain abilities from space effects, but to gain and maintain the space superiority that we need. Said in a different way, space superiority is not just a space officer's task, it's a joint warfighter's task.

Thank you, and thank you very much for all you do for Air Force Space Command, we can't do this without you, these are always great events to network and share ideas and thoughts, and I really appreciate the attendance.

www.spacefoundation.org

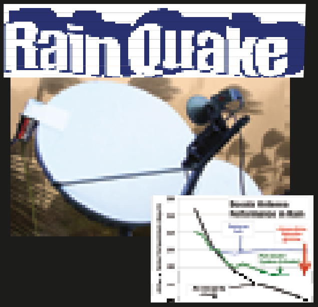
www.spacesymposium.org

www.afspc.af.mil/

WALTON DE-ICE
We Cover the World
#1 in Antenna De-Icing Worldwide
Protecting Networks From Snow & Ice

Hot Air
De-Ice

Ice Quake
Snow Shield


Rain Quake

GLOBAL PROLIFERATION OF COUNTERSPACE CAPABILITIES AND SPACE SUSTAINABILITY

By Dr. Brian Weeden, Director of Program Planning, and Victoria Samson, Washington Office Director, Secure World Foundation (SWF)

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth, but also more congestion and competition in space.

From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. The growing use of, and reliance on, space for national security has also led more countries to look at developing their own counterspace capabilities that can be used to deceive, disrupt, deny, degrade, or destroy space systems.

The existence of counterspace capabilities is not new, but the circumstances surrounding them are. Today there are increased incentives for development, and potential use, of offensive counterspace capabilities. There are also greater potential consequences from their widespread use that could have global repercussions well beyond the military, as huge parts of the global economy and society are increasingly reliant on space applications. Yet, because national security in space is so highly classified, it is difficult to have an open, public debate about counterspace programs.

ESA infographic of the company's Space Situational Awareness program. The objective of the SSA program is to support Europe's independent use of, and access to, space through the provision of timely and accurate information, data and services regarding the space environment, and particularly regarding hazards to infrastructure on orbit and on the ground. Image credit: ESA-P, Carril

Our hope is that the existence of this unclassified analysis may help facilitate public discussions about the policies of counterspace.

To address this, SWF recently published an open source assessment of global counterspace capabilities. SWF convened a group of international experts to work with our staff to compile publicly-available information for various countries developing counterspace capabilities across several categories: ***direct ascent***, ***co-orbital***, ***directed energy***, ***electronic warfare*** (EW), and ***cyber***.

For each of these categories, SWF assessed what the current and near-term capabilities might be for the countries examined in the report, based on the open source information. Also assessed was the potential military utility for each capability, which includes both the advantages and disadvantages of the capabilities.

Finally, when possible, we also examined each country's policy, doctrine, and budget to support the offensive counterspace capabilities being developed. Taken together, the analysis is intended to provide a more holistic picture of what each country is working on, and how these capabilities may be used.

Summary of Counterspace Capabilities

The conclusions of the report are worrying, but also provide a ray of hope. The publicly available evidence shows significant research and development of a broad range of kinetic (i.e. destructive) and non-kinetic counterspace capabilities by multiple countries. However, only non-kinetic capabilities are actively being used in current military operations.

Over the last decade, the testing of non-kinetic capabilities has been limited in ways that do not create large amounts of orbital debris. This suggests that countries feel there are still some normative and legal restraints on both the testing and use of counterspace weapons, and that widespread conflict in space is not yet inevitable. The following sections provide a bit more detail on the counterspace activities of several countries and capabilities.

China

The evidence strongly indicates that China has a sustained effort to develop a broad range of counterspace capabilities.

China has conducted multiple tests of technologies for close approach and rendezvous in both Low Earth Orbit (LEO) and Geosynchronous Orbit (GEO) that could lead to a co-orbital ASAT capability. However, as of yet, the public evidence indicates they have not conducted an actual destructive intercept of a co-orbital target, and there is no proof that these rendezvous and proximity operations (RPO) technologies are definitively being developed for counterspace use as opposed to intelligence gathering or other purposes.

China has at least one, and possibly as many as three, programs underway to develop direct ascent anti-satellite (DA-ASAT) capabilities, either as dedicated counterspace systems or as mid-course missile defense systems that could provide counterspace capabilities.

China has engaged in multiple, progressive tests of these capabilities since 2005, indicating a serious organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and may be operationally fielded on mobile launchers within the next few years. Chinese DA-ASAT capability against deep space targets — both Medium Earth Orbit (MEO) and GEO — is likely still in the experimental or development phase, and there is not sufficient evidence to conclude whether it will become an operational capability in the near future.

Although official Chinese statements on space warfare and weapons have remained consistently aligned to the peaceful purposes of outer space, privately they have become more nuanced. China has recently designated space as a military domain, and military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance.

That being said, it is uncertain whether China would fully use their offensive counterspace capabilities in a future conflict or whether the goal is to use them as a deterrent against U.S. aggression. There is no public evidence of China actively using counterspace capabilities in current military operations.

Russia

There is strong evidence that Russia has embarked on a set of programs over the last decade to regain some of its Cold War-era counterspace capabilities.

Since 2010, Russia has been testing technologies for close approach and rendezvous in both LEO and GEO that could lead to a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. However, the technologies could also be used for non-aggressive applications, and the on orbit testing done to date does not conclusively prove they are for an ASAT program.

Russia is almost certainly capable of some limited DA-ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to U.S. space assets. Core Russian direct-ascent ASAT capabilities are not yet operational, and those currently in development are not planned to have the capability to threaten targets beyond LEO. Russia appears highly motivated to continue development efforts even where military utility is questionable, due at least in part to bureaucratic pressures.

Russia places a high priority on integrating EW into military operations and has been investing heavily in modernizing this capability. Most of the upgrades have focused on multifunction tactical systems whose counterspace capability is limited to jamming of user terminals within tactical ranges. Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of unmanned aerial vehicles (UAVs), guided missiles, and precision guided munitions, but has no publicly known capability to interfere with the GPS satellites themselves using radio frequency interference.

The Russian Army fields several types of mobile EW systems, some of which can jam specific satellite communications user terminals within tactical ranges. Russia can likely jam communications satellites uplinks over a wide area from fixed ground stations facilities. Russia has operational experience in the use of counterspace EW capabilities from recent military campaigns.

Russia has a strong technological knowledge base in directed energy physics and is developing a number of military applications for laser systems in a variety of environments. Russia has revived, and continues to evolve, a legacy program whose goal is develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no indication that an operational capability has been yet achieved.

Although not their intended purpose, Russian ground-based satellite laser ranging (SLR) facilities could be used to dazzle the sensors of optical imagery satellites. There is no indication that Russia is developing, or intending to develop, high power space-based laser weapons.

Russian military thinkers see modern warfare as a struggle over information dominance and net-centric operations that can often take place in domains without clear boundaries and contiguous operating areas. To meet the challenge posed by the space aspects of modern warfare, Russia is pursuing lofty goals of incorporating EW capabilities throughout its military to both protect its own space-enabled capabilities and degrade or deny those capabilities to its adversary.

In space, Russia is seeking to mitigate the superiority of U.S. space assets by fielding a number of ground, air, and space-based offensive capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

United States

The United States has conducted multiple tests of technologies for close approach and rendezvous in both LEO and GEO, along with tracking, targeting, and intercept technologies that could lead to a co-orbital ASAT capability.

These tests and demonstrations were conducted for other non-offensive missions, such as missile defense, on-orbit inspections, and satellite servicing, and the United States does not have an acknowledged program to develop co-orbital capabilities. However, the United States possesses the technological capability to develop a co-orbital capability in a short period of time if the nation chooses to do so.

While the United States does not have an operational, acknowledged DA-ASAT capability, it does have operational mid-course missile defense interceptors that have been demonstrated in an ASAT role against low LEO satellites. The United States has developed dedicated DA-ASATs in the past, both conventional and nuclear-tipped, and likely possesses the ability to do so in the near future should it choose to.

The United States has an operational EW counterspace system, the Counter Communications System (CCS), which can be deployed globally to provide uplink jamming capability against geostationary communications satellites. The United States likely has the capability to jam global navigation satellite service receivers (GPS, GLONASS, Beidou) within a local area of operation to prevent their effective use by adversaries.

In addition to interfering with adversarial use of satellite navigation, the **Navigation Warfare** program seeks to assure the availability of GPS services for U.S. military units in operations. The effectiveness of measures to counter adversarial GPS jamming and spoofing operations is not known.

The United States has had established doctrine and policy on counterspace capabilities for several decades, although not always publicly expressed. Most U.S. presidential administrations since the 1960s have directed or authorized research and development of counterspace capabilities, and in some cases greenlit testing or operational deployment of counterspace systems. These capabilities have typically been limited in scope, and designed to counter a specific military threat, rather than be used as a broad coercive or deterrent threat. The U.S. military doctrine for space control includes defensive space control (DSC) and offensive space control (OSC), and is supported by space situational awareness (SSA).

Since 2014, U.S. policymakers have placed a heightened focus on space security, and have increasingly talked publicly about preparing for a potential "*war in space*", speaking openly about space being a warfighting domain. This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems.

It is possible that the United States has also begun development of new offensive counterspace capabilities, although there is no publicly-available policy or budget direction to do so. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

Iran

Iran has a nascent space program, building and launching small satellites that have limited capability.

Technologically, it unlikely Iran has the capacity to build on orbit or direct-ascent anti-satellite capabilities, and little military motivations to do so at this point. Iran has demonstrated an EW capability to persistently interfere with commercial satellite signals, although the capability against military signals is difficult to ascertain.

North Korea

North Korea has no demonstrated capability to mount kinetic attacks on U.S. space assets: neither a direct ascent ASAT nor a co-orbital system.

In their official statements, North Korea has never mentioned anti-satellite operations or intent, suggesting that there is no clear doctrine in Pyongyang's thinking at this point. North Korea does not appear motivated to develop dedicated counterspace assets, though certain capabilities in their ballistic missile program might be eventually evolved for such a purpose. It is unlikely that North Korea would use one of its few nuclear weapons as an electromagnetic weapon.

North Korea has demonstrated the capability to jam civilian GPS signals within a limited geographical area. Their capability against U.S. military GPS signals is not known. There has been no demonstrated ability of North Korea to interfere with satellite communications, although their technical capability remains unknown.

India

India has more than five decades of experience with space capabilities, but most of that has been civil in focus and only over the past several years has India started organizationally making way for its military to become active users and creators of its space capabilities.

India's military has been developing an indigenous missile defense program that its supporters argue could provide a latent ASAT capability, should the need arise; this capability has not been tested. It is possible that India would move into rapidly testing an ASAT if it felt that the international community was getting close to creating an international legal regime banning kinetic ASAT tests; otherwise, given the substantial investment the Indian military is making in its satellite capacity and the income that India is receiving from launching other countries' satellites, it is unlikely that they will move to actively create an official counterspace program.

Cyber Capabilities

Multiple countries possess cyber capabilities that could be used against space systems; however actual evidence of cyber attacks in the public domain are limited, due to concerns about classification and/or the unwilling sharing of proprietary information.

The United States, Russia, China, North Korea, and Iran have all demonstrated the ability and willingness to engage in offensive cyber attacks against non-space targets. Additionally, a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors.

There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems that create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyber attacks capabilities of leading nation-states and other actors.

Implications for Commercial Space Sector

The global proliferation of counterspace capabilities has significant implications for the future of space commercialization. The increased instability created by a counterspace arms race could itself impede or retard the growth of space commercialization.

Today we are seeing a rapid expansion of investment and innovation in commercial space activities around the world. Many countries are putting in place policies to encourage commercial space development and hope to reap the socioeconomic benefits that may result. However, as is the case with other domains, geopolitical instability and uncertainty are not conducive to business growth and investment. As the rhetoric about potential armed conflict in space heats up, investors and insurers may be less likely to see space as a risk worth taking.

Actual armed conflict in space could have devastating consequences for commercial space. Governments are increasingly turning to commercial services and capabilities to augment their own, which creates the possibility that commercial satellites and space services could be targets during an armed conflict.

Even if commercial satellites are not directly attacked, widespread electronic warfare attacks against military satellites would likely also cause significant service disruptions for nearby commercial satellites. Use of destructive kinetic weapons against military satellites would likely create large amounts of space debris, which could increase the risk to commercial space operations for decades. There are a few steps that the commercial space community can take to help prevent these dire outcomes.

The first is to help develop norms of behavior for commercial space activities, and in particular those that use dual-use technology such as rendezvous and proximity operations. As has been the case in other domains, norms of behavior can help militaries discriminate between normal commercial activity and potential threats and reduce the chances of misperceptions or mistakes that could trigger crises or increase tensions. Even if the norms are only applied to commercial activities, they are still likely to have an influence on how military space operations are conducted, as is the case in the air and maritime domains. In addition, commercial actors should also work to increase sharing of space situational awareness data that can reinforce norms of behavior and further increase the transparency of space activities.

SWF also encourages commercial space actors to get more involved in the space security debate. Commercial entities need to ensure that their interests and perspectives are well-represented in debates and discussions on policies and strategies for dealing with the proliferation of counterspace capabilities. Commercial space actors need to ensure governments fully understand the implications of aggressive strategies that could increase instability and uncertainty, and may increase the chances of armed conflict extending into space.

Implications for Militaries and National Security

The global proliferation of counterspace capabilities has significant implications for future military use of space and the potential for conflict on Earth.

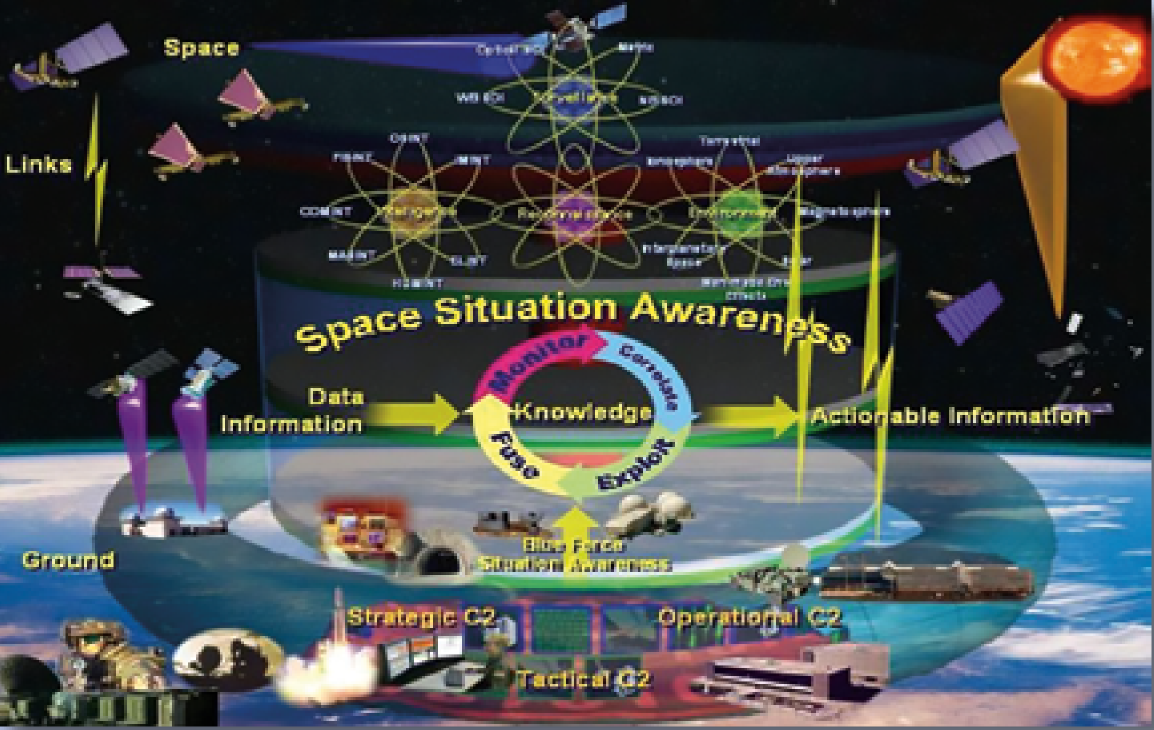
The increased reliance on space capabilities to support and enhance military activities on Earth is driving the proliferation of counterspace capabilities. The offense-dominant nature of the space domain makes it easier to attack space capabilities than defend them, which could lead to an arms race during peacetime and create instabilities during crises that escalate to armed conflict. During an actual armed conflict, there may be incentives to use offensive counterspace capabilities early in the conflict, either as an attempt to deter further attacks or to seize a military advantage.

Widespread use of offensive counterspace capabilities during an armed conflict would have devastating humanitarian consequences. While today's wars are by no means devoid of tragedy and suffering, the precision strike complex enabled by space capabilities has led to drastically fewer civilian casualties than during previous wars between great powers. Instead of firebombing entire cities or dropping millions of pounds of bombs across vast stretches of countryside, space allows for a much more precise application of force than was previously possible, and more stringent application of international humanitarian law to protect non-combatants. Eliminating space from the equation would likely force militaries to fall back on older methods and greatly increase the loss of life and suffering. Additionally, the distinction between military and non-military use of space is increasingly blurred and it is likely attacks on some military space capabilities may have significant civilian impacts.

There are steps governments can take to minimize these negative consequences. **First**, they can focus more on increasing the resilience of space capabilities against attacks. Doing so in a way that is visible to potential adversaries could help deter the most devastating kinds of attacks on space capabilities, and if deterrence fails would ensure space capabilities degrade more gracefully and retain at least some military utility throughout the conflict.

Second, there needs to be a better understanding of how international law, and specifically the law of armed conflict (LOAC) and international humanitarian law (IHL), applies to armed conflict in space. Examples of this are the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (***ihl-databases.icrc.org/ihl/INTRO/560?OpenDocument***), the *HPCR Manual on International Law Applicable to Air and Missile Warfare* (***assets.cambridge.org/97811070/34198/frontmatter/9781107034198_frontmatter.pdf***) and the *Tallinn Manual on International Law Applicable to Cyber Operations* (***ccdcoe.org/research.html)***, which all provide guidance on the application of IHL for the maritime, air, and cyber domains, respectively.

These manuals were developed by experts and practitioners to provide advice to military lawyers on the application and use of IHL in their respective domains. While not binding agreements, the manuals have nonetheless had an impact on how militaries conduct activities in peacetime, periods of tension, and armed conflict.



*Lockheed Martin is providing the Commonwealth of Australia with an iSpace space situational awareness training and demonstration mission system. iSpace collects data from a worldwide network of government, commercial and scientific community space surveillance sensors to provide space situational awareness and space command and control. Image is courtesy of Asia-Pacific Research (**www.asia-pacificresearch.com/**)*

In addition, governments need to discuss strengthening norms or even binding legal prohibitions against the use of offensive counterspace capabilities that are deemed unacceptable. In every other domain of warfare, governments have largely agreed that certain types of weapons, such as flamethrowers, chemical or biological weapons, or flechettes, should be prohibited because they cannot be used in a way that discriminates against lawful and unlawful targets or cause undue suffering. But in the space domain, this topic has largely gone undiscussed, in part because space arms control has traditionally focused on controlling technology instead of behavior. And also because this approach represents a middle ground between prohibiting all conflict in space and allowing complete freedom of action that neither side wants to compromise on.

Finally, there needs to be continued progress made on improving space situational awareness (SSA) for all space actors, as it is the foundation for all of these steps. Improved SSA will help militaries better discriminate between non-hostile malfunctions and accidents and hostile threats, and also better defend satellites against all types of threats.

Improved SSA will also enable better understanding of space activities that lead to development of norms of responsible behavior in space, and could be used to verify future legally-binding agreements that restrain deployment or use of prohibited counterspace capabilities.

swfound.org/

Dr. Brian Weeden is the Director of Program Planning for Secure World Foundation and has nearly two decades of professional experience in space operations and policy.

Dr. Weeden directs strategic planning for future-year projects to meet the Foundation's goals and objectives, and conducts research on space debris, global space situational awareness, space traffic management, protection of space assets, and space governance. Dr. Weeden also organizes national and international workshops to increase awareness of and facilitate dialogue on space security, stability, and sustainability topics. He is a member and former Chair of the World Economic Forum's Global Future Council on Space Technologies, and is also a member of the Advisory Committee on Commercial Remote Sensing (ACCRES) to the National Oceanic and Atmospheric Administration (NOAA).

Prior to joining SWF, Dr. Weeden served nine 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), Dr. Weeden directed the orbital analyst training program and developed tactics, techniques and procedures for improving space situational awareness.

Read Dr. Weeden's publications
swfound.org/about-us/staff-publications/publications-by-dr-brian-weeden/.

Victoria Samson is the Washington Office Director for Secure World Foundation and possesses 20 years of experience in military space and security issues. Before joining SWF, Ms. Samson served as a Senior Analyst for the Center for Defense Information (CDI), where she leveraged her expertise in missile defense, nuclear reductions, and space security issues to conduct in-depth analysis and media commentary. Prior to her time at CDI, Ms. Samson was the Senior Policy Associate at the Coalition to Reduce Nuclear Dangers, a consortium of arms control groups in the Washington, D.C. area, where she worked with Congressional staffers, members of the media, embassy officials, citizens, and think-tanks on issues surrounding dealing with national missile defense and nuclear weapons reductions. Before that, she was a researcher at Riverside Research Institute, where she worked on war-gaming scenarios for the Missile Defense Agency's Directorate of Intelligence.

Read Ms. Samson's publications
https://swfound.org/about-us/staff-publications/publications-by-victoria-samson/

THE NEW WARFIGHTING DOMAIN

A solution to tackle cybersecurity in tactical communications

By Charlie Kawasaki, Chief Technical Officer, PacStar

Cyber has emerged as a new warfighting domain. From fears of Russian hackers disrupting tactical networks to ISIS threatening a global cyberattack, the risk continues to grow as adversaries are now equipped with cyber and electronic warfare (EW) capabilities.

Accordingly, the **Department of Defense** (DoD) is now considering cyber at the same level as traditional land, sea and air warfighting domains.

At the same time, the inevitable shift underway to an Internet of Battlefield Things (IoBT) multiplies cyber risks. In a new paper by *Alexander Kott*, chief of the **Network Science Division at the Army Research Laboratory**, he surmises that, *"numerous, artificially intelligent, networked things will populate the battlefield of the future, operating in close collaboration with human warfighters, and fighting as teams in highly adversarial environments."*

More interconnected devices and sensors on the battlefield introduce cyber vulnerabilities that U.S. adversaries can exploit for maximum damage.

For these reasons and others, delivering cybersecurity on the battlefield and in tactical settings to guarantee secure communications offers a unique challenge, as the DoD must overcome a variety of factors including:

- ***Limited Visibility into Cyber Threats***
  Cybersecurity technologies today are too large and expensive to deploy. The result is that tactical networks are not equipped with the mobility and scalability needed in a cyber warfighting environment. Without the correct technologies in place, soldiers' views into the threat landscape can be restricted and even at times inaccurate, as real-time situational awareness of cyber threats is impaired

- ***Shortage of Cybersecurity Skills in Tactical Settings***
  A response to cybersecurity threats on the battlefield must come in real-time, as the difference between waiting hours and days versus seconds and minutes to respond could have dire consequences. Yet the shortage of cyber specialists that can be

readily deployed and available in tactical environments makes real-time response difficult, if not impossible. And even for tactical operators in the field, maintaining multiple systems can be overwhelming.

- ***Poor Cybersecurity at the Edge***
  The electronic footprints of current tactical networks are often easy to discover. And the closeness of adversaries in battlefield environments makes it easier for communications to be intercepted, which is all the more heightened given how tactical networks are traditionally dispersed. Internal and external cyber threats at the edge of the network challenge the DoD when it comes to rapid detection and response.

It's true that the DoD faces many challenges when it comes to the battle against cyber adversaries, but steps are being taken to close the gap. The U.S. Army, for example, continues to modernize its network, while the DoD raised **U.S. Cyber Command** to a unified combatant command, a move strengthened by the president's request of $647 million for Cybercom in fiscal year 2018. This represents a 16 percent boost from the previous year, in efforts to help the command bolster its cyber capabilities.

A Solution to Address Cyber Gaps

Current gaps in tactical cybersecurity capabilities cannot be viewed solely as a manpower and policy challenge. Vendors must also step up to provide solutions and demonstrate what is possible.

One answer lies in using small form-factor (SFF) modular solutions that offer automated detection and response to cyber threats and address the unique conditions that warfighters face. PacStar develops and supplies advanced communications solutions for the DoD and recently partnered with **Fidelis**, a leader in automated threat detection and response, to launch a joint solution that helps fill gaps in cyber operational efficiencies in a warfighter environment where resources are limited.

The **PacStar Tactical Fidelis Cybersecurity System** is a small-form factor and ruggedized solution employed with response capabilities to protect the plethora of communication use cases that warfighters in the battlefield must handle, including vehicle mount, in-theater communications, forward operating base deployments, and executive communications.

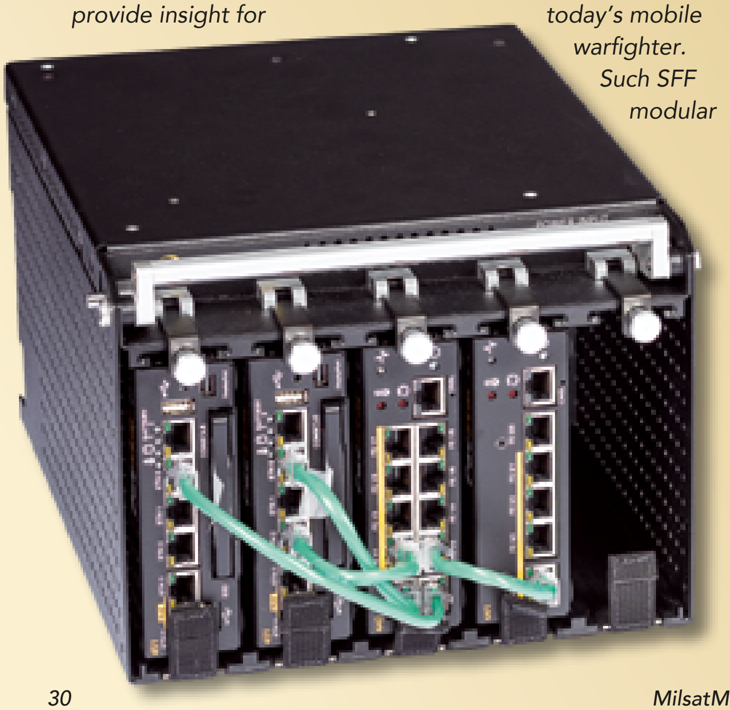
Providing the **Fidelis Elevate**™ platform in a rugged compact, form factor, the system is ideal for meeting the demanding size, weight, power and reliability requirements necessary for military tactical cyber defensive operations. This includes pre-positioned cyber sensors and deployable "hunt mission" kits.

Network specialists are able to easily facilitate and manage tactical configuration and troubleshooting thanks to the system's "single-pane of glass" approach to incident response, which is made possible by the implementation of PacStar IQ-Core Software.

Providing automated detection and response to cyber threats in tactical and deployable systems is key to secure communications. Moreover, the PacStar Tactical Fidelis Cybersecurity System is designed to address the specific limitations that make secure communications in the battlefield so difficult, including:

- *Improving Situational Awareness — The system offers enhanced visibility to remote cyber defender support organizations that traditionally do not have the real-time insight necessary to support the warfighter environment, including threat analytics capabilities. High speed network security analytics means that network session metadata can be indexed and stored long term, equipping warfighters with a more complete picture of the threat landscape over time and thus the ability to more quickly detect patterns and flag abnormalities. And the compact, quick setup of the system means that capabilities can be quickly up and running to provide insight for today's mobile warfighter. Such SFF modular solutions are key to addressing security gaps in the field where time, equipment and manpower are limited.*

- *Simplifying Incident Response Detection — Given the limited availability of cyber experts in the field, cyber incident response tools must be easy to implement and deploy. This system simplifies that process thanks to automated detection and*



validation of alerts. Moreover, the system determines the appropriate response and suggests to soldiers the best course for resolution. Such an approach equips entire units with integrated cybersecurity knowledge while limiting the number of warfighters having to undergo the extensive training typically shouldered by a cybersecurity specialist. Moreover, soldiers can confidently address cyberthreats immediately without having to waste precious time waiting for a cyber specialist to arrive and confirm or refute the proposed response.

- *Bolstering Security at the Tactical Edge — The small size, weight and power of the system makes deployment at the edge possible. For networks traditionally lacking protection, this system provides real-time cyber threat detection and response. System capabilities include running malware detection and intrusion prevention. Warfighters are often hard-pressed to find such abilities in resource-constrained environments that typically characterize the modern-day battlefield.*

The PacStar Tactical Fidelis Cybersecurity System is based on a PacStar 451 module that hosts analytics, management and sensor functions (*see image on the previous page*). With sizeable deployments, additional PacStar 451 and 455 modules can be added to provide large, long-term, meta-data storage requirements, offering flexibility as the environment evolves and warfighter needs change. Supplemented with PacStar 400-series routing and switching modules, the system can be delivered as a complete all-in-one solution.

Both PacStar and Fidelis have extensive experience supporting enterprise customers, federal civilian, defense, and intelligence agencies, as well as government integrators and defense industrial based contractors.

Beyond the military, the PacStar Tactical Fidelis Cybersecurity solution is ideal for field operations including Homeland Security, first responders, oil and gas companies, and other industries that face similar challenges as DoD. Confronting cybersecurity capabilities on the front line of tactical communications is an immediate need as the cyber threat continues to advance.

Securing communications across multiple devices and operating systems is no easy task, but it must be a priority for the DoD. Accordingly, vendors such as PacStar and Fidelis will continue to innovate and provide solutions to better equip the federal government to tackle the growing threat of cybersecurity.

Charlie Kawasaki is CTO for PacStar, developer of secure tactical communications solutions. He has 35 years' experience in product development, software engineering, technology licensing, patent development, business development, product marketing, general management and M&A.

pacstar.com/

www.fidelissecurity.com/

OVERCOMING THE LARGEST THREATS TO MILITARY SATELLITES AND INCREASING RESILIENCY

By Ryan Schradin, Senior Contributor and Executive Editor of SES-GS' Government Satellite Report

Every satellite-focused discussion involving experts from the military and Department of Defense (DoD) over the past half-decade has had at least some time dedicated to the topic of the threats facing military satellite networks — and for good reason.

The once benign operating environment of space is now a heavily congested and contested environment. This means that satellites that were built and launched without mission assurance capabilities now operate in a domain where they could be compromised.

When you consider the mission-critical services that military satellites provide — and the essential capabilities and communications they deliver to — it becomes abundantly clear why this topic dominates so many military space discussions.

Compromising or neutralizing a military satellite now means that Americans have to go without essential communications connectivity, Intelligence, Surveillance and Reconnaissance (ISR) data and mission-critical network applications and tools. These types of mission degradations would have immediate and negative impacts on lethality, and on the survivability of American troops.

Defending a Contested Space Domain

It comes as no surprise that defending satellites was once again the hot topic of discussion during a Defense One-organized, "*Cocktails and Conversations*," event that was recently held in Washington D.C.

"*It's going to be a combination of proliferation, disaggregation, diversity, distribution, protection, proliferation and deception. Those factors can combine for any space capability that we know about to make them resilient...*" — **Douglas Loverro**, President of **Loverro Consulting, LLC.**

This event included a number of military satellite decision makers and thought leaders, each with incredible depth of experience and knowledge into the military's satellite challenges and requirements. Present on the panel were:

- *Douglas Loverro: President of Loverro Consulting, LLC and Former Deputy Assistant Secretary of Defense for Space Policy*
- *Colonel George R. Nagy: Chief of the Space Support to Operations Division at the Pentagon*
- *Deanna Ryals: Chief of the International Programs Division within The MilSatCom Systems Directorate at the Space and Missile Systems Center, Air Force Space Command*
- *Dr. Brian Weeden: Director of Program Planning at the Secure World Foundation*

The conversation began with basic overviews about DoD satellite strategy and the ongoing wideband analysis of alternatives (AOA) before shifting to the topic of resiliency.

As it turns out, resiliency and mission assurance aren't new issues, which was well illustrated by this anecdote from Dr. Weeden, "*I was looking at some documents from the end of the Ford Administration, they were worried about threats to U.S. space systems from a growing adversary counter-space problem and the fact that their systems were not designed to be able to defend themselves or be survivable in the face of an attack.*"

That administration ended more than 40 years ago.

No Simple Solution

Although this is clearly an old challenge, there has yet to be a perfect solution implemented across the DoD — most likely because there is no one, simple solution.

As Mr. Loverro elaborated, "*You can't just build a bunch of satellites and say you're resilient. You can't just go ahead and put armor on your satellite and say you're resilient. You can't just go ahead and say just use commercial, or do responsive launch and say you're resilient." Instead, he challenged the military to, "...look at your mission, look at your architecture and the tools available and think about what makes it difficult – if not impossible – for someone to take that apart.*"

Ultimately, multiple panel participants agreed that it's going to be a combination of disparate solutions — a "***basket of solutions***" as Dr. Weeden referred to it — that can be combined to better protect military satellite infrastructures and architectures.

That "basket of solutions" was further defined by Mr. Loverro when he said, "*It's going to be a combination of proliferation, disaggregation, diversity, distribution, protection, proliferation and deception. Those factors can combine for any space capability that we know about to make them resilient, and – quite frankly – it doesn't cost a lot of money if you combine them correctly.*"

Although the panel all agreed that resiliency in satellite networks was of paramount importance for the DoD, they did disagree when it came to identifying exactly which threat was the largest one facing military satellites.

Two of the panelists were concerned about cyber attacks and cyber threats impacting military satellites. Mr. Loverro was more concerned about a somewhat less sophisticated, albeit equally effective, threat to satellites — jamming.

According to Mr. Loverro, "*Cyber attack against a variety of communications networks is a difficult challenge. But the far simpler thing that Russia can do. That North Korea can do. That Iran can do. That Botswana can do. That some guy in the middle of a field with a TV truck can do…is jamming. Jamming is very hard to protect against, unless you have the right equipment.*"

And that's an area where commercial satellite can help.

Getting Down to the Jam

When making the decision about which orbit to place their military satellites will take, the DoD selected GEO because fewer satellites could provide coverage for much of the Earth's surface. Fewer satellites meant less money. But, as Mr. Loverro noted, "*What is good for economics isn't good for the military.*"

Jamming a satellite's signal requires being within the satellite's beam — or coverage area. This is much easier with GEO satellites, because their coverage areas are so large. By launching military satellites into GEO, the coverage the military wanted came at a lower price tag, but with an increased risk of jamming. As Mr. Loverro explained, "*GEO was cheap to launch, but harder to defend.*"

However, there are commercial solutions that can help protect military communications from jamming.

Today's commercially-available HTS use steerable spot beams that provide incredible throughput, but cover smaller areas. Some of these satellites are currently operating in MEO orbits, meaning they combine high throughput with low latency, and are naturally more prolific and harder to jam. By embracing these commercial HTS and MEO satellite constellations, the military can essential get anti-jamming capabilities baked in.

Dr. Weedon (l) and Douglas Loverro (r) at Defense One.

"*…we recognize that the commercial industry is one of our biggest partners that we have not yet tapped to help us build this architecture and build this infrastructure.*" – ***Deanna Ryals*** of **Air Force Space Command** on the role of COMSATCOM in the military's satellite architecture.

Luckily, the door could be opening for an increased role for commercial partners in the military's space architecture – making these HTS and MEO constellations more readily available for military users. As part of the wideband satellite AoA, the DoD is exploring new ways to approach the construction of their satellite architecture, and is looking seriously at a more integrated network of commercial and military-owned satellites.

By building a combined architecture that embraces a combination of purpose-built, military-owned satellites and commercial capabilities, the military can better take advantage of the innovative new solutions that commercial providers are bringing to market. Based on statements from Mrs. Ryals, that could very well be in the cards:

"*There's a big push to expand and increase our partnerships for resiliency and national defense — to build capabilities together. I think that expands not just to allied partners, but also commercial partners. With the amount of commercial capability that's out there and available today, we have to find ways to change the way that we procure SATCOM capabilities. We have to look through the AoA and look at how we're approaching that balance of military vs commercial. But we recognize that the commercial industry is one of our biggest partners that we have not yet tapped to help us build this architecture and build this infrastructure.*"

By tapping this previously under-utilized resource, the military can better protect its satellite capabilities from jamming and ensure that the warfighter never has to go without essential services again.

This article is republished, courtesy of The Government Satellite Report (GSR) and Executive Editor Ryan Schradin*. He is a communications expert and journalist with more than a decade of experience and has edited and contributed to multiple, popular, online trade publications that are focused on government technology, satellite, unified communications and network infrastructure. His work includes editing and writing for the GovSat Report, The Modern Network, Public Sector View, and Cloud Sprawl.*

His work for the Government Satellite Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting written and podcast interviews. Ryan also contributes to the publication's industry events and conference coverage, providing in-depth reporting from leading satellite shows.

The Government Satellite Report is sponsored by…
SES Government Solutions
www.ses-gs.com

CYBERSECURITY WITHOUT LIMITS

The Cyphre Solution...

By Lance Smith, Chief Executive Officer, Cyphre (A RigNet Company)

As far as can be projected into the future, what is clear that this world will experience ever-increasing connectedness, — that means all are headed into a brave new world of unbounded attack surfaces.

Yes, along with boundless connectivity comes a stratospheric demand for data protection and the urgent need for more powerful cyber tools to maintain the peace. While there are great tools in today's security portfolios, they're inadequate to counter and survive the spectrum of breaches that await the unprepared... this means that attention must be paid to the source of such incursions and protect the data itself using state-of-the-art encryption technology.

Many satellite users have worked hard to weave cybersecurity into their fabric (for instance, NATO is spending more US$3.2 billion to boost the coalition's cybersecurity and satellite communications programs over three years), embracing best practices around encryption, subscriber management, access control, and overall system hardness. Still, there is more that can, and must, be done.

Cyphre, a RigNet company, exists to create a truly limitless data protection capability that scales to run across today's and tomorrow's networks and service clouds. Cyphre has helped the connected security space evolve from an age of bulky, hard-to-use products to tools that are inherent within the networks themselves.

Cyphre offers carrier grade, cloud-scale infrastructure that can be put into a service framework to transparently protect data in transit and at rest unequivocally. Cyphre works with a range of network service providers using all the standards in place today, keeping unbreachable data protection behind the scenes, transparent to the end user experience.

Halt Satellite Cyberdata Threats in Their Tracks

The "key" to unbreakable industrial grade encryption that can run inherently within the network models on a global basis is hardware-based cryptography.

AES-256 encryption — a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files in most current encryption algorithms, protocols and technologies — is solid for now (at least until quantum computing comes of age — that's another story).

However, software-based encryption does have vulnerabilities. Software encryption keys and certificates can become exposed to compromise. This is a fact of cybersecurity life — plaintext keys held resident in a server's main memory present a major exploitable opportunity for hackers.

As the network computing landscape has evolved, Cyphre has focused on protecting crypto material using an iron-clad model based on hardware underlying the service framework. Cyphre has developed a technology the firm calls **BlackTIE**® that assigns an individual, chip-resident encryption key to each file, rather than one key for many files.

This added layer of protection provides deeper and stronger data security that prevents secrets from being discoverable in any way. Because encryption keys are stored in a hardware layer, they are never exposed. Even if an attacker obtains root access into the server, the keys are both protected and unusable. Cyphre encryption renders any hijacked data useless.

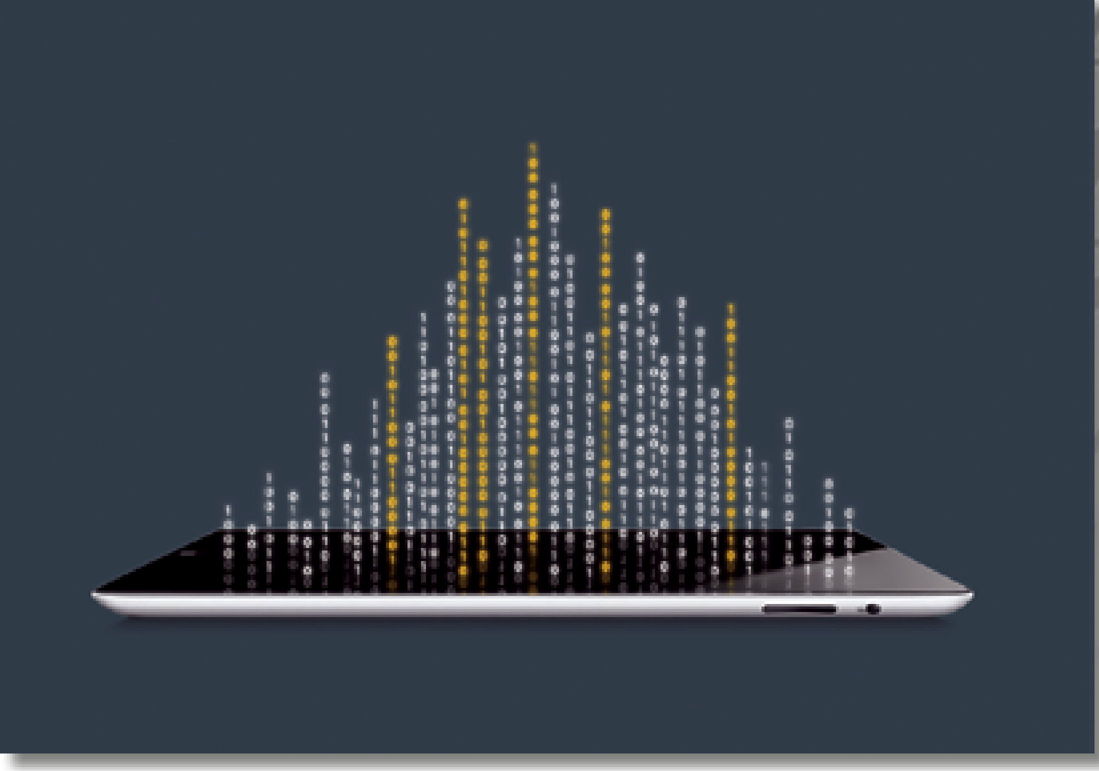
CyphreLock and CyphreLink

When cybersecurity knows no bounds it must protect data anytime, anywhere.

For data at rest, the **CyphreLock** network resident service couples standard AES-256 grade encryption with this unique one-key-per-file technology to create "blackened" keys that can only be produced by the hardware engine and brought back by the engine.

CyphreLock is built to carrier grade cloud scale; its encryption processing actually has no impact on network latency or performance. Data is protected in a unified fashion across cloud providers, with unique encryption keys that are never visible.

Enterprises can leverage the cloud storage service by routing data through CyphreLock to encrypt files at rest. Encryption services can also be provided on the customer's premises, if desired.



For data in transit, CyphreLink uses BlackTIE® technology to effectively bolster the strength of any TLS/SSL session. BlackTIE® assigns an individual, chip-resident encryption key to each file, rather than one key for many files. Data can securely transit any network, whether wireless, cellular, mobile, or satellite, without being vulnerable to man-in-the-middle attacks.

For companies that want to move some traffic into public network connections but want to make certain they can trust the connectivity, CyphreLink authenticates endpoint identities and connects data safely, with protection traveling with the file as it travels.

To protect network traffic, CyphreLink is deployed at network end points to create a completely encrypted tunnel from endpoint to endpoint that secures communications over the entire data path. CyphreLink's hardened security solution protects data, certificates, keys, and connections from eavesdropping, surveillance, overt and covert interception, and man-in-the-middle attacks. Connections for IoT data transmitted across networks is also immune to man-in-the-middle attacks.

Consider a maritime customer transmitting data ship-to-shore through VSAT equipment, where information is communicated via satellite to onshore teleports. Expensive and cumbersome protocols and dedicated links are required to provide an adequate level of security — and breaches can still occur through backdoor exploits and other attack vectors.

Placing CyphreLink onboard ships and at endpoints secures the data throughout the entire transmission, regardless of any vulnerabilities that may exist along the network path. Because Cyphre solutions run "over the top," data is secured all along its path.

Crucial "Human-Nature-Proof" Security

Cyphre's security solutions provide 360-degree data protection that is invisible to end users, highly scalable, device-resident, and cost-effective for medium and large scale environments.

Crucially, Cyphre's automatic protection of information requires no proactive action by the teams managing and moving the data. This establishes a "zero knowledge" stance for employees, eliminating them as a possible point of exposure.

Configuring, updating, patching, and upgrading systems and devices against breach vulnerabilities is a massive effort that is extremely prone to human error. Cyphre's encryption technology ensures that staff failures — essentially a certainty in an era of boundless connectivity — do not imperil information security.

Challenges

There are challenges — scaling encryption to meet the massive needs of the growing connected world means handling many more certificates and keys.

In the past, key management was typically a manual process. Happily, key orchestration has evolved greatly and is now highly automated, transforming a difficult function to one that is easy to perform.

Another issue is the fractured universe of encryption, especially in cloud computing. With many service providers available for storage, SaaS, and other functions, each with its own security features for its platform, Cyphre provides unified encryption models and management across cloud and enterprise platforms.

A future of boundless connectivity calls for cybersecurity without limits — and that requires a level of unbreachable encryption for data at rest and in motion that is only delivered by innovative hardware-based solutions such as Cyphre's BlackTIE® technology.

www.cyphre.com/

Lance Smith is a seasoned entrepreneur with 20 years of executive leadership experience at ACS/Xerox, Atos, cloud Infrastructure-as-a-Service company VAZATA, and forming businesses focused on the payment card industry and managed service solutions for the Global 1000.

As CEO of Cyphre, Smith has focused on building a strong culture that is centered on solving the toughest Internet safety challenges. He maintains active board memberships at several private companies, as well as serving as Board President for a non-profit board focused on STEM education.

Smith holds a Bachelor of Arts degree in Economics from Austin College and a Master in Public Administration degree from the University of North Texas.

"Very well done. Terrific evolution from the first MilSatCom USA in 2016."
MilSatCom USA Attendee, 2017

SMi
LINKING BUSINESS *with* INFORMATION

SMi Group presents its 3rd annual conference on...

MilSatCom USA

Identifying And Optimising Next-Generation SatCom Capabilities

27th - 28th
JUNE
2018

KEY BRIDGE MARRIOTT, ARLINGTON, VIRGINIA, USA

BENEFITS OF ATTENDING

- Hear about the implications of the **National Defence Authorization Act 2018** and the **Wideband AoA** and how these will impact on future MilSatCom and space systems moving forward
- Learn about the **MilSatCom programmes** from national allies and how international collaboration can benefit future strategies
- Join the discussion on key topics of resilient **MilSatCom architectures** and the military utilisation of **ComSatCom** systems
- With the era of **mega-constellations in LEO** fast approaching, debate how best government and industry can utilise these capabilities to meet operational requirements

2018 USA SPEAKERS INCLUDE:

Senior Leadership, Office of the Chief Information Officer, G6, **U.S. Army**

Brigadier General Tim Lawson, DCG-O (Deputy Commanding General for Operations), **U.S. Army SMDC/ASTRAT**

Brigadier General Mark Baird, Director of Space Programmes, **U.S. Air Force**

Robert Tarleton, Director, Military Satellite Communications Directorate, **U.S. Air Force**

Dr Brian Teeple, DoD CIO C4, **U.S. Department of Defense**

Colonel Charles Daly, Director of J63, **U.S. Special Operations Command**

Captain Mike Thrall, Chief, Plans and Programs Division, Cyberspace Operations, **NORAD and U.S. Northern Command**

Colonel Hugh McCauley, CCJ6 Operations Division Chief, **U.S. CENTCOM**

Norman R Yarbrough, Operations Research Analyst, U.S. Department of Defence, **Office of Secretary of Defense Acquisition and Sustainment**

Dr Lawrence "Robbie" Robertson Mission Lead, Satellite Communications, Space Vehicles Directorate, **U.S. Air Force Research Laboratory**

Jessie L. Showers, Jr., Infrastructure Directorate Executive, Infrastructure Directorate (IE), **Defense Information Systems Agency (DISA)**

2018 INTERNATIONAL SPEAKERS INCLUDE:

Colonel Stig Nilsson, Head of Space Programmes, **Norwegian MoD**

Commander Marcio Costa, Chief of the Space Systems Coordination and Implementation Commission (CCISE), Department of Air & Space Technology - DCTA, **Brazilian Air Force**

Major Geoffroy Beaudot, SatCom and CIS Programme Manager, **Luxembourg Directorate of Defence**

Giovanni Durando, SATCOM Service Area Owner, **NATO Communications and Information Agency (NCIA)**

GOLD SPONSORS:

AIRBUS
HUGHES An EchoStar Company
LOCKHEED MARTIN

SPONSORS AND EXHIBITORS:

inmarsat The mobile satellite company
SES GOVERNMENT SOLUTIONS
SKY Perfect JSAT Corporation
smiths interconnect bringing technology to life
XTAR Satellite Communications

www.milsatcom-usa.com/MilSatMag

Register online or fax your registration to +44 (0) 870 9090 712 or call +44 (0) 870 9090 711

SPECIAL RATES AVAILABLE FOR MILITARY AND GOVERNMENT REPRESENTATIVES

CPD CERTIFIED The CPD Certification Service

@SMiGroupDefence
#MilSatComUSA

INFORMATION ASSURANCE: THE U.S. MILITARY'S NEED FOR WHAT COMMERCIAL SATCOM PROVIDERS OFFER

A SatCom Frontier Perspective

When the U.S. military began using satellite communications many decades ago, space was a sanctuary.

That's no longer the case today. New potential adversaries and a proliferation of non-kinetic techniques have increased the risks to satellite communications even as the military's reliance on this technology grows.

Meanwhile, the commercial industry's efforts to improve SATCOM resiliency illustrates the discrepancy between military and commercial satellites.

Todd Harrison, Director of the aerospace security project and defense budget analysis at the Center for Strategic and International Studies, noted in a recent interview that the United States military is operating outdated satellites that are mostly undefended and unprotected, originally built with the mindset that space was a sanctuary.

"That's not true anymore," Harrison said in the article. Such a situation leaves the U.S. military vulnerable at a time when it relies heavily upon satellites for everything from basic communications to GPS to precision-guided weapons.

Non-kinetic weapons, such as jammers, are inexpensive and easy to use, making them widely accessible. There have even been cited examples of insurgents using jammers to interfere with U.S. satellite communications in Iraq and Syria.

"This is coming from a ragtag group of insurgents that aren't technologically sophisticated, don't have deep pockets, and don't have training or technical expertise," Harrison said.

Meanwhile, the integration of terrestrial and satellite networks "...is massively increasing the security landscape," *Vinit Duggal*, Intelsat Director and Chief Information Security Officer, told SpaceNews.com. "It's not so much the threat actors that have changed, but (that) they are getting a larger playground to play in."

Artistic rendition of the Intelsat-33e satellite.

Intelsat's Tysons Corner, Virginia, satellite operations center.
Photo is courtesy of Intelsat.

The most effective and cost efficient way for the U.S. government to mitigate threats like these is to address security early on in the engineering cycle — or to turn to a commercial SATCOM provider like **Intelsat General**.

According to *Duggal*, Intelsat spends about five percent of its technology budget on information security. "*If you address security upfront and make it part of your engineering cycle, it reduces the cost dramatically*," he told Space News during a recent trade show.

For example, **Intelsat Epic^{NG}** is engineered to allow for a more protected level of commercial SATCOM. Low-probability of intercept (LPI) and jamming-resilience greatly enhance anti-jamming capabilities on Epic^{NG} satellites, even to non-hopping modems. They are also engineered to allow customers to change power levels, and Intelsat is looking at the possibility of adding beam shaping to future satellites.

"*(With beam shaping), you can change the shape of the beam whenever you want to from the ground*," ***Mark Daniels***, Intelsat General Corp.'s Vice President for new technologies and services, recently said, "*You would be able to start with a beam shaped for a particular region but if demand changes or there are problems with jamming, you can reconfigure the beam to increase the coverage area or notch out an area to avoid jamming.*"

Intelsat Epic^{NG} also features interference-mitigation capabilities like on-board power monitoring and notch filtering of interferers/unauthorized users as well as monitoring, re-routing, geo-location, and identification of interferers.

A defense-in-depth approach to security ensures that Intelsat General's customers receive the highest quality-of-service. The company meets DoD-mandated security requirements for information assurance by assessing its own infrastructure and third-party networks against the most stringent DoD Instruction 8500.01 and NIST Risk Management Framework (RMF) cyber security recommendations and controls.

A comprehensive Information Assurance assessment and remediation program includes annual penetration assessments, organization-wide control assessments, and third-party SOC3 audits of both satellite and terrestrial environments. Intelsat even pays to have its customers' VSAT equipment assessed by third-party security firms. "We pay for that ourselves," Duggal told Space News. "There is an automatic, default expectati0n that security is built into VSAT platforms. It's not. When we go to market as an industry there are a lot of moving parts."

By retaining complete control of both the space and terrestrial components of the global Intelsat network, IGC can better detect, prevent, and mitigate cyber threats.

Space is no longer the sanctuary it once was, and the U.S. military cannot afford to take a reactive approach to information security—nor does it have to. The commercial satellite industry offers the protected SATCOM that the military needs today.

www.intelsatgeneral.com/

The preceding article is courtesy of Intelsat General's SatCom Frontier infosite and editorial team.