SATCOM for Net-Centric Warfare

MilsatMagazine

April 2020 issue

Artistic rendition of the Lockheed Martin-built AEHF-6 satellite launch. The photo is courtesy of United Launch Alliance.

PUBLISHING OPERATIONS

Silvano Payne, Publisher + Executive Writer
Simon Payne, Chief Technical Officer
Hartley G. Lesser, Editorial Director
Pattie Lesser, Executive Editor
Donald McGee, Production Manager
Andy Bernard, Sales Director
Teresa Sanderson, Operations Director
Sean Payne, Business Development Director
Dan Makinster, Technical Advisor

SENIOR COLUMNISTS

Chris Forrester, Broadgate Publications
Karl Fuchs, iDirect Government Services
Bob Gough, Goonhilly Earth Station
Rebecca M. Cowen-Hirsch, Inmarsat
Ken Peterman, Viasat
Giles Peeters, Track24 Defence
Koen Willems, Newtec

THIS ISSUE'S AUTHORS

John Beckner
Tony Frazier
Brad Grady
Catherine Melquist
Major William Russell
Ryan Schradin

TABLE OF CONTENTS

INDEX OF ADVERTISERS

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 © 2020 Satnews Publishers

SPACEBRIDGE

BRINGING SATCOM TO THE CLOUD

ZERO OVERHEAD, FULLY MANAGED CLOUD-BASED SATCOM SERVICE

SpaceBridge delivers high quality dynamic SCPC BoD (Bandwidth on Demand) satellite connectivity as a fully managed cloud-based service - no hub or even teleport required!

Simply partner up with **SpaceBridge**, sign up for the period of time and amount of bandwidth desired, and you're all set. We'll provision your very own slice of our satellite infrastructure -equipment and optional bandwidth -CAPEX-free, with 24/7 management and technical support, maintenance; full visibility and control included.

Best of all, **SpaceBridge**'s pay-as-you-grow scalability will allow you to cost-effectively expand your satellite communication assets as you go.

Sign up today, and enjoy SpaceBridge's cost-effective, efficient and scalable satellite connectivity-as-a-service!

- **High quality dynamic SCPC BoD satellite connectivity**
- **A fully managed, 24/7 cloud-based service**
- **OPEX only subscription engagement basis**
- **Optional teleport services**

SPACEBRIDGE
ALL THINGS CONNECTED

www.spacebridge.com

ULA'S AEHF-6 LAUNCH SUCCESS FOR USSF

The United Launch Alliance Atlas V 551 rocket lifted off at 4:18 p.m. EDT (2018 UTC) carrying the sixth Advanced Extremely High Frequency (AEHF-6) communications satellite for the U.S. Space Force's Space and Missile Systems Center from Cape Canaveral Air Force Station, Florida.

Following the first stage of flight, the Centaur upper stage performed an initial burn that achieved a parking orbit. A second burn then injected the rocket and payload into a standard GEO orbit. The cubesat rideshare payload was then deployed.

Five-hours later, the Atlas rocket coasted away from Earth to reach apogee, or the high point, of the orbit and Centaur performed a third and final burn and raised perigee, or the low point, of the orbit and reduced inclination, relative to the equator.

The seven hour countdown started at 8:07 a.m. EDT under the guidance of ULA Launch Conductor ***Scott Barney***. The rocket was powered up and underwent standard day-of-launch testing while crews finished configuring the launch pad. The "go" for fueling was given by ULA Launch Director ***Tom Heter*** III at 12:39 p.m. Tanking operations were successfully performed as 66,000 gallons of liquid oxygen and liquid hydrogen were placed into the rocket's tanks. The clear to launch was given at 4:12 p.m. EDT by Space Force Mission Director Col. ***Robert Bongiovi***.

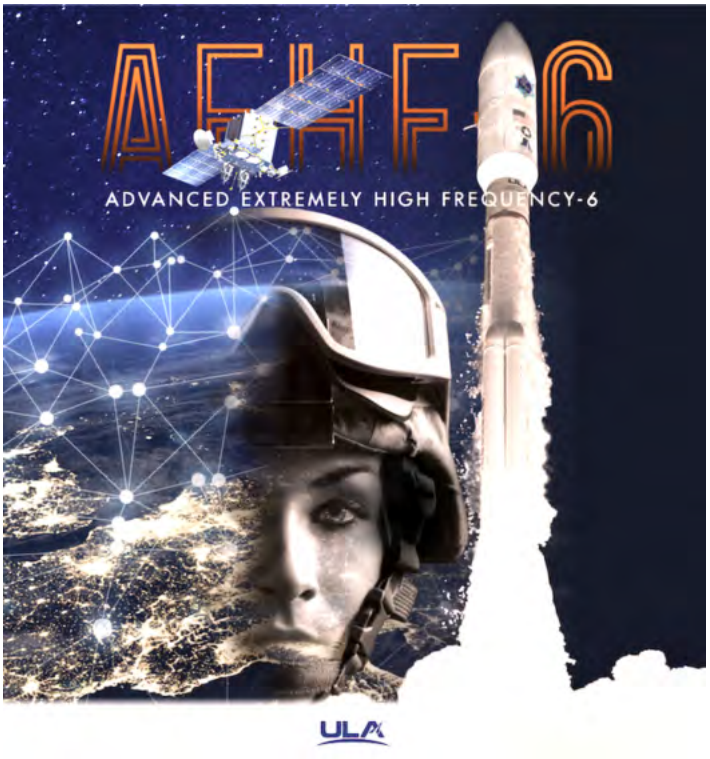
The AEHF system, developed by Lockheed Martin, provides vastly improved global, survivable, protected communications capabilities for strategic command and tactical warfighters. This jam-resistant system also serves international partners including Canada, the Netherlands, the United Kingdom and Australia. AEHF-6 will be a protected communications relay to provide the highest levels of information protection to the nation's most critical users.

The Lockheed Martin A2100 satellite gives senior leadership a survivable line of communications to military forces in all levels of conflict, including nuclear war. The system features encryption, low probability of intercept and detection, jammer resistance and the ability to penetrate the electro-magnetic interference caused by nuclear weapons to route communications to users on land, at sea or in the air.

The Atlas V 551 rocket will deliver AEHF-6 into an optimized, high-energy geosynchronous transfer orbit. ULA and the AEHF program produced this ascent profile to maximize mission flexibility over the satellite's lifetime.

Atlas V rockets successfully launched the first five AEHF satellites in 2010, 2012, 2013, 2018 and 2019. These satellites were placed in geosynchronous orbit 35,888 km (22,300 miles) above Earth to augment and eventually replace the legacy MILSTAR communications satellite fleet. One AEHF satellite has greater capacity than the entire five-satellite MILSTAR constellation.

ulalaunch.com



WALTON DE-ICE

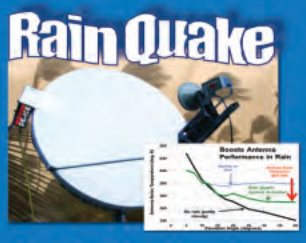
New LEO / MEO Design

The **Portable Radome** makes satellite networks more survivable and deployable into extreme and harsh environments. Protect transportable antennas and equipment from, snow, ice, burning sun, sandstorms, torrential rains, up to 85 mile-per-hour winds, and more.

- Single-person setup in less than an hour — conventional radomes can take days.
- New LEO/MEO design for full-arc / elevation angle performance. L, C, Ku, X, & Ka Bands.

The industy's most powerful, cost-effective De-Icing. For antennas from 3.7 to 32 meters.

Sheds off snow before ice forms. Huge — up to 100 X — energy savings compared to conventional systems. 0.6 to 6.3 meters.



Minimize Signal Loss due to Rain Fade. Reduce data loss — by 20X or more.

+1 (951) 683-0930 | sales@de-ice.com | www.De-Ice.com
WB Walton Enterprises, Inc. P.O. Box 9010 San Bernardino, CA 92427, USA

VIASAT WORKING TO TOP THEIR RECORD BREAKING 2019 PERFORMANCE

In the defense sector, Viasat aims to top a record-breaking 2019 by improving their Defense and Government Communications technology for warfighters, all of which will drive the company's efforts in 2020 to improve crucial communications for warfighters.

Having achieved a series of key milestones over the course of the last year, 2020 may prove to be another record-breaking period for Viasat as the company continues to enhance its market-leading technology and thoughtful leadership throughout the defense sector.

Highlights in 2019 saw Viasat's Government Systems business exceeding $1 billion in annual revenue for the first time in the company's history.

Viasat was also prominently featured across a series of industry-leading government rankings. These saw the company climbing from 82nd to 46th in the "2019 Washington Technology Top 100" as well as jumping 90 spots in the "Bloomberg Government (BGOV) 2019 Federal Industry Leaders List". Viasat also demonstrated differentiated progress in the 2019 "Defense News Top 100".

According to Viasat's President for Government Systems, ***Ken Peterman***, this ongoing success presents an exciting future for the company as it continues to support warfighters and military forces operating around the world.

Ken Peterman

He said that Viasat is one of the fastest movers in terms of growth trajectory in the defense market today. The company's unique culture of innovation, technology leadership, agile development processes and flexible business models are seeing enormous demand from warfighters and the firm's military customers.

Peterman highlighted the company's mix of veterans, engineers and technologists as key to the company's ability to maneuver in a more entrepreneurial fashion throughout the defense market. He noted that this agility enables Viasat to accelerate the delivery of cutting-edge mobile networking, cybersecurity, information assurance, satellite communications and cloud-enabled capabilities to support today's warfighter.

Peterman continued by stating that most of these technologies were invented by the defense community, but over the past 15 years, leadership has firmly transitioned into commercial hands. That enables companies such as Viasat to continue to accelerate the delivery of turnkey capabilities at unprecedented levels.

Today's private sector technology is moving faster than the current acquisition systems and processes can move. Viasat, in large part, is moving beyond traditional acquisition process and policies to get much needed technology to the warfighter, faster and more effectively than ever before. A close understanding of the customer by Viasat's team is instrumental to this success.

A specific technology area of interest completed by Viasat in 2019 included ongoing development and growth of the company's next generation tactical data link (NGTDL) business

Key NGTDL milestones achieved throughout the year included the delivery of the 1,500th KOR-24A Small Tactical Terminal (STT)

Delivery of almost the 2,500th AN/PRC-161 Battlefield Awareness and Targeting System-Dismounted (BATS-D) handheld Link 16 radio

Successful integration of Advanced Concurrent Multiple Reception (CMR) technology capabilities across Viasat's extensive line of next generation link 16 products

New advancements for the company's Move out / Jump off (MOJO) expeditionary tactical gateway system, which is designed to blend air and ground situation awareness pictures.

In 2019, Viasat also won a development contract to design the first Link 16 satellite that will be launched into LEO. This enables the future possibility of the company extending Link 16 capabilities to Beyond Line of Sight (BLOS) operations as well as networking the LEO satellite to the ViaSat-3 geostationary (GEO) constellation for a truly global solution.

A clearer battlefield picture in the fog of war with Link 16. Image is courtesy of Viasat.

Viasat also continued to further develop its Hybrid Adaptive Network (HAN) concept, which will be designed to maximize warfighter connectivity, security and resilience by providing simultaneous access to multiple commercial and military networks. With more than 100 HAN demonstrations completed over just the last 120 days of 2019, Viasat successfully proved its ability to assure resilience, advance security and deliver significantly improved levels of connectivity at the tactical edge, Peterman confirmed.

Work included a demonstration to the U.S. Air Force's AFWERX program as part of the Multi-Domain Operations Challenge in July, which saw Viasat supporting connectivity in integrated operations in the air, space, land, sea, cyber and across the electromagnetic spectrum.

Expected to be capable of meshing together LEO, MEO and GEO satellites offering Ku-, Ka- and Mil-Ka frequency bands; multiple ground infrastructure support systems; and multiple, external networks, the HAN is expected to support Line of Sight and BLOS communications as well as real-time network management; visualization and control; real-time active cyber security; cloud-enabled technologies; and real-time situational awareness across multiple end user devices.

The HAN's end-to-end communications network will be designed to provide government customers with more rapid sensor-to-shooter targeting cycles; reductions in cognitive burdens; as well as predictive analytics to support intelligence, surveillance, target acquisition and reconnaissance (ISTAR) missions, force protection; and battlefield medicine.

Peterman added that the HAN will also be supported by the ViaSat-3 constellation. He then said that, ultimately, this all comes down to the warfighter. When the nation's young men and women put on a uniform and go into the service, the company has an obligation to give them the same kind of technological capabilities that they have grown up dependingd upon — Viasat's employees are committed to working toward finding a better way for the men and women in uniform everyday — and we don't plan to slow down anytime soon.

www.viasat.com

GOOD NEWS FOR MILITARY SATELLITE & SPACE SECTORS

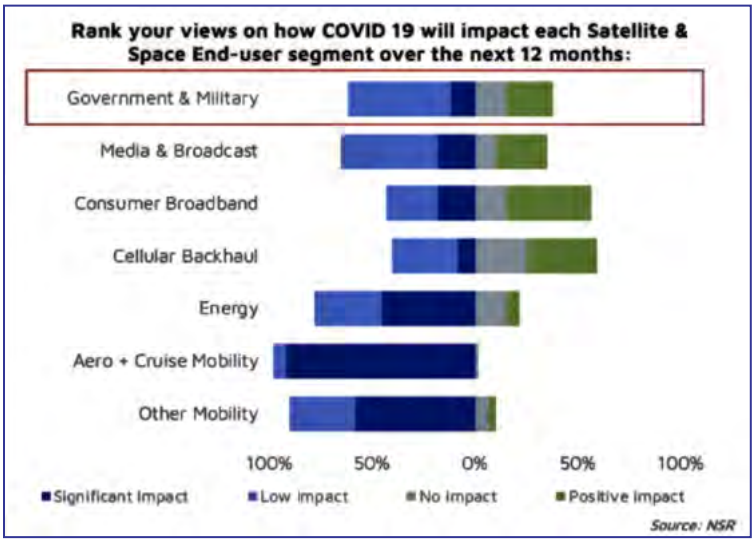
As the Satellite & Space sectors face the same challenges as the rest of the economy, one market seems particularly robust in the face of COVID-19 – Government & Military Satellite Communications services.

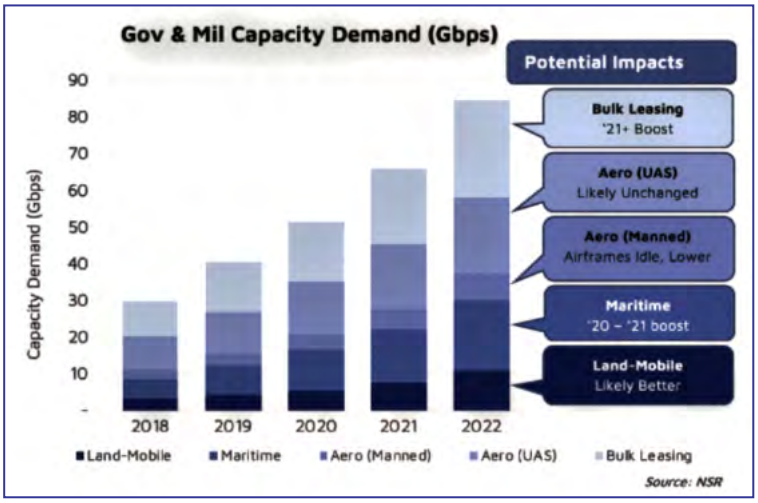
With ongoing procurement for next-gen MILSATCOM technologies from U.S. Space Force, the commercial opportunities continue. While the future remains uncertain, compared to other mobility-centric satellite end-user markets, Gov & Mil appears to remain insulated from larger world events.

According to a recent survey conducted by NSR across a wide variety of the Satellite & Space sector value-chain, Gov & Mil markets was identified as one end-user vertical that is expected to see some of the lowest levels of significant impact, and some of the few markets with an expected positive impact from COVID-19 to the Satellite & Space value-chain.

Just as armed conflicts generally boost consumption of satellite services by Gov & Mil end-users (think the 2008 troop surge for Global War on Terror), this different fight appears no different. Facing a multi-faceted challenge of the immediate requirements for connectivity to enable telemedicine and response coordination, continuing procurement activities appear to be a key pillar of the economic response for governments around the world.

Moreover, as NSR continues to evaluate how rapidly changing world events are impacting markets today, and long-term ramifications – NSR's Government & Military Satellite Communications, 16th Edition report appears to remain largely unimpacted right now. There are segments of the market that are naturally feeling pressures – world leaders are not traveling as much and thus their fleet of highly connected vehicles are idle now – yet, that capacity is quickly getting reallocated towards other missions or applications.





As we have seen with the reallocation of capacity for the USNS Mercy and, more recently, USNS Comfort, quickly reallocating capacity can occur, yet at the expense of the current users of MILSATCOM capacity from systems such as WGS.

If there are any long-term trends to emerge from the COVID-19 response so far, robust communication networks are a must-have. More than ability to deploy engineers onsite and quickly reallocate resources from one platform to another – multi-band and multi-network ground infrastructure will become a key enabling technology to meet the multi-domain requirements of Gov & Military operations.

What is unclear is the balance between Gov-owned and Gov-Leased capacity.

With the Space Development Agency moving forward with Industry Days for their proliferated LEO "Transport Layer" and an RFP release slated for May 1st, the market is waiting to see if the U.S. DoD can provide another lifeline to the LEO Space Market. As with early-days of Iridium, can SDA's Transport Layer provide the much-needed 'steady consumer' on either the spacecraft hardware or connectivity business models required to bring these dreams to reality? Bottom Line

In these uncertain times, Governments are taking significant economic action to boost domestic industries – from increased or ongoing procurement to direct stimulus. With all that was happening in the Satellite & Space sector before COVID-19, the near-term outlook for this market continues to be one of the few positive spots across the value-chain. From potential spacecraft sales in the post-OneWeb world to spending on enhanced ground infrastructure to more bandwidth demand – there remain reasons to be optimistic on the growth opportunity for Government and Military players.

www.nsr.com

Article author: Brad Grady, NSR Analyst

AN ENHANCED HORNET SATCOM TERMINAL DEBUTS FROM PARADIGM

Paradigm has released an enhanced version of the firm's field-proven, HORNET SATCOM terminal.

The HORNET is a modular solution, allowing the user to interchange between different sized antennas, RF head and modem modules. This provides a single SATCOM solution for many different operational requirements. The terminal is environmentally rugged yet still lightweight and crucially can now be packed into an airline-friendly case.

The HORNET integrates the easy-to-use and field-proven PIM (Paradigm Interface Module) which allows any non-skilled user to point the antenna in just a few minutes.

Available modules for the HORNET currently include a choice of 60, 80 and 100 cm. antennas with RF modules between 5 and 80W; frequency bands cover Ka-, Ku- and X-band over both extended commercial and military ranges. The terminal is also modem agnostic, supporting all the main high performance modems.

The PIM is a rugged, field-proven, terminal controller operating in many different market sectors across 5 continents. It provides the 'brains' of a SATCOM solution and can work with any air interface to provide a common pointing experience across a whole range of manufacturers' terminals. Operators simply point the terminal using easy to follow onboard audio and visual cues.

The PIM integrates into all the major satellite networks as well as a wide range of modems, supporting the major types including iDirect, Newtec, UHP, Comtech and Teledyne Paradise among others.

Ulf Sandberg, Managing Director of Paradigm, added that by developing the firm's HORNET terminal into this incredibly versatile solution, customers can now purchase one system that will meet just about every SATCOM requirement. In the Paradigm demos, everyone has been extremely impressed with its simplicity, its ruggedness and its single-case portability.

paracomm.co.uk

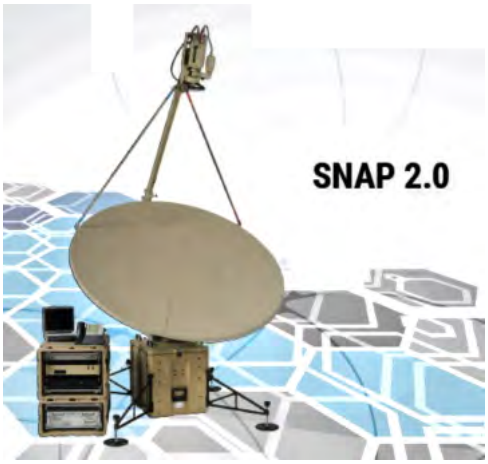
MILITARY AND GROUND STATION TERMINAL CONTRACTS RECEIVED BY COMETECH EF DATA

Comtech Telecommunications Corp. (NASDAQ: CMTL) announced today that their Mission-Critical Technologies group, which is part of Comtech's Government Solutions segment, received an order consisting of additional funding of $9.1 million (of which $7.7 million was in the third quarter), on the previously announced three-year $124.2 million contract to provide ongoing sustainment services for the AN/TSC-198A SNAP (Secret Internet Protocol Router ("SIPR") and Non-classified Internet Protocol Router ("NIPR") Access Point), and baseband equipment.

SNAP terminals provide quick and mobile satellite communications capabilities to personnel in the field. The contract has been funded $87.0 million to date.The Mission-Critical Technologies group is focused on ensuring its customers are able to successfully carry out their mission, whether that be communicating in an austere environment on land or at sea, launching or tracking a satellite, or protecting the cyber security posture of their network.

Regarding this contract, Mr. Kornberg said that, more than ever, it is important that the company's U.S. Army customer has access to reliable advanced communications equipment and the firm looks forward to providing additional essential equipment and services under this contract in future periods.

Additionally, Comtech Telecommunications Corp. (NASDAQ: CMTL) announced that, during the company's third quarter of fiscal 2020, their Tempe, Arizona-based subsidiary, Comtech EF Data Corp., which is part of Comtech's Commercial Solutions segment, received $1.6 million in orders for satellite ground station equipment from the world's largest Mobile Network Operator ("MNO") based in China — this equipment will be used to support the upgrade of its existing mobile backhaul and teleport technologies.



After a competitive Request for Information ("RFI") process was completed by the MNO, it selected Comtech EF Data's Heights™ Networking Platform as the premier solution, which can support its current 2G and planned 4G mobile backhaul services, while also being 5G ready for the future. In addition, the MNO selected a range of Comtech EF Data's RF Products and RAN/WAN Optimization solutions to complement the Heights™ Networking Platform.

The Heights™ Networking Platform features high efficiency DVB-S2X shared outbound which, when coupled with the evolutionary Heights™ Dynamic Network Access ("HDNA") technology and built in LTE optimization, provides the highest performance solution capable, while offering the best Total Cost of Ownership ("TCO").

Additionally, the solution delivers the highest Quality of Experience ("QoE") by minimizing jitter and latency, making it ideal for full 2G/3G and 4G LTE service delivery.

Fred Kornberg, Chairman of the Board and CEO of Comtech Telecommunications Corp., stated he was pleased that Comtech was selected to provide the Heights mobile backhaul solution for mobile end-customers based in China. He believes this order is evidence that Comtech's advanced satellite ground station technologies are essential, especially during a time of difficult conditions caused by the coronavirus. Kornberg is cautiously optimistic, that as normal conditions eventually return, additional orders from new customers will be received in the future.

Richard Swardh, Senior Vice President, MNO of Comtech EF Data commented that the company is excited that this MNO selected the Heights™ solution to support its mobile services over satellite today and to prepare for the future roll out of 5G services. The company has, yet again, proven to have the highest QoE across all generations of mobile technology. The firm's industry-leading jitter and latency performance make it easy and convenient for MNOs to deploy satellite backhaul with the highest Key Performance Indicators ("KPIs").

www.comtechefdata.com

Advantech Wireless Technologies

Military & Government Solutions

X-Band SSPAs/BUcs
GaN & GaAs configurations

Engage Class Integrated
SATCOM Terminals

X-Band / Ka-Band
Frequency Converters

Troposcatter Products

LNAs / LNBs

Solid State
Pulsed Amplifiers

Faster & More Secure Communications for Military and Government Agencies

At Advantech Wireless Technologies, we have over 25 years of experience delivering cutting-edge innovations in communications that solve mission critical communications challenges.
We understand the challenges that government & military leaders face and our technologies empower them with the freedom to communicate quickly, reliably and securely.

ADVANTECH
Wireless Technologies

advantechwireless.com

DEEP SPACE SURVEILLANCE SYSTEM CONTRACT FROM USAF TO SERCO

Serco Inc. has been awarded a new contract from the U.S. Space Force (USSF) to manage, operate and maintain the Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) system — the contract has an eight-month base period and six one-year option years, with a total value of $57 million.

The GEODDS system supports the U.S. Strategic Command and theater war fighters' requirements through the detection and surveillance of deep space satellites using one-meter telescopes that are equipped with highly sensitive digital camera technology.

The GEODSS system detects, tracks, identifies and reports on all deep-space man-made objects in the Earth's orbit. Both new objects that are discovered and objects already in the catalogue require regular observations in order to keep the orbit information accurate.

Under this new contract, Serco's operators will be performing space observation, including operating the telescopes, maintaining and supporting the systems, and logging and reporting the findings in support of the Combined Space Operations Center (CSpOC), the National Space Defense Center (NSDC) and the 18th Space Control Squadron (SPCS); Serco operators will also be undertaking Space Object Identification tasks in support of the National Air and Space Intelligence Center (NASIC).

Serco has extensive past performance experience supporting the Air Force Space Command (AFSPC) under the AFSPC C4ISR and C4I2TSR contracts. Serco Group has supported space projects for more than 50 years.

Today, the company has highly skilled scientific, technical and engineering teams supporting military and civilian space programs in Europe, the UK, Australia and now in the United States.

Serco will provide operation and maintenance (O&M), along with exercise and testing, and mission systems maintenance including repairs, logistics management, civil engineering, and support depot modifications. Work will be performed at all three geographically-separated GEODSS locations in Socorro, New Mexico; Diego Garcia, British Indian Ocean Territory (BIOT); and Maui, Hawaii.

Dave Dacquino, Serco's Chairman and CEO, said this is an exciting new win for Serco in supporting the U.S. Space Force and their GEODSS systems as it goes through upgrades and expansions. This win builds on Serco's presence in the space domain, in particular the company's UK and Europe division, with its contracts in Earth Observation (EO) support services and spacecraft and satellite management.

www.serco.com

www.spaceforce.mil

Ground-Based Electro-Optical Deep Space Surveillance sites, such as Detachment 2, Diego Garcia, British Indian OceanTerritory shown in this photo, play a vital role in tracking deep space objects. Photo is courtesy of U.S. Air Force Space Command.

U.S. SPACE FORCE ID'S USAF MISSIONS TO TRANSFER TO THIS NEWEST SERVICE

In a significant step that enhances the U.S. Space Force's capabilities and development, the Department of the Air Force has identified 23 U.S. Air Force organizations whose space-related missions will soon transfer to the Space Force.

Secretary of the Air Force ***Barbara Barrett***, in conjunction with Chief of Space Operations, Gen. ***John "Jay" Raymond*** and Chief of Staff of the Air Force Gen. ***David Goldfein***, directed the transfer which entails shifting space missions from U.S. Air Force organizations into the newest military branch.

Currently, Space Force is comprised primarily of units which previously fell under the former Air Force Space Command prior to the service's establishment on December 20, 2019.

According to Space Force officials, the goal is to have each of the 23 space missions formally transferred from the Air Force into the Space Force within the next three to six months based on timing and conditions specific to each organization and mission.

The CSAF and CSO have been delegated the authority to actually execute the transfer when they jointly agree the necessary conditions have been met to affect a smooth transfer.

This transfer plan does not include the physical movement of units or billets to a different geographic location, nor does it include moving any of the people assigned to units.

The missions and billets will simply be transferred to the Space Force and remain in place to leverage the talent, infrastructure, and key capabilities at their current location.

The mission transfers are aligned with the White House's Space Policy Directive-4 vision, which calls for the Space Force to "consolidate existing space forces and authorities for military space activities."

Barret said that building the U.S. Space Force represents a top priority for the Department of the Air Force. These mission transfers incorporate existing forces into the agile Space Force, which stands ready to defend American and allied interests.

The list of affected units emerged from analysis and planning by Department of the Air Force planners who determined that transferring these missions would play a critical role in directly supporting space missions and related operational capabilities.

Approximately 1,840 Air Force billets will be transferred into the Space Force from across the 23 units.

Importantly, while the mission transfers will change the alignment of units themselves from the Air Force to the Space Force, these actions will not constitute a change in service for the people assigned. In the near term, military personnel will remain

in the Air Force, although assigned to a unit in the Space Force.

During the coming months, and when appropriate provisions are in place as part of a separate process, military members who meet applicable criteria will be given the opportunity to volunteer to transfer to the Space Force. If they choose not to transfer, they will remain in the Air Force and assigned to the Space Force unit until their normal assignment rotation is complete, at which time they will be moved to an assignment within the Air Force.

The status of civilians, as Department of the Air Force employees, is unchanged. Whether serving in Air Force or Space Force billets, civilians will remain DAF employees and have the ability to remain in their current positions, or apply for other positions across the department. As the stand-up of the Space Force continues, additional space missions may be identified for transfer, which will be coordinated and approved by separate action.

The following locations have been identified for a transfer action:

> 17th Test Squadron, Peterson Air Force Base, Colorado
> 18th Intel Squadron, Wright-Patterson AFB, Ohio
> 25th Space Range Squadron, Schriever AFB, Colorado
> 328th Weapons Squadron, Nellis AFB, Nevada
> 527th Space Aggressor Squadron, Schriever AFB, Colorado
> 705th Combat Training Squadron OL-A, Schriever AFB, Colorado
*> 7th Intel Squadron, Ft. Meade, Maryland**
> 16th AF/Advanced Programs, Schriever AFB, Colorado*
*> 32nd Intel Squadron, Ft. Meade, Maryland**
*> 566th Intel Squadron, Buckley AFB, Colorado**
> 544th ISR Group Staff & Detachment 5, Peterson AFB, Colorado
> Detachment 1, USAF Warfare Center, Schriever AFB, Colorado
> 533rd Training Squadron, Vandenberg AFB, California
> National Security Space Institute, Peterson AFB, Colorado
*> AFRL Research Lab Mission Execution, Wright-Patterson AFB, Ohio**
*> AFRL Space Vehicles Directorate, Kirtland AFB, New Mexico**
*> AFRL Rocket Propulsion Division, Edwards AFB, California**
*> AFRL Electro-Optical Division, Maui, Hawaii & Kirtland AFB, New Mexico**
*> AFRL Sensors Directorate, Wright-Patterson AFB, Ohio**
> Counter-Space Analysis Squadron, Wright-Patterson AFB
> Ohio Space Analysis Squadron, Wright-Patterson AFB
> Ohio Air Force Operational Test and Evaluation Center Detachment 4, Peterson AFB
*> Colorado Air Force Safety Center - Space Safety Division, Kirtland AFB, New Mexico**

** Partial mission transfer (i.e., size of a flight, branch or division or above)*

Article authored by Maj. William Russell , U.S. Space Force Public Affairs

SPACE MICRO'S LASER COMMS TERMINALS CONTRACT WIN FROM USAF

Space Micro has received a $3 million award by the USAF Space and Missile Center (SMC) for the development of modified laser secure communications terminals to be used for upcoming Air Force missions.

The U.S. Space and Missile Systems Center (SMC) conducted their Pitch Day to enable the quick acquisition of technologies for *military use. Dr.* Will Roper, assistant secretary of the Air Force for acquisition, technology and logistics, has championed these rapid acquisition events.

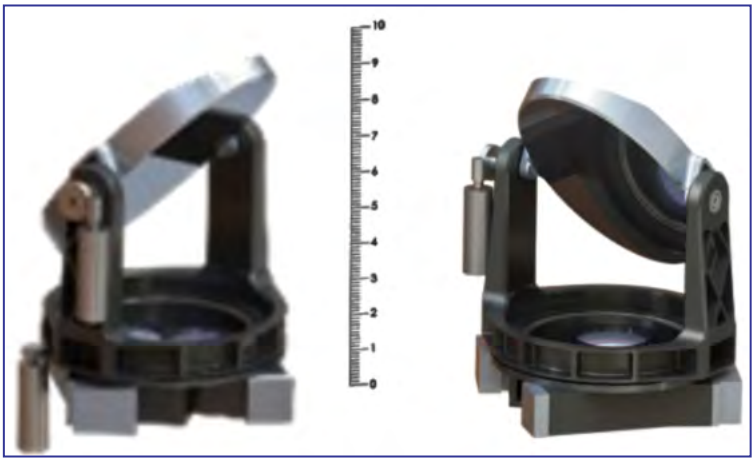
Space Micro's µLCT™ 100 Laser Communication Terminal operates at a data rate of 100 Gbps and is based on space-qualified, Telcordia-grade 1550 nm telecom components and boasts a SEL threshold of > 60 MeV-cm2/mg, SEFI immunity, and 30 krads(Si) total ionizing dose tolerance, with the option of reaching up to 100 krads(Si).

Space Micro's µLCT 100 comprises an optical modem, optical power amplifiers, pointing, acquisition and tracking (PAT) electronics and an optical head. The µLCT 100 can be used as an OISL (Optical Inter-Satellite Link), a spacecraft to ground link or a spacecraft to UAV link.

SMC commander and USAF Space program executive officer, Lt. Gen. *John Thompson*, said the Air Force is leveraging modern commercial business practices to enable the rapid development of small business ecosystems that have dual-use, cutting-edge technologies to enable the fielding of fast, relevant and affordable solutions that support our Air Force.

, Space Micro CEO, added that the company is pleased to be in this select group of companies to present the firm's advanced secure space communications technology and products to senior Air Force and DoD officials — and then the company was selected for the maximum contract value of $3.0 million. Signing the initial contract on the spot within 10 minutes of verbal selection was truly amazing.

www.spacemicro.com



AvL TECHNOLOGIES

CONNECTING YOU TO THE FUTURE

1.35M FIT

FLEXIBLE INTEGRATED TERMINAL

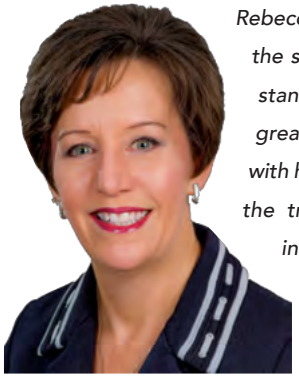
SMALL PACKAGE. BIG GAIN.

- ARSTRAT KA-BAND CERTIFICATION
- COMPUTER ASSISTED SATCAP MANUAL POINTING OR AUTO-AQUISITION
- BUILT-IN TUNER & BEACON RECEIVER
- TRI-BAND X, KU AND WIDEBAND KA FEEDS WITH QUICK CHANGE RF KITS
- MODULAR & FLEXIBLE MODEM, BUC & LNB OPTIONS
- SCALABLE: 75CM, 98CM & 1.35M
- SET-UP BY ONE PERSON IN MINUTES
- LIGHTWEIGHT IATA-COMPLIANT CHECKABLE CASES

avltech.com

An Interview with Rebecca Cowen-Hirsch, U.S. Government Business Unit, Inmarsat

Interview conducted by Catherine Melquist, President, MSUA, & Sr. Director of Channel Partnerships, NetNumber



Rebecca Cowen-Hirsch is an unmistakable leader in the satellite mobility industry and a valued, long-standing member of the MSUA Board. It is with great pleasure that I share my recent interview with her. Always thoughtful, Rebecca elaborates on the trusted partnership between the USG and industry, the role of satellite in the digital transformation era, today's satellite user communities, and why she values MSUA and serving on the MSUA Board.

Catherine Melquist (CM)
There is so much happening in the U.S. Government related to space. What activities do you believe to be most important to the satellite industry?

Rebecca Cowen-Hirsch (RCH)
Clearly, with the passing of the 2020 National Defense Authorization Act, the official launching of the U.S. Space Force brings the potential to transform space for the U.S. government with satellite communications (SATCOM) being one particular area of interest to Inmarsat. Led by Gen John W. "Jay" Raymond, Air Force Space Command and U.S. Space Command Commander, the Space Force will run as an independent service with Title 10 responsibilities. It will organize, train and equip forces to support operations run by U.S. Space Command or other combatant commands. Gen Raymond has said that, by creating the Space Force, "the President and Congress have given us a great opportunity to build the force we need to respond to the challenges we face in the space domain.

The creation of the Space Force represents a major milestone in what we have seen in recent years as impactful, forward momentum. This momentum has inspired the U.S. government to increasingly focus on the acceleration of a defendable space and the need for diversity, redundancy and resiliency of assets. Subsequently, the U.S. government has taken a number of steps and implemented strategies that promise to redefine how it acquires SATCOM, with the goal of developing an integrated SATCOM architecture of the future with enhanced capabilities, resiliency and affordability made available through commercial SATCOM owner-operators.

Just recently, the Space Force formally announced the signature of its Vision for SATCOM with the following imperative: "The signing of the U.S. Space Force Enterprise SATCOM Vision comes after a number of recent events that gave the command an opportunity to transform how SATCOM is procured, managed and delivered to USSPACECOM and other combatant commands around the world."

With this as backdrop in the current U.S. government environment, one key area of interest for the mobility communications industry is how this shapes new processes for acquisition reform, or how the U.S. government buys satellites communication and other services. Additionally, how the Department of Defense (DoD) forges new and evolving partnerships with commercial and Allies will be informative of how business relationships will change as a result.

CM
How do you see the USG and industry teaming together to leverage the benefits and opportunities of space? What are the challenges?

RCH
We are seeing meaningful, forward momentum to expand opportunities for the U.S. government and trusted commercial providers to work together as partners toward the achievement of these goals. This is supported by shifts in acquisition practices resulting in the government moving away from the ineffective status quo in favour of a more robust, integrated architecture. The Air Force has drafted an ambitious plan that could fundamentally change how it develops, buys and uses SATCOM. This plan is expected to identify next steps and timelines for implementing what is being called "the SATCOM Enterprise," which aspires to create a "holy grail" seamless network of military and commercial communications satellites, accessed by troops, vehicles, ships and aircraft via ground terminals and mobile receivers that would seamlessly roam from one satellite network to another.

Also, the DoD and federal agencies are updating their acquisition directives to remove restrictions requiring lowest price technically acceptable, which has been the predominant source selection criteria for commercial SATCOM (COMSATCOM). This would amend the Federal Acquisition Regulation to implement a section of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which states that specific criteria must be met in order to include LPTA source selection conditions in a

solicitation; and that procurements predominantly for the acquisition of certain services and supplies must avoid the use of LPTA source selection criteria "to the maximum extent practicable." The specific criteria should directly tie to architectural enhancements that the DoD is seeking to improve the resilience and performance of its integrated SATCOM Enterprise. As part of this, the DoD intends to enforce policies which will incrementally merge COMSATCOM capabilities into the overarching enterprise – a model that merits the wholehearted support of industry.

However, there are challenges to overcome for the partnership to truly realize its full potential. We need a clear line of authority that understands all of the essential pieces, pulls them together and watches over them – establishing a single, unified architecture. This authority would serve as a strong advocate of a government-commercial partnership, to champion investment as "commercial first" with funded programs which address SATCOM issues through improved capabilities, flexibility, mobility and resiliency, while eliminating the reliance on Overseas Contingency Operations funding, or OCO funds for COMSATCOM purchase.

An integrated architecture that plans for and funds, through appropriated budget as well a Defense Working Capital Fund, the all of SATCOM, military and commercial, is essential. Users should have open access to nothing less than a "fully stocked tool shed" – with some legacy, purpose-built platforms for their specific needs, but more modern, commercially-developed options primarily – to readily obtain mission-critical mobile and highly-available SATCOM across multiple spectrum. Without such a tool shed, an essential, fully integrated architecture with heterogeneous networks, modern capabilities and flexible resiliency will remain out-of-reach.

CM

As you know, we are well into the Digital Transformation Era. What does that mean to Inmarsat and U.S. government users?

RCH

The integrated architecture represents the very best of digital transformation thinking. It would allow for all altitudes and capitalize on capabilities which are existent and trusted, and continue to invest in innovative technologies. Such an architecture would make coverage and capacity "yesterday's conversation," with military and industry leaders more focused on combining a robust ground segment with adaptable terminals and a space layer, and COMSATCOM adding flexibilities through software-enhanced capabilities and flexible modem operations.

This is why we we should frame our imperatives upon SATCOM as a Service, which has emerged as the satellite acquisition model for the modern age that helps deliver that digital edge to end users. This is the model that Inmarsat's mobile-centric strategy embraces, unique in the market. Inmarsat's end-to-end robust network is owned and managed by Inmarsat, consisting of satellites, robust ground infrastructure and Inmarsat type-approved terminals. It is purpose built for government users who require worldwide mobility delivered through a single managed subscription. Its Committed Informatin Rates (CIR) throughout the world are backed-up by Service Level Agreements (SLAs) that guarantee government end users always get what they need and pay for.

SATCOM as a Service stays ahead of the demand curve by delivering next-generation technology advancements that arrive without additional capital investment from our customers. This enables the desired flexibility, security and cost-efficiency that allow government users to complement their MILSATCOM systems when and where needed, without any upfront commitment.

CM

MSUA was founded by Inmarsat as a forum for connecting with satellite user communities. As you know, MSUA is considering new forms of engagement with today's user communities. How do you group user communities for the USG? Do today's user communities differ from 20+ years ago when MSUA was created?

RCH

Highly mobile government users must share information in real time wherever their mission takes them. It is imperative that they stay connected, whether on land, at sea or in the air. Given that these users are always moving across the globe, often with little or no-notice, there is a sense of urgency for high-performing, reliable and secure voice, data and video that is always available. A dropped connection could jeopardize the mission, and ultimately, even lives.

These users include unmanned airborne operations with long reach and range that require more than air-to-ground links. For Beyond Line of Site (BLOS) communications as well as high data rate exfiltration, reliable, always-on satellite capability provides critical communications. Military forces at sea, U.S. Coast Guard operations, special operations vessels and other maritime units depend upon consistent satellite performance that is unaffected by geographic changes. With capacity in greater demand, through reliable satellite communication connectivity, tactical commanders make key decisions and pass along information about military assets in near real-time, anywhere in the world. When a natural or man-made disaster strikes, first responders must stand ready to deploy anywhere on Earth, at a moment's notice. In those situations, every second counts, and reliable

connectivity is imperative to maintain seamless communication services when existing access and core infrastructure may be damaged or destroyed.

Today, SATCOM is widely considered as a mission-critical enabler. Reliable access to, and distribution of, information always serves as a necessary part of any operation. Users need high-performing voice, data and video that "moves" seamlessly with them, throughout the entire mission, from training, in transition and at the designated site, no matter the geographical environment.

Even with all of this, I think the most significant change in our user community today is the increase pace of their activities and the dramatic increase in data rate demands over time, especially as the environment in which they operated is increasingly complex. Also, the users of today, across all sectors, are far more network savvy and expect a much higher quality of service then two, probably even just one decade ago. They expect the same type of quality, ubiquity and assurance that we enjoy from today's terrestrial and mobile telephony in our daily lives. These users are clever, innovative, and are already considering applications that were beyond the wildest dreams when we began MSUA.

CM

What is the best way to engage USG user communities so they are clear about the benefits of satellite versus other wireless technologies?

RCH

While perhaps trite to say, the answer is "communication." Clarifying the advantages of satellite technology as well as the interdependence of terrestrial and wireless technologies is even more important than ever. For U.S. government users, whether military or federal, the key is the recognition of the criticality of assured satellite communication networks in their mission-critical communications. Once this dependence is understood, then the comparative advantages of one technology over another in a given scenario can be properly applied. Over time, the real digital transformation will further be enabled when a user is able, through policy-based routing and mobile ad-hoc networking, to autonomously leverage the proper network solution, whether it be satellite, terrestrial, or wireless at the time and speed of need. Though we may be a few years away from that yet.

CM

Given that user experience/expectations is typically set by forms of wireless connectivity other than satellite, what steps is Inmarsat taking to align with the high-performance expectations of 5G?

RCH

As the backbone of the world's communications infrastructure, satellite services will play a critical role in enabling and extending terrestrial 5G networks by providing the network resilience and ubiquity of coverage needed. Both satellite and mobile operators will need to work collaboratively to deliver the 5G revolution. Neither can do it alone. Inmarsat sees our capabilities as complementary with 5G. Our network is robust and secure, trusted worldwide by governments, international institutions and global organizations to deliver safety and security. Our ubiquitous coverage means that we are uniquely positioned to help join the dots of connectivity between urban and rural, the developed and developing world, and sea, air and land. This will be even more vital in a world of smart cities, future mobility technologies, IoT and 5G.

CM

What are the most important Inmarsat innovations — current and future — in mobile connectivity to USG customers?

RCH

Seamless mobility is and will be core to U.S. government missions around the world, and Inmarsat is a major driving force behind technological innovation in mobile satellite communications. Inmarsat owns and operates the world's best global portfolio of satellite networks, specifically designed for customer mobility, and we strive to deliver government-focused innovation with continuous network improvements that lead the evolution of always-on global mobile connectivity and assured access.

Inmarsat's funded and approved investment strategy for the future ensures backward-compatible operations right alongside of innovations to provide trusted, mobile, global SATCOM networks well into the next generation.

The most significant current and future initiatives driving our innovation in narrowband and wideband include global L-band continuity well into 2040 and the expansion and innovation of our Global Xpress network:

Inmarsat 5th Global Xpress satellite - GX5, launched in November 2019, is the first step to be followed by further payloads all focused on meeting growing and changing market demands. Through this evolution of Global Xpress, we are taking revolutionary leaps forward in the way we design, deliver and operate our infrastructure; from satellites and ground stations, to terminals and network management. This is all to ensure that we are able to deliver new broadband capacity in step with rapidly growing and highly-dynamic customer demand.

The GX5 satellite will deliver additional, focused capacity to meet the rapidly growing demand for reliable, seamless, high-capacity

wideband services in the EMEA region with four independently steerable mil-Ka beams, complementing military satellite resources.

Inmarsat's sixth-generation, or Inmarsat-6, fleet, with the first satellite scheduled for launch in 2020, offers a unique hybrid payload that supports Global Xpress and extends L-band services to 2040. It will also usher in a new generation of capabilities for the 5G era, from advanced global safety services and low-cost mobile services to high definition streaming. The advanced Ka-band payload adds further depth to Global Xpress coverage, increasing capacity in regions with the highest demand.

Global Xpress Arctic Payloads, or GX10A & 10B, in partnership with Space Norway and its subsidiary, Space Norway HEOSAT, represent the world's first and only mobile wideband payload dedicated to the Arctic region and will integrate seamlessly into the current and planned Global Xpress network. The payloads, scheduled to launch in 2022, will be fully compatible with current and future Global Xpress terminals, ensuring that current Global Xpress customers can benefit from the further extension of the network. The new Arctic payloads will be placed into Highly Elliptical Orbits (HEO), with continuous coverage above 65° North and the ability to direct capacity in real-time to areas of highest demand. These payloads will also bring mil-Ka capacity through service beams and high-capacity steerable beams, complementing military satellite resources cost effectively for optimal redundancy, protection, scalability and global portability.

The next evolution of Global Xpress, which we call the GX7, 8 and 9 program, with the first satellite scheduled to launch in H1 2023, is a continuation of the transformation of our Global Xpress network capacity, capabilities and operational agility. Backed by the most advanced cybersecurity features of any global network, the next evolution of Global Xpress will deliver dynamically-formed beams that enable agile and precise allocation of ultra, high-power capacity over high-demand areas and allow for superior interference resistance. This innovative, software-defined global architecture with GEO satellites has flexible payloads that can be relocated when and where required across the geostationary arc and connect to any Inmarsat software-defined ground network node, enabling higher throughput speeds and flexible and dynamic capacity scaling based on user-specific resource demands.

CM

What's it going to take for satellite to successfully compete and gain visibility in the larger IT / Telecom market place?

RCH

Clearly, satellite communications encompass an entire universe of robust information technologies, beyond merely the satellites themselves. Most commercial users, whether enterprise or consumer, view satellite communications as a critical capability to support their business or mission need. For the government market, however, even with the advanced maturity and ubiquity of telecommunications provided by the commercial satellite industry, there remains a divide between historical military acquisition and the use of commercial systems how the industry delivers, and its users buy, services.

In the national security enterprise, technology is not the impediment — processes and cultural reluctance are. At what could be a turning point for systems procurement, the DoD will benefit tremendously when it commits to a fully integrated commercial foundation in the enterprise architecture which leverages the best that industry has to offer.

The final step is to embrace satellite communications as a service. Across the DoD and the broader national security enterprise, services acquired "as a service" models are widely employed for a vast range of mission-critical telecommunication and information technology capabilities. When communications satellites are viewed as a network, or even a network of networks that enable mission success, the processes and methodologies for acquiring these services can evolve accordingly.

CM

Final question — Inmarsat is a founding member of MSUA and you are a longstanding and highly valued member of the MSUA Board. To industry colleagues considering a membership in MSUA, what would you say are the most important benefits of joining the organization?

RCH

As one of the longest running industry and user associations, I would advocate engagement and active membership to not only stay abreast of industry relevant topics but also to help shape and influence the direction of the mobility industry. The Association also enables important connections for the growth of its membership companies' business as well as expanding its members' professional network. MSUA membership dues are affordable and a great return on investment since engagement with the association and benefiting from its reach and connections.

www.msua.org

Catherine Melquist is the President of the MSUA, and Senior Director of Channel Partnerships, NetNumber

SPACE FOUNDATION STATE OF SPACE 2020

What didn't come up...

Government Satellite Report: by Ryan Schradin, Executive Editor, GSR, and Senior Contributor

At the Space Foundation State of Space conference earlier this year, the full growth potential of the Global Space Economy was on full display.

Tom Zelibor

Driven by invigorated government interest in space capability and the innovations of private industry, Space Foundation President ***Tom Zelibor*** proclaimed that the $451 billion Space Economy is "*booming…[and] in the next two decades, it will climb to a trillion dollars.*"

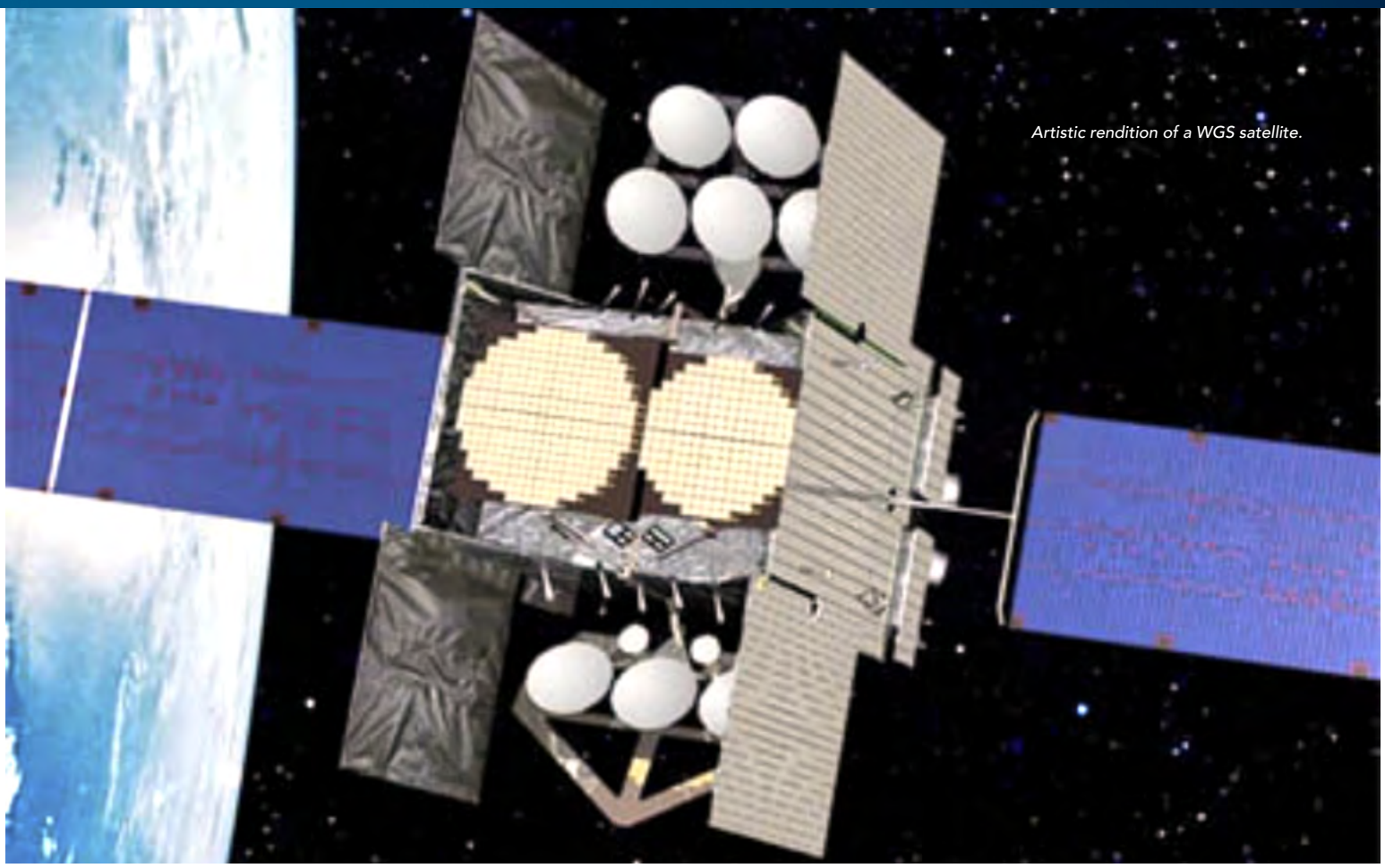
One panelist, ***Andrew Chanin***, manager of the **Procure Space ETF**, even predicted that "*space may be the first quadrillion dollar industry.*"

Andrew Chanin

With all of the opportunity and interest in the final frontier, the conference covered a wide variety of topics from beating near-peer competitor states to a permanent Moon base to the role of commercial launches and spacecraft.

But what also came up—repeatedly—were concerns about how quickly space is becoming a contested environment.

"*As everyone here knows, we're making the transition from when space was a sanctuary to space as a contested domain,*" Rep. ***Doug Lamborn*** (R-CO) remarked, citing a Russian satellite's recent apparent surveillance of the U.S. National Reconnaissance Office satellite USA 245. "*The future [of military satellites],*" *the Congressman continued, "is going to be [about] resilience. Things that are replaceable, things that are cheaper…[and] proliferated in great numbers.*" That way, he said of our military's satellite infrastructure, "*it's harder to take them all down.*"



Artistic rendition of a WGS satellite.

However, what wasn't mentioned were the various ways that commercially available innovations could address this need as well as secure our military's increasingly important space assets from so many of the other threats that any would-be adversary may bring to bear. For example, the government only operates ten WGS satellites worldwide, and if a near-peer adversary wants to deprive our military of satellite services, there are only ten satellites that they need target.

Leveraging commercial satellite constellations alongside those military satellites widens that range of potential targets to more than 150, making the denial of satellite capability to the deployed warfighter a much harder, if not unfeasible, proposition. Or, as the U.S. Naval Network Warfare Command's satellite communications operations head has said, "*you go after our [military-owned] systems, I've got something else that I can get to.*"

This resiliency is further increased by the latest generation of commercial satellites, which offer the military further means to guard against jamming and other attempts to deny satellite services.

These new satellites — including the spacecrafts that will make up the O3b mPOWER satellite service — feature a number of anti-jam capabilities, including smaller, more powerful beams and beam dynamics that can be modified in short order to evade or counteract an adversary's efforts to jam their signals.

As lawmakers and military leaders continue to consider means to steel our military enterprise against peer and near-peer adversaries and raise concerns about them at forums like State of Space, one thing that should be remembered is the number of solutions that commercial satellite constellations could bring to those problems.

The post ***Space Foundation State of Space 2020: What Didn't Come Up*** appeared first on ***GovSat***.

Ryan Schradin is the Executive Editor of GovSat Report. A communications expert and journalist with over a decade of experience, Ryan has edited and contributed to multiple popular online trade publications 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 GovSat Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting both written and podcast interviews. Ryan also contributes to the publication's industry event and conference coverage, providing in-depth reporting from leading satellite shows.

THE WEST'S MILITARY TECHNOLOGY IMPERATIVE

Public/Private Partnerships

by John Beckner, Chief Executive Officer, Horizon Technologies.

In 2019, Orbital, via an Antares 230, facilitated the launch of the first of the UK IOD programs (In-Orbit Demonstrator), run by the Satellite Applications Catapult.

The satellite carried Colorado-based Orbital Micro Systems' (OMS) payload to detect micro-weather via a space-based microwave radiometer sounding spectrometer, retrieving temperature data in eight vertical atmospheric layers. OMS is also teamed with Lockheed Martin UK, and provides the blueprint on how successful Public/Private partnerships work as they enter the lucrative GeoInt market.

This mission is proof that the UK's approach on incentivizing US/UK industry to work with government in getting cutting edge technology deployed and in operation quickly is working. The UK model of Public/Private partnerships in aerospace differs from the that of the US but offers lessons to the US and other Western powers.

The IOD-1 GEMS launch proved that the government supported innovation schemes can play a key role in the West's attempt to compete with China; economically and militarily. As pointed out in a recent paper by Stanford's Cyber Policy Center, Dr. ***Anthony Vici,*** the former CTO at the NGA (National Geospatial Intelligence Agency), noted that "*Simply increasing national security funding or R&D spending will not ensure victory against a competitor able to outspend the United States. Instead, we will need once again to revolutionize public-private partnerships to meet the challenge, harnessing more efficient ways of developing and implementing new technology.*"

Anthony's paper lays out a number of excellent suggestions on how public/private partnerships can be harnessed in the US to get private companies to move technology from TRL (Technology Readiness Level) -1 (Basic Research) up to TRL-8 (System Test, Launch, and Operation) much quicker than before,

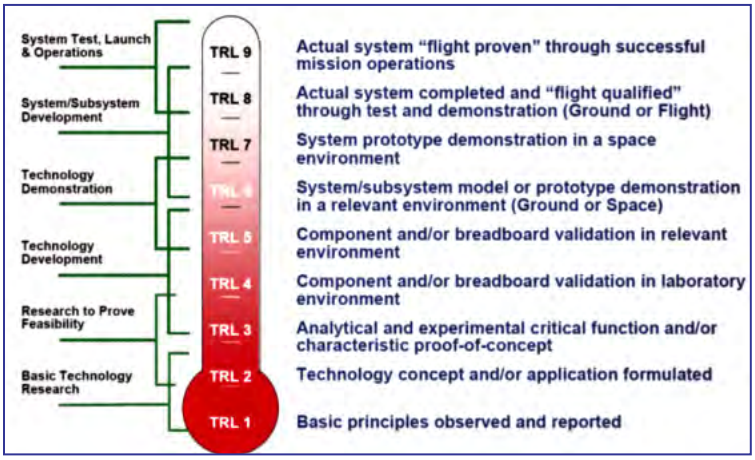
and be allowed to keep (or jointly own) their IP which is critical for many startups looking to success in the commercial as well as the aerospace/military market.

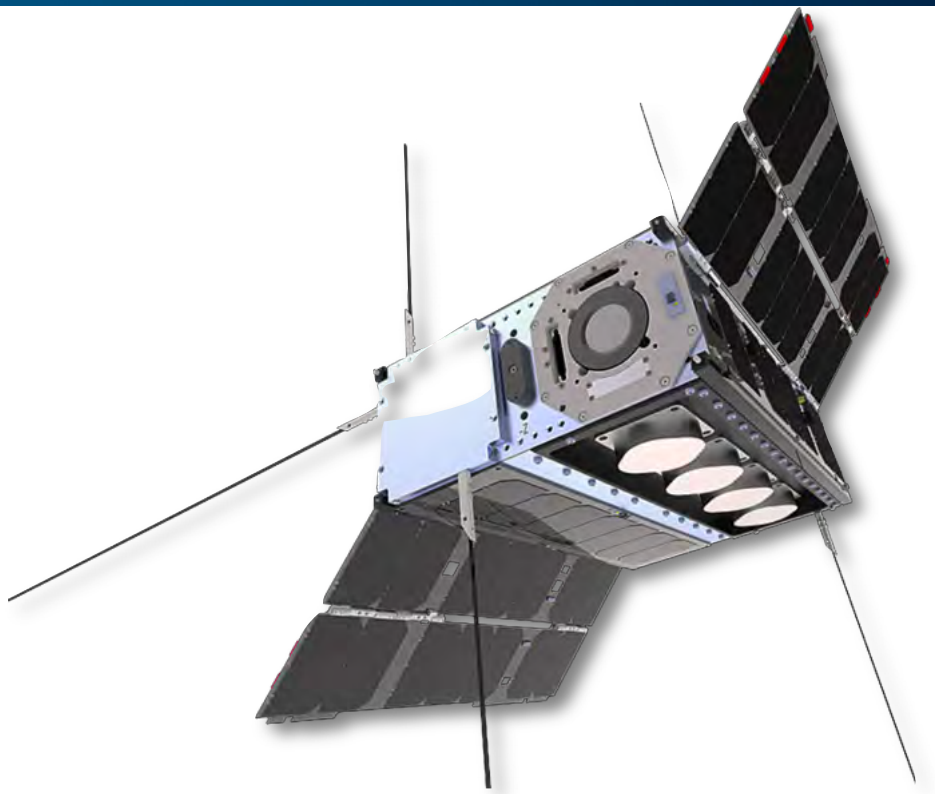
The problem for Western governments is very clear. Either they can stay with their slow cycles of tendering, procuring, and implementing new technology, or they can incentivize industry to spend their own money, keep their own IP, and let industry profit on technologies which have dual commercial/government value. Under the DoD traditional procurement process, over "requirement-ization" (as some call it) reigns supreme, and stifles innovation.

UK startup Horizon Technologies is at "ground zero" of the public/private effort in the UK as the company was selected for the 3rd Innovate UK-funded IOD mission by the Satellite Applications Catapult.

The IOD-3 Amber™ mission will see the first of a constellation of six (6) cubesats launch into Low Earth Orbit (LEO) to offer the UK and Allied nations a Maritime Domain Awareness (MDA) data product via "*Commercial SIGINT*" sensors on our payload. These sensors will track ships' AIS signals, maritime radars, SatPhone usage, and even illegal GNSS jammers which are increasing in prevalence. It's an innovation partnership whereby the UK government essentially funds 80 percent of the first satellite into orbit and operation; Horizon is required to invest its own money and provide the cubesat payload to the Catapult for £1.

Horizon didn't bid to any government requirement, or specification, tender or study program. They simply saw a need — worldwide military/civilian need to combat so-called maritime "*dark targets*"; those vessels who turn off their AIS transponders while engaging in illegal activity.





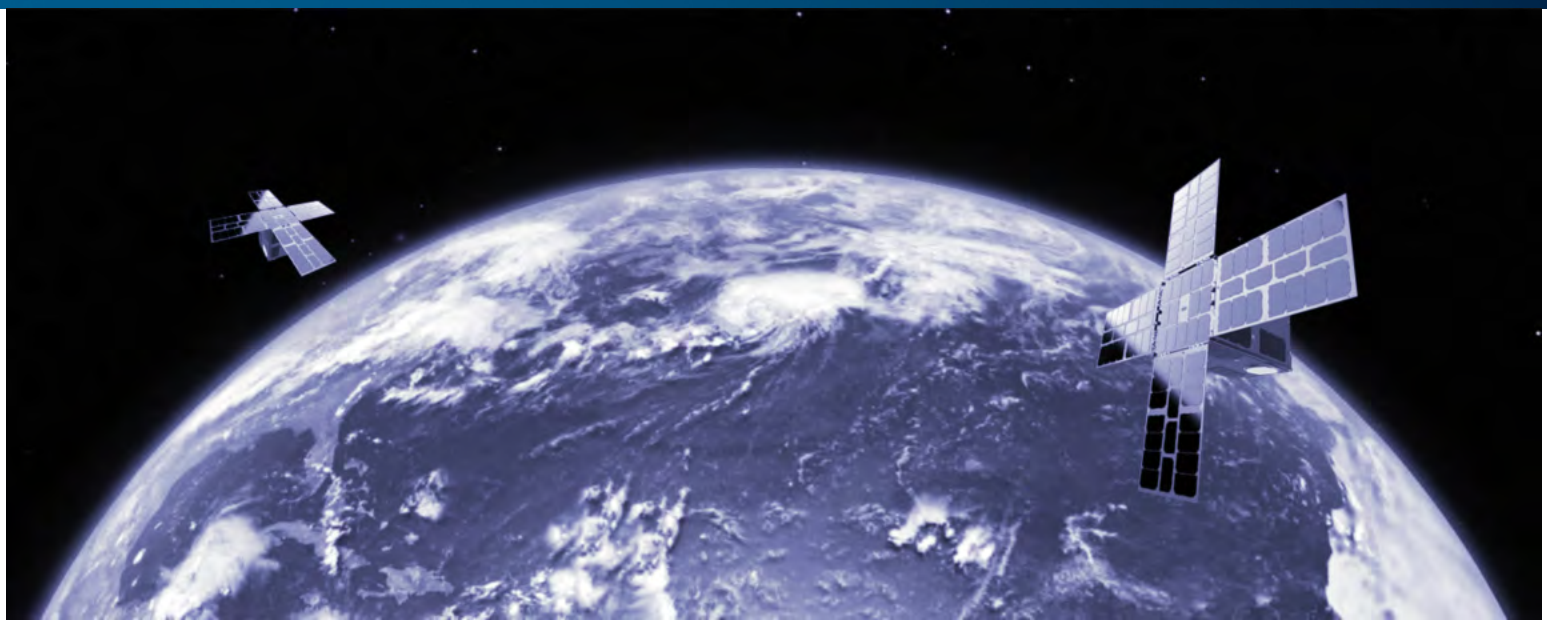
Artistic rendition of Horizon Technologies' Amber smallsat. Image is courtesy of the company.

Think of piracy, illegal fishing, smuggling, transshipments, and Iranian oil shipments. Under the UK's world-leading policy of incentivizing and funding cutting-edge technologies, small companies can move from "*PowerPoint to a cubesat in orbit*" in less than 24 months. Essentially, TRL-4 to TRL-9 in this short period. As someone who's been involved in aerospace, in and out of government, since 1982, this is nothing less than incredible.

Under the IOD program, the Catapult essentially acts as the program manager between the payload provider and the bus provider (in the case of IOD-3, AAC Clyde Space in Glasgow). The Catapult are delivering Innovate UK's vision to harnesses UK space/satellite expertise, and ensure that the IOD missions come to fruition, meet their goals, and provide economic growth for the UK.

There is a three (3) month down-select process whereby the leading candidates/technology have to present to a cross agency UK government board. Presented with a space-based GeoIntelligence (GeoInt) data source which they didn't have to fund or support, it's no wonder that the UK MoD has greeted the Amber™ program with open arms as have an increasing number of both large and small Allied countries which urgently need MDA/GeoInt data in their countries/regions with latency of less than one hour.

The current situation in the United States is different, and currently is focused not so much on public/private partnerships per se, but rather finding ways to get non-traditional technology



companies (like those in Silicon Valley) into DoD acquisition system and fielded.

With an R&D budget of $55.4 Billion (CY 17), the DoD is in a vastly different position than a much smaller European country like the UK. As stated above, it's very clear that there is a "*technology race*" on with China. China doesn't need innovation from private firms (which it lacks, in any case). It fuses commercial/military intelligence gathering to its topflight (often Western-educated) military R&D centers, and spends whatever is required to move ahead with new military technology; read AI, cryptography, hypersonic air vehicles, etc.

In the US, the first step to using non-traditional private industry to assist the DoD came with the formation (under the Obama Administration) of the DIU agency in 2015. While not a true Public/Private partner as the UK IOD program, it has proven to be a strong "*first step*" in getting non-traditional commercial companies to provide accelerated dual technology to the DoD.

According to ***Mike Madsen***, the DIU's director of strategic engagement (in a recent issue in *National Defense),"we start with the DoD customer with a DoD problem, and put it out to the tech sector to help solve our problems.*"

Recently the DoD gave DIU new contracting authorities in order to cut through the bureaucracy. In total, DUI has awarded about 150 contracts to 122 non-traditional vendors, with 66 being first-time suppliers to the military.

The beauty of the DIU approach is that, due to its locations in Mountain View and Austin, it can easily reach out to the commercial sector and VC investors to find the most appropriate commercial technology needed by the DoD. Currently, the top five DIU focus areas are AI/Machine Learning, Autonomy, Humans Systems, Space, and Cybersecurity.

However, according to a recent *Federal New Network* article, "*Since 2015, millions of dollars have been invested in the DIU, and the agency watched as some of its projects fell flat. Only about 23% the organization's completed projects ended up in the hands of troops.*"

Innovative counter-cyber and counter-drone technologies were a major part of the 23 percent, and these programs, despite some turmoil, have produced results. On the downside, Congress isn't particularly thrilled with the 77 percent of programs that didn't make it to contract.

The individual services in the US are not being left behind, either. The US Air Force Research Lab and AFWERX have partnered to form the U.S. Air Force Small Business Innovation Research (SBIR) program whereby small companies can obtain initial USAF funding outside of the traditional DoD system.

Established in 2017 by the Secretary of the Air Force, "*AFWERX is a catalyst for agile Air Force engagement across industry, academia, and non-traditional contributors to create transformative opportunities. The core mission of AFWERX is to improve Air Force capabilities by connecting innovators, simplifying technology transfer, and accelerating results.*"

AFWERX teams together with the Air Force Research Laboratory (AFRL), which works to streamline the SBIR process. The AFWERX/SBIR process defines requirements and technologies of interest to the USAF and gives small businesses the chance to get into market and start generating revenue. The AFWERX program has awarded $220 Million since 2018 in contracts to small business.

The EU has not yet embraced the public/private partnership technology route. The EU does have its own program to (1) start competing with China and Russia as well as (2) become more technology independent of the US and at the same time supporting competitiveness and innovation in the military/aerospace sector.

On June 7, 2017, the European Commission officially launched the European Defence Fund. This Fund has the goal of financing military R&D from an overall EU perspective. The main priorities are autonomous systems including UAVs, ISR, cyber and maritime security.

The budget for this program is €590 million from 2017 until 2020, and then €13 billion from 2021 until 20217. Unfortunately, with Europe's far less advanced high-tech technology startup culture, this funding is expected to go to the traditional European defense players. While more defense spending by the EU is certainly a good thing, the EU program simply does not incentive or unleash European commercial high-tech innovation.

It's very clear that there is an emerging awareness in the US and, with its Allies, that it has to use high-tech commercial base better to compete in a very challenging multi-polar world. To quote ***David Lloyd George***, "*Don't be afraid to take a big step if one is indicated. You can't cross a chasm in two small jumps.*"

Unfortunately, compared to the Chinese threat, many of the efforts listed above are too small, conform too much to existing traditional government procurement practices and don't engage the power of the small tech innovators. Yes, they are attracting new companies to the field, and that is certainly a positive step. However, there should be more "*leaps*" from TR-X to TR-9. In this, the US DIU and UK IOD satellite programs stand out. They should be emulated.

On a recent panel discussion as part of DGI 2020 where we recently participated, Dr. Vici used a fitting historical example for the way forward in harnessing technology via public/private partnerships. He cited the UK wartime program to crack the German Enigma encryption devices (themselves, ironically, a commercial product developed outside the 1920's Reichsmarine procurement channels) during World War 2.

The UK government went outside their normal MoD channels to recruit all sorts of people "*outside the system*" (civilian crossword puzzle experts, Oxford dons, chess masters etc.) who helped crack German Enigma messages. That is the spirit which is needed today; using non-traditional personnel and methods for military gain.

A broader historical example is President ***Franklin Roosevelt***, against tremendous bureaucratic resistance, appointing ***Bill Knudsen*** from General Motors to go outside of the War Department and head military/defense production in 1940 before America was in the war. In simple terms, the US used its world-leading commercial production techniques and applied them to military/industrial procurement on a massive scale. The US Navy could never have built "*Liberty Ships*" on such a vast scale, and so quickly, without private industry taking the lead; public/private partnership at its finest.

A typical World War II Liberty Ship. Photo is courtesy of the Library of Congress.

With the Chinese tech threat increasing, it is imperative that the United States, the UK and the West find development and procurement models which harness the innovation and agility of small commercial companies and allow them to leapfrog technologies to keep us at the forefront of this technological race.

The only way to do this is with Public/Private partnerships under a model which allow private industry to offer dual-use technologies to the military while retaining their IP, and their commercial rights.

In the end, I'm convinced "*High tech capitalism*" will beat state-targeted technology development, technology theft and spying.

www.horizontechnologies.eu/

John Beckner is the CEO of UK-based Horizon Technologies. Horizon Technologies is under contract to launch the UK's first SIGINT CubeSat constellation, Amber, as part of a public/private partnership sponsored by the UK Government.

CRITICAL MISSIONS SUPPORT

How the U.S. Government Leverages Commercial Innovation

by Tony Frazier, Executive Vice President of Global Field Operations, Maxar Technologies

In the last decade, the U.S. commercial space industry has pushed the limits of innovation to entirely new heights.

The industry is developing novel space-based solutions that support a wide range of missions and pioneering the development of technologies that will improve lives on Earth and explore and advance the use of space. Capabilities like artificial intelligence and machine learning (AI/ML) are increasing the speed at which analysts are able to solve critical problems from space; companies are coming up with disruptive new ideas that promise to increase access to what once was a frontier only available to national governments; and satellite imagery is becoming more persistent and more valuable.

This swell of innovation has not gone unnoticed by the U.S. government, which in recent years has placed an increasingly high value on the use of commercial services, hardware and imagery.

As reported by CNBC, this year's NASA budget request mentions the word "*commercial*" almost twice as much as last year's budget request. In a similar vein, the DoD and Intelligence communities have been focused on reforming acquisition to enable the rapid procurement of commercial technologies for years. For example, earlier this summer, the U.S. National Reconnaissance Office (NRO) selected Maxar to help them understand the satellite imaging capabilities that will be available in the years ahead.

As a trusted partner to the U.S. government for decades, Maxar plays a crucial role in delivering innovative Earth Intelligence and Space Infrastructure solutions for critical missions. In my role, I am responsible for all sales, business development, account management and service delivery across our combined national security and commercial customer base. This position provides me with a unique vantage point into the U.S. government's increasing use of commercial capabilities.

What I see in the Earth Intelligence realm is an insatiable appetite for more persistence and actionable intelligence — not just pixels. Persistence is the ability to stay on target and not lose track of objects of interest, whether located in space or on Earth.

At Maxar, we're amping up the delivery of persistence with the company's forthcoming WorldView Legion constellation, which will triple our 30 cm resolution capacity over the highest-demand regions on the planet and allow us to image the Earth from sunrise to sunset.

We're also leveraging our deep mission expertise and 1,500 cleared experts to continue delivering the highest resolution and most accurate commercial satellite imagery to the NRO through the

Maxar is building the Power and Propulsion Element of the NASA-led Gateway.

Maxar's WorldView Legion constellation will triple its 30 cm resolution capacity over the highest-demand regions on the planet.

EnhancedView contract and mission-ready satellite imagery in multiple classification levels through the Global EGD program, which was recently extended four years by the National Geospatial-Intelligence Agency. Maxar's WorldView Legion constellation will triple its 30 cm resolution capacity over the highest-demand regions on the planet.

Industry-leading imagery is not just the end product but a vital raw material for the answers and actionable insights we provide to various U.S. defense and intelligence agencies. Using our extensive expertise in AI/ML, data science, big data integration and domain-specific analytics, we gather content from many sources, sensors and providers, and then combine that content with powerful geospatial analytics to help customers be more predictive in their critical decisions and more productive in their daily operations.

This effort is highlighted in our recent work with the U.S. Air Force and U.S. Special Operations Command to help automate intelligence production cycles and integrate machine learning and computer vision capabilities into operations – evolving the mission from mapping to automated intelligence using machines. Maxar uses artificial intelligence and machine learning to deliver actionable insights for U.S. government customers.

On the Space Infrastructure side, we're seeing revolutionary capabilities brought to bear by the commercial industry. As demand for persistence grows along with humanity's desire to explore the universe and need for 24/7 global internet access, the necessity for more sophisticated technologies and greater access to space has become paramount. To address these requirements, entirely new approaches are being developed to enhance our understanding and use of space.

As in Earth Intelligence, Maxar is a leader in this arena. A few months ago, we were selected to build and fly the first element of the NASA-led Gateway, an essential component to NASA's Artemis program to land American astronauts on the surface of the Moon by 2024 and enable future crewed missions to Mars. In August of last year, NASA asked Maxar to leverage its experience as the space robotics partner for all six of the agency's Mars landers and rovers to deliver a robotic arm for use on the Moon. Maxar is integrating some of this robotic technology on the spacecraft it is building for NASA's Restore-L, which will refuel a satellite in Low Earth Orbit (LEO). Maxar is building the Power and Propulsion Element of the NASA-led Gateway.

Increasing access to space — the lifeblood of the space industry — is something that we're working on from multiple angles. Using robotics, we're developing SPIDER (*Space Infrastructure Dexterous Robot*), a dexterous system that will enable the on orbit assembly of satellites, telescopes and other systems that might not fit into a standard rocket fairing when fully assembled. With the firm's highly flexible, 1300-class satellite platform, we're able to offer rides to space for free-flying satellites and hosted payloads, including NASA's TEMPO pollution-monitoring instrument. We're entering a new and exciting era wherein commercial providers are creating revolutionary capabilities and disruptive ideas for space. This swell of innovation is transforming the way U.S. government agencies approach the development of new technologies.

As a trusted partner in Earth Intelligence and Space Infrastructure, Maxar is working at the leading edge of innovation to deliver disruptive, cost-effective and powerful solutions that build a better world and help our U.S. government customers solve their most complex problems.

www.maxar.com

Tony Frazier joined Maxar in 2017 after its acquisition of DigitalGlobe and serves as our EVP of Global Field Operations. In this role he leads all sales, business development, and services delivery activities for the company outside of the Canadian market. Prior to this role Mr. Frazier served as President of Radiant Solutions. Mr. Frazier served as Senior Vice President, General Manager of DigitalGlobe's Services business from 2013 and led GeoEye's Marketing and Communications team since 2010, prior to its acquisition by DigitalGlobe in 2013. Prior to GeoEye, Mr. Frazier served as Senior Director of Product Management at Cisco Systems, where he brought to market emerging technologies core to Cisco's video and collaboration strategy.

Prior to Cisco, Mr. Frazier held senior marketing roles at Infor, iPhrase Technologies, an MIT start-up acquired by IBM, and pcOrder.com. Mr. Frazier began his career in strategic consulting at Bain & Company. Mr. Frazier holds a Bachelors of Systems Engineering from the University of Pennsylvania and an MBA with distinction from Harvard University.

A UNIQUE PARTNERSHIP

Spectra SlingShot® and Inmarsat L-TAC™

Spectra Group and Inmarsat have established a remarkable and successful partnership between their two complementary technologies. SlingShot and L-TAC.

They combine to enable a unique capability — that of extending the range of tactical communications Beyond Line of Sight (BLOS) while maintaining Communications on the Move (COTM). Easily and accessibly. Designed initially with Special Forces in mind, but with obvious benefits for the broader military market, Spectra's SlingShot system comprises an appliqué, omni-directional antenna and a power source. The small appliqué converts in-service tactical UHF and VHF radios to L-Band satellite frequency so that it is possible to use Inmarsat's Global (except Polar regions) L-band Tactical Satellite (L-TAC) service. Complementing Military SATCOM (TACSAT), L-TAC with SlingShot is a genuine and effective COMSATCOM alternative but with added advantages.

SlingShot's simple conversion of UHF/VHF radio signals to L-band, transmitted across Inmarsat's non-contended global satellite network, offers the same BLOS communications enhanced with "on the move". These Channels are readily available across Inmarsat's Global Spot Beam network. This is a major advantage to legacy MILSATCOM, where communications must take place generally on the pause, and where Channels are in extremely short supply due to the high demand and limited capacity.

The combination allows users to augment and expand their existing tactical communications systems without the need to modify radio hardware or cryptography and in the knowledge that the channel is available where and when required. L-TAC channels are available on flexible leasing, from a month, and so can prove far more cost-efficient and flexible than comparable options.

Working uniquely together, SlingShot and L-TAC offer a combination of reliable voice and data connectivity, independent of local infrastructure, and available globally for vehicle-mounted and man-portable, land, maritime and air communications systems. Additionally, the SlingShot hardware is easy-to-use, requires minimal training and is highly cost-effective, in that it utilises in-service radio equipment.

The following scenario clearly illustrates the unique utility of SlingShot with L-TAC for command and control communications:

A coalition operation has a force lay-down that, by nature of the tactical situation and terrain, requires troops to be widely dispersed and able to manoeuvre rapidly.

Using in-service VHF manpack radios fitted with SlingShot and transmitting over L-TAC, the lead reconnaissance foot-patrol can provide a steady flow of information and intelligence as it moves forward; seamlessly in touch with their higher command, now situated well to the rear, without pausing to set up antennas. Live Situational Awareness feeds are transmitted from forward troops to the HQ by the SlingShot-enabled tactical radio over L-TAC, so they know the exact position of troops and assets at all times.

Through the same communications networks, the mounted elements of the main assault force can maintain communications with both the reconnaissance patrols and their HQ as they manoeuvre far beyond the range of tactical VHF combat radio, without the need to establish and secure radio re-broadcast equipment.

On another level, also using SlingShot / L-TAC combination, the force commander can be on the move and still able to speak securely and reliably to all subordinate elements, as well as to flanking coalition partners. Logistic elements that follow to the rear, possibly hundreds of kilometres away, can re-deploy to forward supply areas while maintaining effective communications, without the need for range-extension sites or the technical challenges of establishing mobile HF comms.

Combined with Inmarsat's L-TAC lease service, SlingShot is designed for security and reliability. Once deployed, remote management and support are provided through Spectra's 24/7 network operation centre, supported additionally by Inmarsat's 24/7 NOC. So, whether required for defence & security, border security, aid and emergency, or commercial utility; if effective, secure, and cost-effective, BLOS voice and data communications are necessary for demanding, remote and hostile environments, then Inmarsat's L-TAC enabled by Spectra's SlingShot is the solution.

In summary SlingShot, in combination with L-TAC, can provide:

> Strategic, secure tactical communications
> Global coverage
> Dedicated bandwidth
> Voice and data; including Situational Awareness

With the following features:

> Uses existing radio hardware and cryptography
> Very small form factor, lightweight and low power consumption
> Multi-platform: works with dismounted personnel and on land, marine and air platforms (fixed wing and helicopters).
> Global access with strategic backhaul
> Narrow, Multi-headed and Customized Beam footprints available
> Beyond Line of Sight Communications independent of local infrastructure
> Easy to use
> Netted voice and data for an all-informed network
> On the move, on the Pause or in Static HQs
> Flexible leasing, with channel lease options from one month

Delivering Beyond Line of Sight capabilities including:

Ø Secure Voice
Ø Biometric Database Access
Ø Situational Awareness
Ø Artillery fire-plans
Ø Email, file transfer and chat/free text

www.spectra-group.us

www.inmarsat.com/service/l-tac/

SPACE DEBRIS CONCERNS FOR MILITARY OPERATIONS

by Brian Swinburne, Director, Space Data Association (SDA)

Space debris is not a new issue, it has been an ongoing problem in orbit for years. Since the first launch in 1957, defunct human-made objects have been accumulating in space.

Whether it's the debris that was deliberately released from a launch vehicle and spacecraft separating, the fragments generated from unexpected collisions, or simply derelict payload carriers. As of January 1, 2020, the volume of debris in Earth's orbit putting military satellite operations at risk, *exceeded 8,000 tons*[1].

Military Communications

Communications for all sectors of the satellite industry are important, but for the military they are absolutely essential. While concerns within the commercial sector revolve solely around financial stability, for the military they extend to political stability as well. ISR data from satellites, supports the monitoring of enemy movements, enabling personnel to respond swiftly to approaching threats. Consistent connection represents a vital support for national security.

Without tools such as PNT services to monitor and target the enemy reliably, operations are left vulnerable. In situations where changes in intelligence have life or death consequences for troops on the ground, it is imperative that they are able to pick-up and send information as quickly as possible. Operations in the field rely on stable communication. Removing the need for ground systems infrastructure, provides versatility and ensures troops can react quickly to commands. However, carrying equipment across uneven terrain leaves personnel vulnerable and tests the limits of the communication tools available to them.

The best way to support personnel in dangerous situations, is by efficient management of communication, and that relies on effective management of the space environment. Space situational awareness is key to ensuring missions operate as efficiently as possible. Satellite communications represent the secure transfer of intelligence, which in turn facilitates the ongoing safety of missions – space debris threatens this exchange.

Orbital debris is assessed by the U.S Space Surveillance Network, its records cover objects larger than 10cm in LEO and objects spanning 30cm to 1m in GEO. More than 23,000 of these larger pieces of debris are regularly monitored. However, the total number of objects including those as small as 1cm, are estimated at around 500,000 — fragments smaller than that and the number grows to over 100 million. From these huge figures only a tiny proportion of objects, approximately 1,200 are operational satellites. While these numbers provide an indication of the scale of the issue as it currently stands, it will soon increase exponentially.

Changes to Low Earth Orbit

More cost-effective access to Low Earth Orbit (LEO), means there are currently several commercial entities exploring potential LEO missions. In October 2019 SpaceX requested permissions to launch an additional *30,000 LEO satellites* on top of the 12,000 already approved by the ITU and FCC. Before recently filing for bankruptcy, OneWeb had been aiming to secure *25 percent of global space broadband capacity*, by the end of 2021. It is currently unclear who will step-up to take OneWeb's place, but the opportunity to provide low-latency connections, to rural areas in the developing world, will be of interest to many potential contenders.

These changes to orbit led by the commercial sector, along with hundreds more small satellite launches from non-profits and universities, means space is about to become very crowded indeed. Now is undoubtedly the time to collate data for effective space traffic management, before our orbit becomes unmanageable.

Navigating the extent of space debris is already difficult, but factor in the volume of new launches scheduled over the next few years and it becomes extremely daunting. Like all big challenges however, this is a collective problem. The only way to resolve it, is for all sectors of the industry to work together. There are a number of precautions that can be undertaken to ensure that debris is managed as effectively as possible.

De-orbiting and Re-orbiting

Successful re-orbiting and de-orbiting is a key factor for consideration. Maneuvering a satellite away from active orbit at the end of its lifetime, is critical to ensuring sustainable long-term use of space.

For geostationary satellites, due to the change in velocity needed to de-orbit, most of the time it is necessary to undertake re-orbit. Transitioning the satellite away from operational orbits which are in regular use, into a higher graveyard orbit. This relocation means that the decommissioned satellite will not return to the active zone for at least 100 years. It involves raising the orbit to one greater than 235km+ (1000 x Cr x Area/mass) above the geosynchronous orbit. Historically there has been mixed results from GEO satellite operators, implementing requirements for re-orbit. Up until the early 2000s approximately two-thirds of GEO disposals were in breach of IADC guidelines. Fortunately, in recent years these numbers have flipped, with two-thirds of GEO satellite repositioning now being undertaken successfully.

Decommissioning satellites in a LEO of below 2000km altitude, represents the biggest challenge by far. The continued increase of individual LEO small-sat and cube-sat launches, as well as plans for LEO mega-constellations scheduled for completion in the next few years, means that strict legislation must be adhered to. IADC regulations require mandatory de-orbit for LEO. Decommissioned satellites must be positioned to descend with atmospheric drag, and re-enter Earth's atmosphere to burn-up within 25 years.

SpaceX has confirmed that it will comply with FCC disposal orbit guidelines, for LEO satellites that have been decommissioned. However, they are not the only player in this lucrative new market. It is currently estimated that 10-15% of small mass-produced satellites will become inoperable before they complete missions. With the projected scale of mega-constellations this would result in extensive debris, seriously jeopardising all active operations. There have been valid concerns that if companies become bankrupt during the initial competitive rush, it will leave abandoned assets without an operator assigned to properly decommission them. OneWeb's recent bankruptcy leaves 74 satellites in orbit and it may not be the only victim of current market uncertainty.

These challenges require a pro-active approach to ensure that the success of all missions is assured for years to come. We cannot adopt a "*fix it later*" mind-set to space debris, and as with any issue involving multiple interested parties the solution lies in collaboration.

Data Sharing

Due to respective security risks and financial investment, both the military and commercial sectors have historically been very protective of information. The Space Data Association (SDA) enables all satellite operators to work together on improving mission safety, without compromising national defence.

In order to mitigate risk, it's important that collective data sharing measures are put in place in ahead of the huge changes to LEO orbit. SpaceX has recently agreed to publicly share two-line element (TLE) data for its operations, to support the monitoring of satellite constellation trajectories. Sharing TLE information is vital for collision avoidance manoeuvring and assists with risk analysis - benefiting all operators.

The military naturally holds concerns regarding satellite operations intelligence, but the SDA's approach safeguards data, and avoids compromising the individual operator. Rather than requiring TLE information to be publicly available, participants are able to access, secure, accurate information which will improve conjunction assessment via the SDA.

This layer of security means members can connect across, military, commercial and non-profit sectors to ensure access to key data without disclosing sensitive information.

By consolidating data that will help prevent collisions, the SDA benefits all operators. Providing technical support and effective use of shared resources from its Space Data Center, to reduce the individual costs and workload involved in monitoring debris. The SDA then provides authoritative contact information, to the operator affected by a given space object to mitigate risk.

Innovating the Future

Machine learning and AI play a key role in the future of space situational awareness and the process of issuing conjunction data. Currently the Space Data Center generates approximately 2,000 conjunction reports, these must then be assessed to see which pose a significant threat.

Machine-to-machine interface provides the automated tools which warn of close approaches, but currently a degree of human support to assess potential dangers is still required. With the addition of more sophisticated AI technology, the accuracy of predications would increase significantly. Providing an earlier conjunction warning system, as well as delivering advance guidance on the best path to avoid collision. In future this could mean an immediate direct response from satellites to prevent collisions. Ground-based operators would then be updated by on-board systems, to ensure that the changes to orbit do not affect other satellite trajectories.

As technology becomes more advanced, the industry can facilitate AI innovation, by providing vital data to develop automated manoeuvre protocols. The industry as a whole, needs to work together to accept collective responsibility and manage space debris. The SDA represents a bridge between military and commercial sectors to enable all operators to safely share information and protect their respective investments, as well as ensuring the safety of all missions.

www.space-data.org

The author is Brian Swinburne, Director, Space Data Association (SDA).

TARGETING U.S. TECHNOLOGIES: PART ONE

A report of foreign targeting of cleared industry — Defense Counterintelligence and Security Agency

The transition of the Defense Security Service into the Defense Counterintelligence and Security Agency (DCSA) has involved integration of new missions, including background investiga-tions, and expansion of our security training enterprise. Even as we transition, we remain dedicated to securing the National Industrial Base (NIB) as part of our mission to strengthen national security and provide risk management services. As such, DCSA continues to work with cleared industry to detect and deter foreign entities' attempts to illicitly acquire classified and sensitive information and technology.

Securing the NIB is more relevant and more challenging than ever as our nation faces the most significant, diverse, and resourceful foreign intelligence threat it has ever experienced. The DCSA transition goes beyond new missions to include the development and implementation of new methodologies to secure the NIB. DCSA's new methodology is data-driven, risk informed, and partner-enabled. DCSA continues to move toward National Industrial Security Program compliance coupled with an asset-focused and threat-driven oversight methodology.

In protecting assets -such as the technologies, information, and personnel at cleared facilities -it is important to identify the threats, determine vulnerabilities, and implement appropriate countermeasures. These factors are essential in developing and successfully applying tailored security plans to protect assets at cleared facilities.

DCSA's annual report, Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry, is a key resource that identifies and describes the threat foreign entities pose to critical technologies and classified information in the hands of cleared industry. I encourage you to use this report as one tool in your risk management toolbox in determining strategies to mitigate risks to critical assets.

Charles S. Phalen, Jr., Acting Director
Defense Counterintelligence and Security Agency

SECTION 1: BACKGROUND

Scope

During fiscal year 2018 (FYI8), the approximately 13,000 cleared contractor facilities reported 6,026 incidents that the Defense Counterintelligence and Security Agency (DCSA) considered a suspicious contact report (SCR). An SCR is a report DCSA receives from cleared industry that contains indicators that are either likely, almost certain, or for which there is an even chance that an individual, regardless of nationality, attempted to obtain unauthorized access to sensitive or classified information and technology or compromise a cleared employee.

These 6,026 reports are the basis for the numeric listing of foreign intelligence entitles (FIE)[1] targeting of cleared industry. In addition, we include case studies and assessments of foreign entitles targeting U.S. technologies based on publicly available sources to augment the data and provide examples of foreign collection targeting cleared industry. The primary source of these case studies is the Department of Justice press releases published following the unsealing of indictments or following adjudication of cases. In case studies based on indictments, these contain allegations that a defendant has committed a crime. These defendants are presumed to be innocent until and unless proven guilty in court. Although some of the actual incidents used in the case studies did not occur in FYI8, the tactics described in the case studies remain relevant.

Assessing Foreign Intelligence Entity Threat to Cleared Industry

This article details and enumerates cleared industry's reporting of SCRs that represent potential FIE attempts to illicitly acquire U.S. technologies resident in cleared industry. As an unclassified product, this report does not provide a holistic view of the FIE threat to cleared industry. An SCR from cleared industry represents an incident where a cleared facility's security protocols identified a potential FIE attempt to collect on U.S. technology. Therefore, an SCR, along with demonstrating FIE targeting to some extent also represents a success for a facility's security posture and its Counterintelligence (CI) awareness and reporting regimen. DCSA cannot estimate in this forum the volume or targets of FIE activity that go unnoticed or unreported by cleared industry. DCSA annually produces a companion report at the classified level — *Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry*.

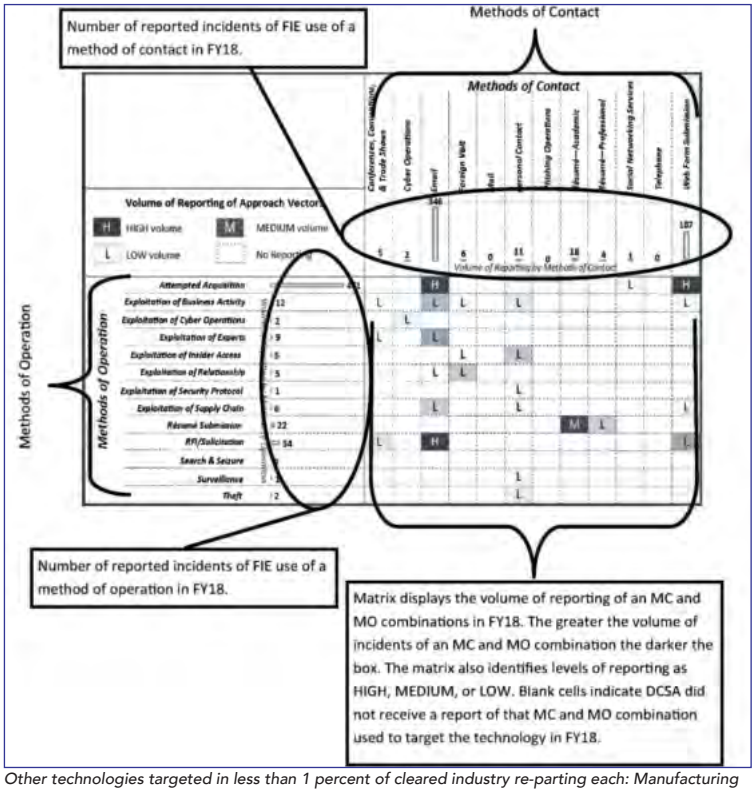
Counterintelligence Awareness and Training

DCSA Counterintelligence Directorate has unclassified outreach products that provide information on CI topics. They are available on the DCSA homepage: ***https://www.dcsa.mil/***

The Center for Development of Security Excellence (COSE) provides diverse security courses and products to Department of Defense (DoD) personnel, DoD contractors, employees of other federal agencies, and selected foreign governments. CDSE content and course information is available at their web site: ***https://www.cdse.edu/***

Displaying FIE Methods of Targeting Technology in Cleared Industry

Foreign entities use approach vectors that include a method of operation (MO) paired with a method of contact (MC) to attempt to illicitly obtain access to information and technology. The graphic below is an example of a matrix of FIE approaches, commonly referred to as the MCMO or 12x13 matrix (12 MCs x 13 MOs). This matrix depicts the volume of reported incidents of targeting of a specific technology in FY18. It displays the MCs and MOs used in incidents reported by cleared industry in FY18, which were likely attempts to illicitly gain access to technology, information, or cleared employees at the facility.



Other technologies targeted in less than 1 percent of cleared industry re-parting each: Manufacturing Equipment & Manufacturing Process; Nuclear; Chemical; Medical; Quantum Systems; Nanotechnology; Energetic Materials; Cognitive Neuroscience; Signature Control. Technologies with no reported targeting in FY18: Computational Modeling of Human Behavior, and Synthetic Biology.

SECTION 2: EXECUTIVE SUMMARY

In FY18, DCSA received nearly 50,000 reports of suspicious activities from cleared facilities operating as part of the National Indus-trial Security Program (NISP). Of these, DCSA CI Special Agents and Intelligence Analysts reviewed and identified 6,026 as incidents of CI concern (considered SCRs) that are likely incidents of a foreign entity attempting to illicitly obtain information or technology resident in cleared industry, or an attempt to compromise a cleared employee. These reports are the basis for ranking FIE targeting of U.S. technologies resident in cleared industry.

Key Findings from FY18 Cleared Industry Reporting

Top targeted technologies based on cleared industry reporting in FY18 and the percentage of reports by Industrial Base Technology List (IBTL) category.

1.	Electronics	9%
2.	Aeronautic Systems	7%
3.	Command, Control, Communications, and Computers (C4)	5%
4.	Armament & Survivability	5%
5.	Optics	3%
6.	Radars	2%
7.	Software	2%
8.	Space Systems	2%
9.	Marine Systems	2%
10.	Energy Systems	2%
11.	Positioning, Navigation, & Time	1%
12.	Sensors (Acoustic)	1%
13.	Materials: Raw & Processed	1%
14.	Ground Systems	1%
15.	Lasers	1%
16.	Biological	1%
17.	Directed Energy	1%
18.	Agriculture	1%

- *The number of reports assessed to be a suspicious contact increased by 3 percent over FY17*
- *The top four most targeted technologies in FY18 were in the top five most targeted technologies in FY17*
- *Optics was the fifth most targeted technology; previously it had not been one of the top five*
- *East Asia and the Pacific was the most commonly identified origin of incidents reported by cleared industry*
- *Attempted acquisition of technology was the most common MO*
- *Exploitation of cyber operations increased by 55 percent in FY18*
- *Email was the most common MC used in 41 percent of the reported incidents*
- *Phishing operation was the second most common MC used in 9 percent of the incidents*
- *Cleared industry reporting also noted foreign collection targeting services provided by cleared industry*

Overview

Overall reporting that DCSA categorized as a suspicious contact report increased by 3 percent in FY18. Reports where the specific technology or Industrial Base Technology List (IBTL) could not be identified amounted to 49 percent of the reporting. This is up from 40 percent in FY17. Electronics was the IBTL category that experienced the greatest increase in volume of reported targeting. Reported targeting of electronics increased by 73 percent in FY18.

Electronics were the most targeted technologies in FY18. Integrated circuits were the most targeted category of electronics.

Aeronautics systems dropped from being the most targeted in FY17 to second most targeted in FY18. Aeronautics systems experienced a 15 percent decrease in targeting in FY18. Actors targeting aeronautic systems most commonly sought Unmanned Aerial Vehicles (UAV) technology and information.

Along with UAVs and drones, unmanned or independent systems were commonly targeted across technology sectors. Artificial intelligence was a highly targeted software. In marine systems, FIE targeted autonomous underwater vehicles and unmanned surface vessels technology. Similarly, unmanned ground systems technology was also targeted.

In FY18, cleared industry identified entities from East Asia and the Pacific region in more than 40 percent of reporting. The volume of reporting DCSA associated to entities in East Asia and the Pacific increased by 20 percent in FY18. Entities from this region were identified in over half of the incidents targeting electronics and a third of the incidents targeting aeronautic systems.

China, an East Asia and the Pacific region country, has been cited in multiple U.S. Government investigations and initiatives as having policies for technology transfer and intellectual property theft that pose a threat to U.S. economic security.

The Near East remained the second most active collector in FY18; even with a 37 percent decrease in the number or reports associated to entities from this region. Entities from this region most commonly targeted aeronautic systems and armament and survivability technologies.

The Near East remained the second most active collector in FY18; even with a 37 percent decrease in the number or reports associated to entities from this region. Entities from this region most commonly targeted aeronautic systems and armament and survivability technologies.

Cleared industry reporting in FY18 identified commercial entities as the collector in 42 percent of all reports. These entities used attempted acquisition of technology MO in approximately 35 percent of reported collection attempts. In addition, these entities relied heavily on email as the MC, using email in nearly 72 percent of these attempts.

FIE applied attempted acquisition of technology, request for information (RFI)/solicitation, or exploitation of cyber operations in 54 percent of incidents in FY18. Most of these attempts were accomplished remotely via email and web form submission, not requiring the collector to have direct contact with the target or even be in the United States.

Exploitation of cyber activity increased by 55 percent in FY18. Although in overall data it was one of the top MOs the origin of the incident and the specific targeted technology are often unknown.

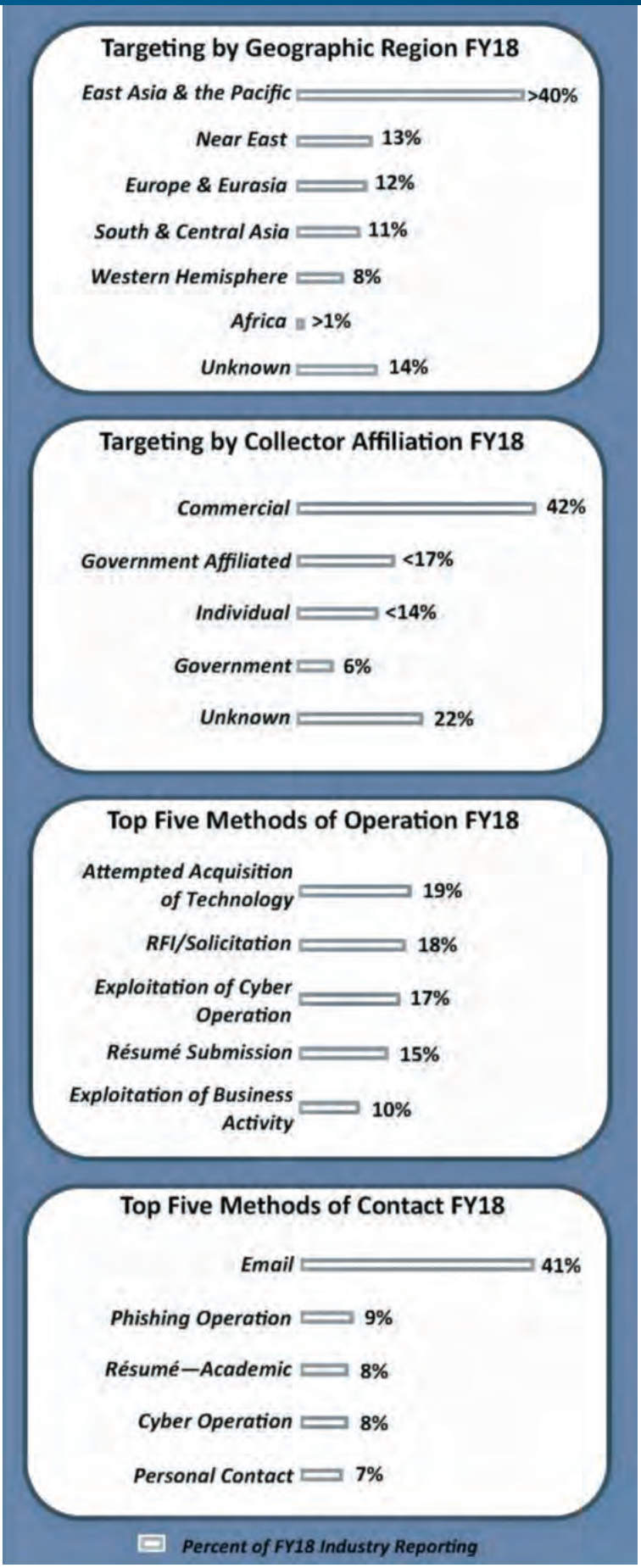
Email was overwhelmingly the most common MC used in FY18 by FIE targeting cleared industry. Cleared industry cited email in 41 percent of the reports. This does not include the 9 percent of FY18 reporting which listed the MC as phishing operation, which is an attempt to send malicious code via an email. Combining email and phishing operation, cleared industry received half of all incidents via email.

FIE use approach vectors in their collection attempts. An approach vector includes an MO, the method the actor uses to obtain the information, with an MC, the method the actor uses to contact the target. The most common approach vector in FY18 was attempted acquisition of technology sent via email.

SECTION 3: TARGETING OF TECHNOLOGIES

Reported foreign targeting of electronics

Electronics is the study and engineering of electrical circuits and components. Electronics are the building blocks for almost all



technologies, and each system may contain hundreds if not thousands of electronics performing a specific function to ensure the operation of a system. Electronics includes, but is not limited to, integrated circuits, programmable memory, and wafers.

Key Findings from FYI Cleared Industry Reporting

- *Electronics was the most targeted technology category in FY18*
- *Reported targeting of electronics increased by 73 percent over FY17*
- *East Asia and the Pacific region was the origin of most reported targeting of electronics*
- *Attempted acquisition of technology was the most common MO and email was the most common MC used to contact industry in attempts to target electronics*

Overview

For each of the past 7 years, electronics has been one of the top three targeted technologies based on cleared industry reporting of suspicious contacts by foreign entities. Integrated circuits, primarily monolithic microwave integrated circuits, were the most targeted subcomponents in FY18.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in over half of the incidents involving electronics. Reported incidents of targeting of electronics by entities from the East Asia and the Pacific region increased by 192 percent in FY18 compared to FY17. Electronics has been the top targeted technology by this region in 4 of the past 5 years. In FY18, their targeting included integrated circuits, radiation hardened (RADHARD) integrated circuits, digital signal processors, and circuit boards.

South and Central Asia entities were the second most active collectors targeting electronics. Entities from this region targeted integrated circuits, RADHARD, and field programmable gate arrays (FPGA). Entities from Europe and Eurasia were the third most active and targeted integrated circuits, FPGAs, and wafers.

Cleared industry identified commercial entities in three quarters of the incidents involving electronics. Commercial was the most common affiliation targeting electronics from all six of the geographic regions.

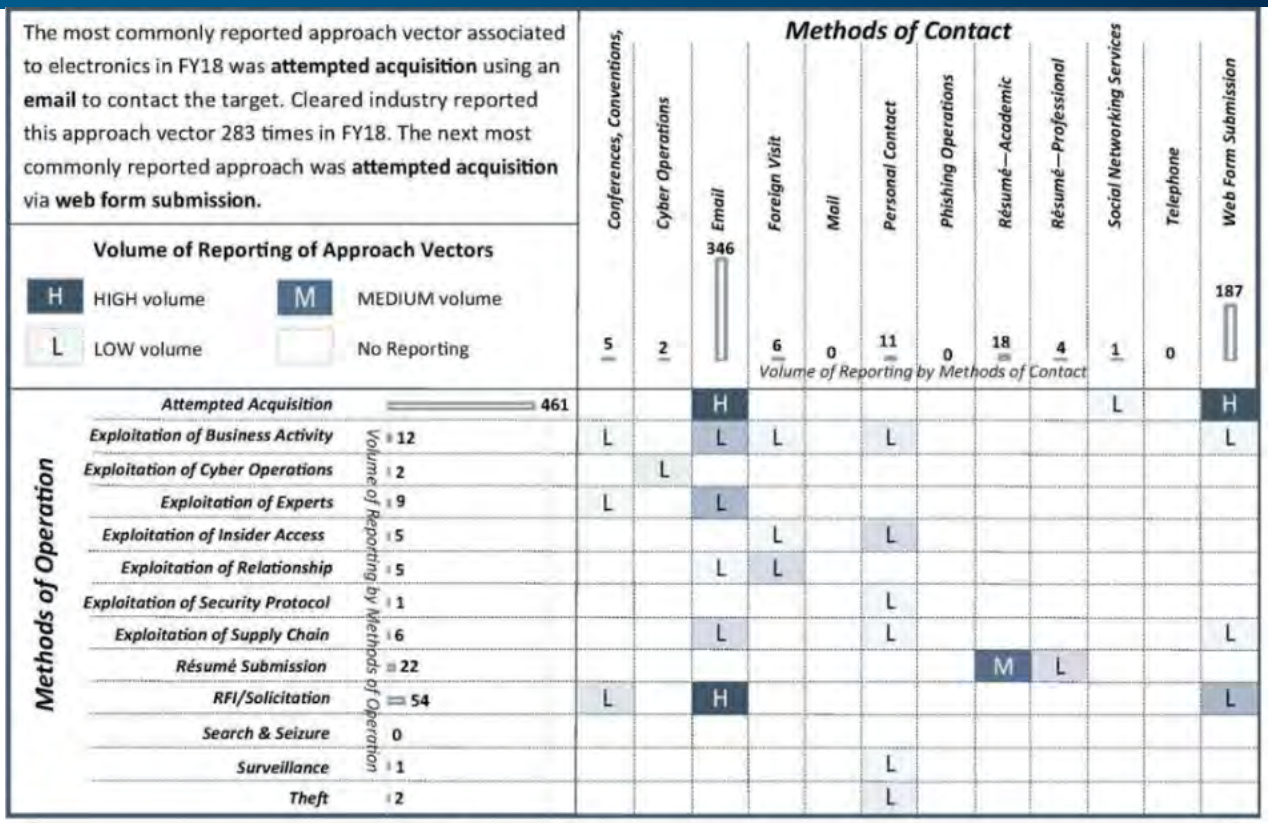
In FY18, entities targeting electronics used the attempted acquisition of technology MO in 79 percent of the reported incidents. Email was the most common MC, used in 60 percent of the incidents.

The most commonly reported approach vector associated to electronics in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 283 times in FY18. The next most commonly reported approach was **attempted acquisition** via **web form submission.**

Volume of Reporting of Approach Vectors

H HIGH volume M MEDIUM volume

L LOW volume No Reporting



Top Targeted Electronics Subcomponents

- Integrated Circuits
  - Monolithic Microwave Integrated Circuits (MMIC)
- Radiation Hardened Integrated Circuits
- Field Programmable Gate Arrays
- Digital Signal Processors
- Circuit Boards
- Vacuum Tubes
- Wafers

Targeting Electronics Case Study

Indicted in 2018, an electrical engineer was convicted in 2019 of conspiring to illegally export MMICs with commercial and military applications to China

- U.S. Person (USPER1) conspired with USPER2 to gain illegal access to a protected computer at a U.S. Company
- USPER1 was the president of a Chinese company placed on the Commerce Department's Entity List in 2014
- USPER2 created an account on the targeted U.S. company's web portal posing as a domestic customer seeking to obtain MMICs for use in the United States
- USPER1 gained access to the company's web portal using USPER2's account

Takeaway: Web form submission is a common MC. It allows a level of anonymity and for illicit actors to pose as legitimate domestic customers and obfuscate the ultimate destination of the parts.

Source: U.S. Department of Justice, U.S. Attorney's Office, Central District of California, https://www.justice.gov/usao-cdca/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips

Takeaway

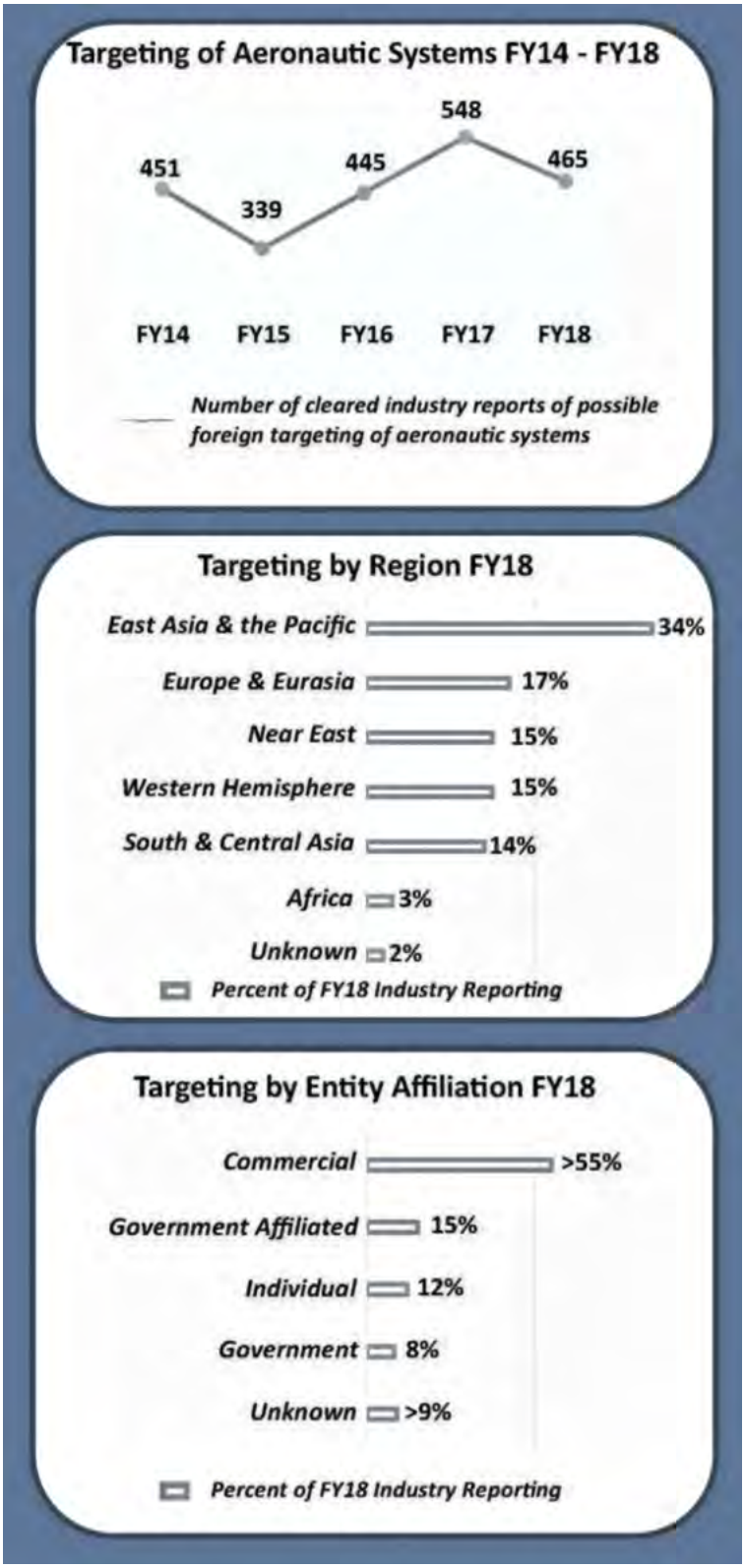
Cleared facilities developing or applying leading edge and legacy electronics technologies are reporting incidents of foreign entities targeting electronics in a greater volume than any other technology category. Integrated circuits, especially with special use properties such as radiation hardening, are highly sought after. The electronics sector is also vulnerable to counterfeit and substandard parts entering the supply chain.

Reported Foreign Targeting of Aeronautic Systems

Aeronautic systems include combat and non-combat air vehicle design and capabilities. This category does not include armament and survivability, C4, and intelligence, reconnaissance, and surveillance (ISR) technologies that may be added to aeronautic systems for a specific combat or non-combat role. Aeronautic systems includes, but is not limited to, fixed and rotary wing aircraft and design, UAV, and airframes.

Key Findings from FY18 Cleared Industry Reporting

- *Aeronautic systems was the second most targeted technology category in FY18*
- *Reported targeting of aeronautic systems decreased by 15 percent from FY17*
- *East Asia and the Pacific region was the origin of most reported targeting of aeronautic systems*
- *Attempted acquisition of technology was the most common MO and email was the most common MC used to contact industry in attempts to target aeronautic systems*



Overview

For each of the past 6 years, aeronautic systems has been one of the top three targeted technologies based on cleared industry reporting of suspicious contacts by foreign entities. Unmanned aerial vehicles and drones, notably counter-drone/ anti-drone products, were the most targeted aeronautic systems technologies in FY18.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in over a third of the incidents involving aeronautic systems. Reported incidents of targeting of aeronautic systems by entities from the East Asia and the Pacific region decreased by 8 percent in FY18 compared to FY17. Entities from this region targeted UAV and drone tech-nologies commonly seeking UAV transponder or counter-UAV technologies.

Europe and Eurasia entities were the second most active collectors targeting aeronautic systems. Entities from this region also targeted UAVs and drones, as well as fixed wing aircraft technologies. Entities from the Near East and Western Hemisphere regions were equally active collectors of aeronautic systems technologies in FY18.

Cleared industry identified commercial entities in over half of the incidents involving aeronautic systems. Commercial was the most common affiliation targeting aeronautic systems from all six of the geographic regions.

In FY18, entities targeting aeronautic systems used the attempted acquisition of technology and the RFI/solicitation MO each in 32 percent of the reported incidents. Email was the most common MC, used in 58 percent of the incidents.

Takeaway

The United States is a leader in this technology field and will remain a target as other countries plan to develop peer capabilities. In addition, aeronautic systems tech-nology is vital in developing force projection, reconnaissance and surveillance, and air dominance capabilities.

Foreign Collection Methodology Targeting Aeronautic Systems

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting aeronautic systems in FY18.

Reported foreign targeting of command, control, communication, and computers

C4 is the backbone of almost all government functions -from battlefield commanders to interagency communications. Monitors, computers, printers, phones, radios, and data links are all necessary in this network centric environment. C4 includes, but is not limited

The most commonly reported approach vector associated with aeronautic systems in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 134 times in FY18. The next most commonly reported approach was **RFI/ solicitation** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Contact

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	31	5	272	41	1	48	2	20	1	18	4	22
Attempted Acquisition	150	L		H								L	M
Exploitation of Business Activity	63	M		M	H		L				L		L
Exploitation of Cyber Operations	9		L					L			L		L
Exploitation of Experts	15			L	L						L		
Exploitation of Insider Access	16			L	L		M						
Exploitation of Relationship	20			L	L		L		L		L		
Exploitation of Security Protocol	11			L			L					L	
Exploitation of Supply Chain	2			L		L							
Résumé Submission	24			L	L				M	L			
RFI/Solicitation	147	M		H	L		L				L	L	L
Search & Seizure	2						L						
Surveillance	5	L					L						
Theft	1						L						

Top Targeted Aeronautic Systems Subcomponents

UAVs & Drones
- Counter-drone/Anti-drone Products

Fixed Wing Aircraft

Airframes & Structural Components

Flight Simulator Software & Training

Rotary Wing Aircraft

Other Fixed Wing Aircraft (Cargo & Transport)

Avionics

Targeting Aeronautic Systems Case Study

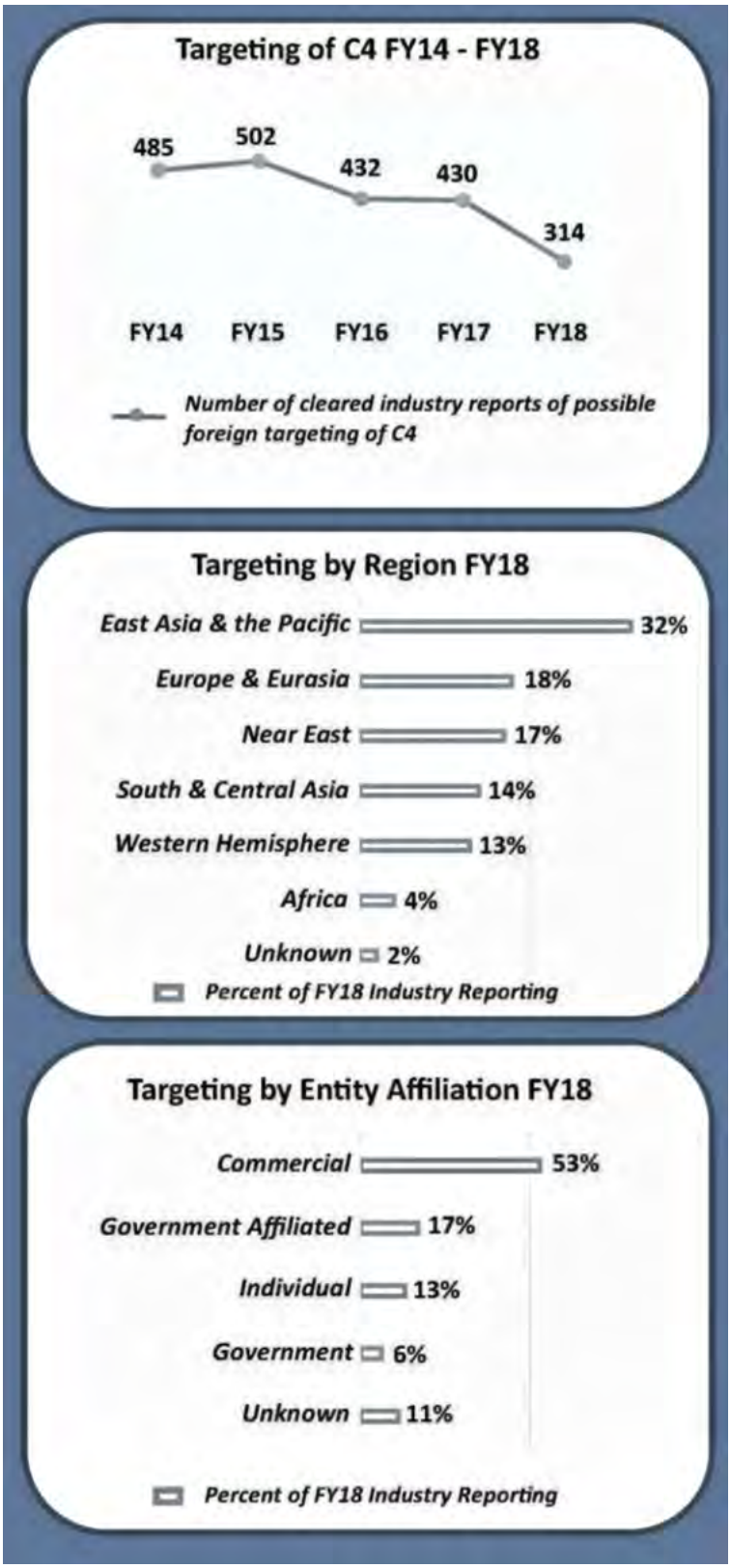
In March 2019, the U.S. District Court for the District of Columbia sentenced an Australian national for shipping aircraft parts to an Iranian company in violation of U.S. Embargo

- Australia extradited the defendant to the United States in 2018
- The defendant solicited purchase orders and business for the goods from a trading company in Iran
- The Iranian trading company also operated companies in Malaysia that acted as intermediaries
- The defendant placed orders for aircraft parts and other items that the Iranian company could not buy directly
- To further conceal the end user, when necessary the defendant used a U.S.-based broker to order the parts

Takeaway: Foreign corporations and governments use brokers in the United States or in countries with favorable trade status to disguise the actual end user and end use of export controlled technologies.

Source: U.S. Department of Justice, Office of Public Affairs, https://www.justice.gov/opa/pr/australian-national-sentenced-prison-term-exporting-electronics-iran

to, computers and central processing units (CPU), common data links, telecommunication devices, and antenna.



Key Findings from FY18 Cleared Industry Reporting

- *Each year since FY13, C4 has been one of the top three targeted technology categories*
- *Reported foreign targeting of C4 technologies decreased by 27 percent in FY18 when compared to FY17*
- *Entities from East Asia and the Pacific region were the most active collectors of C4 technologies identified in cleared industry reporting in FY18*
- *These collectors contacted cleared industry via email in 63 percent of reported incidents*

Overview

With the decrease of 27 percent in targeting in FY18, C4 dropped from the second to the third most commonly targeted technology as identified in cleared industry reporting. Industry reported fewer attempts to target highly sought after C4 components such as antennas, telecommunication devices, computers and CPUs, and common data links. Conversely, reporting identified an increase of incidents relating to wide area surveillance systems and wireless networks and technologies.

In FY18, cleared industry reporting identified entities from East Asia and the Pacific region in 32 percent of the incidents involving C4. Reported incidents of targeting of C4 by entities from the East Asia and the Pacific region increased by 1 percent in FY18 compared to FY17. Entities from this region targeted C4 components such as antennas, wireless networks and technologies, and wide area surveillance systems. In FY17, this region was the second most active region after the Near East region.

Europe and Eurasia entities were the second most active collectors targeting C4 in FY18. Entities from this region targeted telecommunication devices, wide area networks and technologies, computers, and CPUs.

In FY18, commercial entities were identified in over half of the reported incidents of targeting of C4 technologies. This was the most common affiliation targeting C4 from all geographic regions except the Western Hemisphere, in which individual was the most common collector affiliation.

In FY18, entities targeting C4 most frequently used the attempted acquisition of technology MO and email was the most frequently used MC.

Takeaway

C4 technologies are highly sought after by foreign collectors. Beyond targeting industry for sensitive technologies, foreign entities also attempt to provide counterfeit computer parts to U.S.

companies that could subsequently enter DoD supply chains. Counterfeit parts could fail due to substandard quality or by design; either could negatively impact the warfighter.

Foreign collection methodology targeting C4

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting C4 in FY18.

The most commonly reported approach vector associated to C4 technologies in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 118 times in FY18. The next most commonly reported approach was **RFI/solicitation** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Contact

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	13	4	198	7	0	39	1	21	11	4	2	14
Attempted Acquisition	131	L		H			L					L	L
Exploitation of Business Activity	17	L		L	L		L						
Exploitation of Cyber Operations	5		L					L					
Exploitation of Experts	10			L			L				L		
Exploitation of Insider Access	13				L		M						
Exploitation of Relationship	12	L		L			L				L		
Exploitation of Security Protocol	6				L		L						
Exploitation of Supply Chain	3			L									
Résumé Submission	32								M	M			
RFI/Solicitation	82	L		H			L				L		L
Search & Seizure	1						L						
Surveillance	2	L											
Theft	0												

Top Targeted C4 Subcomponents

- Antenna
- Wide Area Surveillance System
- Computers & CPUs
- Air & Missile Defense C2
- Telecommunication Devices
- Wireless Networks & Technologies
- Common Data Links
- Waveguide Components

Targeting C4 Case Study

In early 2019, the U.S. District Court for the Southern District of Texas sentenced a Chinese national for selling counterfeit computer parts

- From at least 2007 until late 2017, the Chinese national directed shipments of counterfeit computer-networking equipment to a retailer in Texas
- He sold counterfeit networking products through several business entities and used corporate and personal aliases to evade detection
- He and his customers agreed to mislabel packages, break up shipments into separate components, alter destination addresses, and use multiple forwarding companies based in the United States

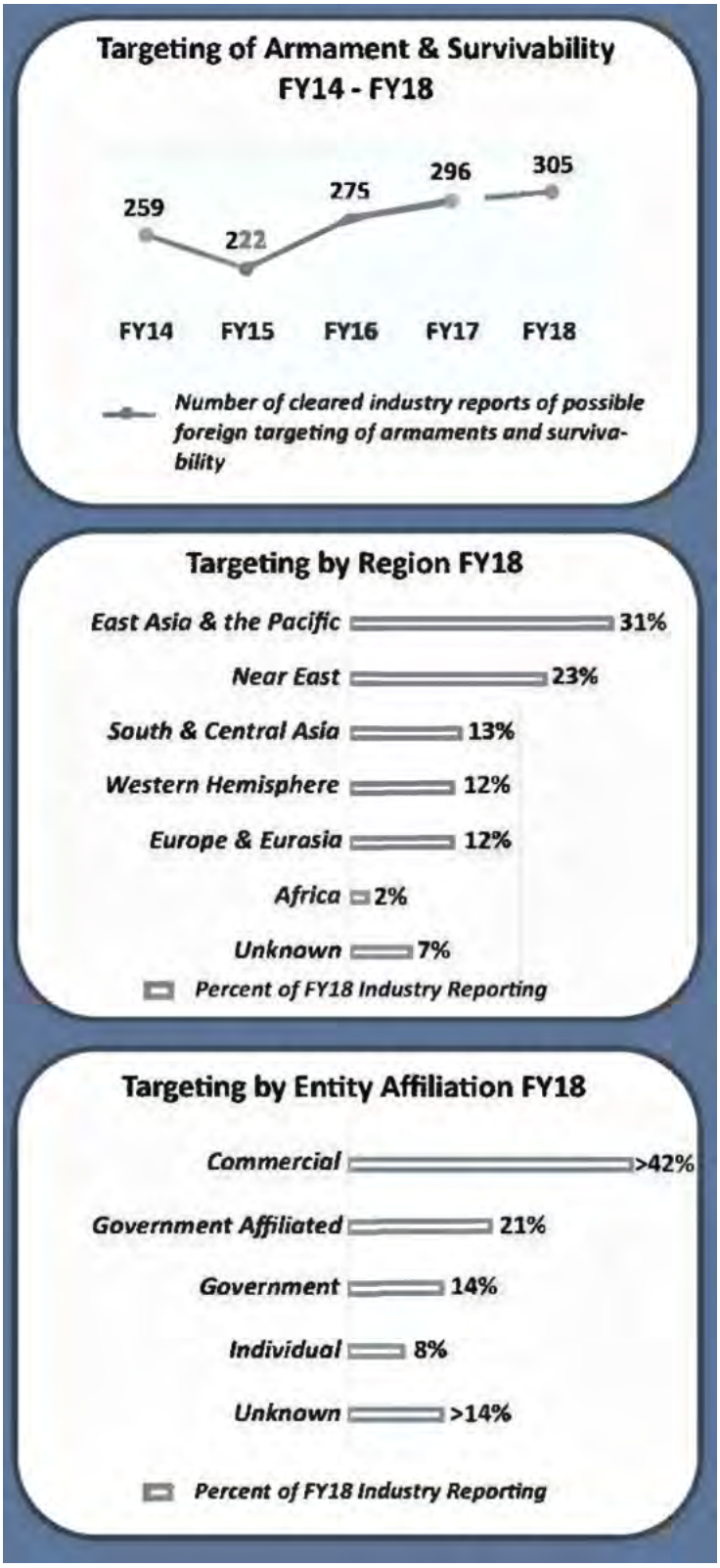
Takeaway: Counterfeit parts are often substandard and may fail under stress. In addition, computer parts could include malicious coding that may allow foreign adversaries the ability to collect DoD data or cause systems to fail.

Source: U.S. Department of Justice, Office of Public Affairs, Press Release 19-130, https://www.justice.gov/opa/pr/Chinese-national-sentenced-prison-selling-counterfeit-computer-parts

Reported foreign targeting of armament and survivability

Armament and survivability

Armaments are the conventional munitions technologies designed to increase the lethality of ground, aeronautic, marine, and space systems. Conversely, survivability technologies provide various levels of protection for ground, aeronautic, marine, and space systems from armaments. Armament and survivability includes, but is not limited to, missiles, rockets, automatic and semi-automatic weapons, electromagnetic rail guns, artillery and mortar rounds, and body armor.



Key Findings from FY18 Cleared Industry Reporting

- *Armament and survivability was the fourth most targetedtechnology category in FY1*
- *Reported targeting of armaments and survivabilitytechnology increased by 3 percent from FY1*
- *East Asia and the Pacific region was the origin of mostreported targeting of armament and survivability*
- *RFI/solicitation was the most common MO and email was themost common MC used to contact industry in attempts totarget armaments and survivability technologies*

Overview

Every year since FY12, except for FY15, the number of incidents of targeting armaments and survivability has increased. FY18 is only the second year that armament and survivability has been one of the top five targeted technologies as rep orted by cleared industry. The most targeted technologies in this category included missiles, automatic and semi-aut omatic weapons, and electronic warfare.

Cleared industry reporting in FY18 identified entities from East Asia and the Pacific region in 31 percent of the incidents. The volume of reporting of East Asia and the Pacific entities targeting this technology increased by 8 percent in FY18. Entities from this region targeted missiles, automatic and semiautomatic weapons, and electronic warfare.

Entities from the Near East were the next most active and were identified in 23 percent of the reporting. Entities from this region most often targeted missiles, automatic and semiautomatic weapons, and missile warning systems.

Commercial entities were involved in over 42 percent of the incidents targeting this technology. In 55 percent of the incidents associated with commercial entities they used RFI/ solicitation as the MO.

In FY18, 41 percent of suspicious contacts listed RFI/solicitation as the MO, the second most common MO was attempted acquisition of technology noted in 17 percent of reports. Email was noted as the MC in 39 percent of the incidents targeting this technology, followed by conferences, conventions, and trade shows, reported in 23 percent of the reports.

Takeaway

The United States is a leader in developing and applying armament and survivability technologies, which include weapon systems and protective tec hnologies. Foreign adversaries that obtain sensitive information relating to these technologies can benefit from replicating U.S. capabilities and developing countermeasures to U.S. systems.

Foreign Collection Methodolgy Targeting Armament and Survivability

Foreign entities use appro-ach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting armament and survivability in FY18.

The most commonly reported approach vector associated with armament and survivability technologies in FY18 was **RFI/solicitation** using an **email** to contact the target. Cleared industry reported this approach vector 68 times in FY18. The next most commonly reported approach was **attempted acquisition** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
	Volume of Reporting by Methods of Contact	69	7	120	14	2	30	1	34	0	7	0	20
Attempted Acquisition	53	L		H									L
Exploitation of Business Activity	43	M		L	L		L						
Exploitation of Cyber Operations	8		L					L					
Exploitation of Experts	6			L							L		
Exploitation of Insider Access	9				L		L						
Exploitation of Relationship	7				L		L						
Exploitation of Security Protocol	5	L				L	L						
Exploitation of Supply Chain	2			L		L							
Résumé Submission	34								H				
RFI/Solicitation	124	H		H	L		L				L		M
Search & Seizure	1						L						
Surveillance	11	L					L						
Theft	2						L						

Top Targeted Armament & Survivability Subcomponents

Missiles
- Terminal High Altitude Area Defense (THAAD)

X-Ray Detection

Launchers (Missile, Torpedo, Rocket, etc.)

Automatic & Semi-Automatic Weapons

Electronic Warfare

Mine/Explosive Detection

Gun Rounds (anti-Armor, Armor Piercing, etc.)

Targeting Armament & Survivability Case Study

In December 2017, an Italian National pled guilty to exporting and attempting to export military technology

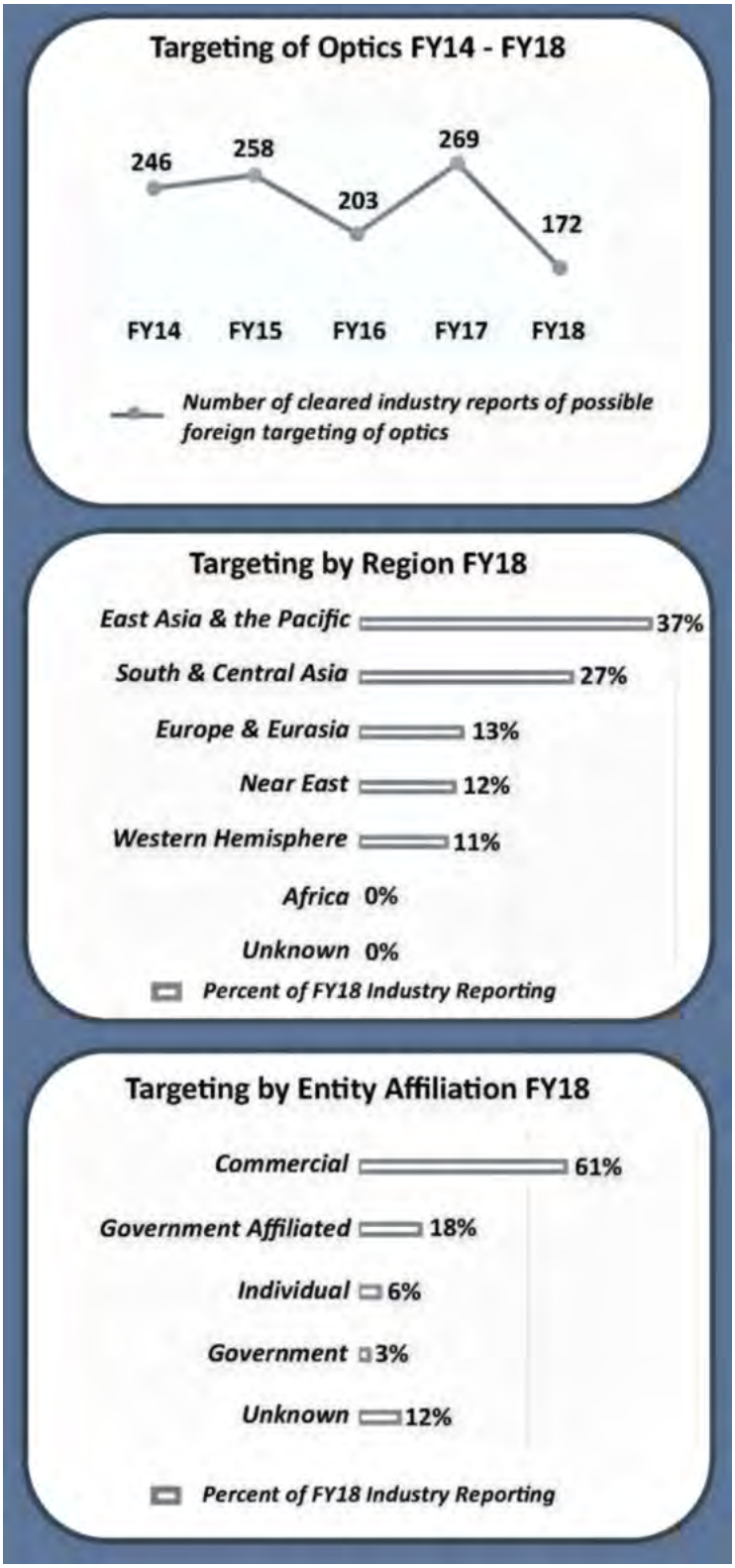
- According to court filings, between June 2013 and May 2017, the defendant illegally exported and attempted to export night vision goggles and assault rifle components
- Defendant purchased export control devices from U.S.-based manufacturers and distributers via internet-based marketplaces
- Defendant directed sellers to ship products to freight forwarders in the United States
- Defendant made false statements to the freight forwarders about the contents in order to export the packages to Italy without required licenses

Takeaway: Shipping to freight companies can be used to obfuscate the actual location and identity of the end user.

Source: U.S. Department of Justice, U.S. Attorney's Office, Eastern District of New York, https://www.justice.gov/usao-edny/pr/italian-national-sentenced-11-months-prison-illegally-exporting-and-attempting-export

Reported Foreign Targeting of Optics

Optics is the study of the behavior of light and its interactions with matter and the development of equipment to detect light. Although other portions of the electromagnetic spectrum exhibit similar properties of light, the optics category refers to the study and detection of light in the visible, ultraviolet, and infrared portions of the electromagnetic spectrum. Optics includes, but is not limited to, cameras, fiber optics, lenses, mirrors, night vision, polarization, reflective coatings, and refractive coatings.



Key Findings from FY18 Cleared Industry Reporting

- *FIE targeting of optics technologies decreased in FY18; however, it was the fifth most targeted technology*
- *The majority of foreign collectors targeting optics were commercial entities*
- *Attempts to purchase optics related technology was the most common approach, often via email*

Overview

FY18 was the first year that optics was one of the five top targeted technologies since FY12 when it was a component of the laser, optics, and sensor category, despite experiencing a 36 percent decrease in reported targeting from FY17. The most targeted optics technologies were night vision, cameras, mirrors, and lenses.

East Asia and the Pacific region was the origin for 37 percent of the incidents reported by cleared industry relating to optics. The volume of targeting from this region decreased by 41 percent from FY17. Entities from East Asia and the Pacific targeted cameras and mirrors more than any other optic technology.

South and Central Asia entities were the next most prolific collectors of optics technology in FY18. Noted in over a quarter of the reports relating to optics, entities from South and Central Asia targeted night vision technology more than any other optic technology.

Commercial entities were by far the most common collectors identified in cleared industry reporting of targeting optics. These entities applied the attempted acquisition of technology and RFI/solicitation MO in nearly 90 percent of the incidents.

In FY18, the MOs attempted acquisition of technology and RFI/solicitation were the most used by FIE targeting optics. One of these MOs was identified in 81 percent of the incidents reported in FY18. Exploitation of business activity was the third most reported MO, accounting for just 6 percent of the incidents. By far, email was the most common MC used targeting optics. Cleared industry reporting listed email as the MC in 71 percent of the incidents.

Takeaway

Optics remains a highly sought after technology, even with the reduction of reported FIE targeting in FY18. High quality night vision provides an advantage to U.S. warfighters. FIE will continue to target U.S. optics technology for military and commercial uses. Once obtained, foreign entities can apply the technology and further proliferate it to other countries for commercial gain.

Foreign Collection Methodolgy Targeting of Optics

Foreign entities use approach vectors that include an MO paired with an MC. The matrix below depicts the volume of reported incidents of targeting optics in FY18.

The most commonly reported approach vector associated to optics in FY18 was **attempted acquisition** using an **email** to contact the target. Cleared industry reported this approach vector 70 times in FY18. The next most commonly reported approach was **RFI/solicitation** via **email.**

Volume of Reporting of Approach Vectors

H HIGH volume | M MEDIUM volume | L LOW volume | No Reporting

Methods of Operation	Volume of Reporting by Methods of Operation	Conferences, Conventions, & Trade Shows	Cyber Operations	Email	Foreign Visit	Mail	Personal Contact	Phishing Operations	Résumé—Academic	Résumé—Professional	Social Networking Services	Telephone	Web Form Submission
Methods of Contact		9	0	122	2	0	8	1	9	1	6	0	14
		Volume of Reporting by Methods of Contact											
Attempted Acquisition	75			H				L					L
Exploitation of Business Activity	11	L		L	L		L						
Exploitation of Cyber Operations	0												
Exploitation of Experts	6			L			L				L		
Exploitation of Insider Access	5				L		L						
Exploitation of Relationship	2						L				L		
Exploitation of Security Protocol	1						L						
Exploitation of Supply Chain	0												
Résumé Submission	9								L	L			
RFI/Solicitation	63	L		H					L		L		L
Search & Seizure	0												
Surveillance	0												
Theft	0												

Top Targeted Optics Subcomponents

Night Vision
- Panoramic Night Vision Goggles

Cameras

Mirrors

Lenses

Reflective Coatings

Holograms & Holographic Technology

Wave-optics Modeling & Analysis

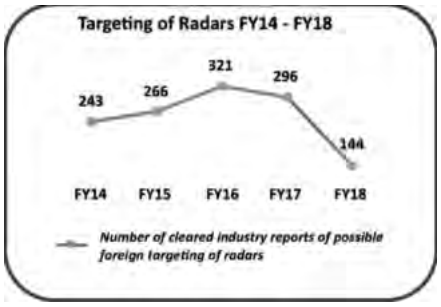
Targeting Optics Case Study

In August 2018, the District Court of Seattle sentenced a Canadian national for conspiracy to export restricted goods and technology to Iran

- Defendant and co-conspirators illegally exported and attempted to export dual-use technologies to Iran
- Specific items included two types of thermal imaging cameras; other items included inertial guidance systems testing equipment
- The thermal imaging cameras can be used in commercial security systems and on UAVs and military drones
- Conspirators falsified shipping documents and deceived manufacturers by claiming goods were being shipped to Turkey and Portugal, while knowing the true destination was Iran

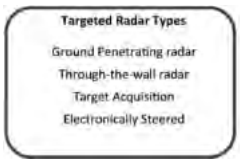
Takeaway: Claiming equipment is bound for a country with positive trade relations is a common method to obtain export controlled technologies for entities in countries under export restrictions. *Source: U.S. Department of Justice, U.S. Attorney's Office, Western District of Washington, https://www.justice.gov/usao-wdwa/pr/canadian-sentenced-3-years-prison-conspiracy-export-restricted-goods-and-technology*

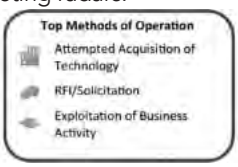
Foreign Targeting of Other Technologies

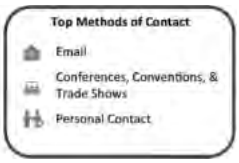


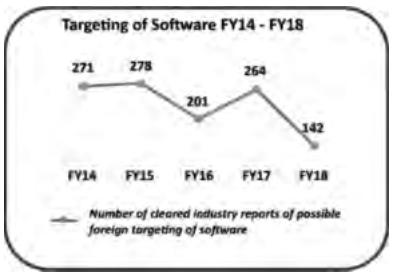
Radars

In FY18, 2 percent of the reports from cleared industry identi-fied radars as the targeted technology. The reported targeting of radars has decreased over the past 2 years, dropping by 51 percent from FY17. The most frequently targeted radars in FY18 have ground forces applications with ground penetrating radar and through-the-wall radar accounting for 24 percent of targeted radar systems. Radars commonly associated with anti-access area denial (A2/AD) such as target acquisition, air defense, and early warning were noted in fewer incidents. In FY18, entities from the East Asia and the Pacific region were the most active collectors targeting radar. They accounted for 39 percent of the incidents, followed by the Near East and South and Central Asia regions. Commercial entities were noted in 49 percent of the incidents targeting radars.





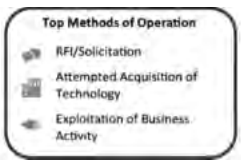


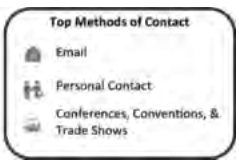


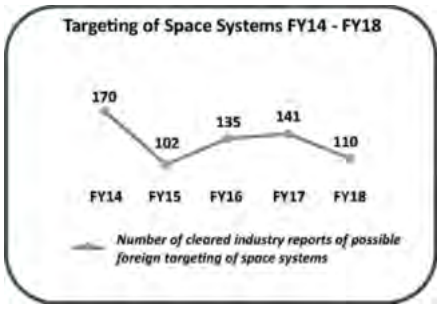
Software

Reporting from cleared industry of incidents relating to software accounted for 2 percent of all reports in FY18. The reports relating to targeting of software dropped by 46 percent in FY18. Cleared industry identified modeling and simulation software in 28 percent of the reporting. The next most reported software was artificial intelligence software, noted in 11 percent of the reporting. All other types of software were noted in less than 10 percent of the reports related to this category.

Not surprisingly, East Asia and the Pacific region entities were the most active collectors targeting software, accounting for 35 percent of the reporting in FY18. Europe and Eurasia entities were the second most active, identified in 25 percent of the reports. Commercial was the most active entity affiliation identified in 43 percent of the reports relating to software.



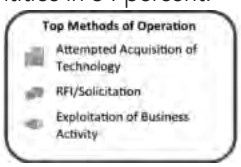


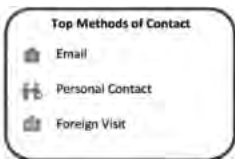


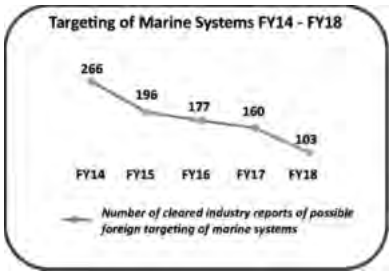
Space Systems

Cleared industry reporting of suspicious contacts identified space systems as the targeted technology in 2 percent of the reports in FY18. The volume of reporting related to space systems decreased by 22 percent from FY17. In FY18, one-third of the reports of targeting space systems involved satellite buses. A satellite bus is a general satellite model on which multiple satellites can be produced with different payloads.

DCSA identified East Asia and the Pacific region entities in 31 percent of the reporting associated with targeting of space systems. Entities from Europe and Eurasia were identified in 24 percent of the reporting in FY18, and entities from the number of cleared industry reports of possible foreign targeting of space systems Western Hemisphere were identified in 20 percent. Cleared industry reported commercial entities in 35 percent of the reporting and government affiliated entities in 34 percent.



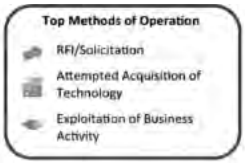


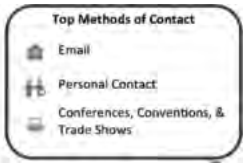


Marine Systems

Since FY13, the targeting of marine systems has decreased each year. In FY18, marine systems were identified in under 2 percent of cleared industry reporting. The volume of incidents targeting marine systems dropped 36 percent from FY17. Of specific marine systems technologies, reports of targeting of combat ships and landing vessels decreased by 63 percent, and that of submarines and designs fell by 25 percent.

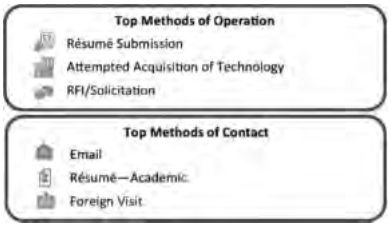
According to FY18 reporting, entities from East Asia and the Pacific region were involved in 48 percent of the incidents and Western Hemisphere entities were the second most active, noted in 17 percent of the reports. Commercial and government affiliated were the two most active entities targeting marine systems in FY18, accounting for 39 and 23 percent of the reporting, respectively.





Energy Systems

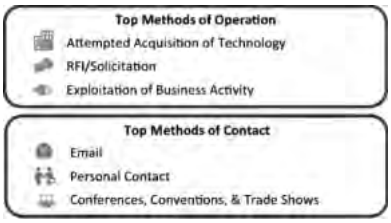
Energy systems was the tenth most targeted technology as rreported by cleared industry in FY18. These technologies were targeted in just under 2 percent of cleared industry reporting. The East Asia and the Pacific region was the origin of over half of the reported attempts to collect on energy systems.



Targeted Energy Systems	
Gas Turbine Engines	Batteries
Propellants	Rocket Engines
Turbo Fan Engines	Ocean Power Technologies
Energy Systems Components	Generators

Positioning, Navigation and Time

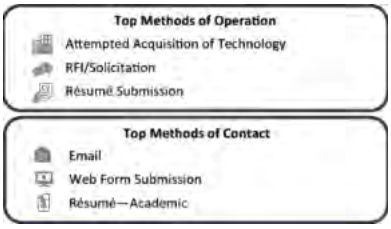
Positioning, navigation, and time (PNT) accounted for the targeted technology in just over 1 percent of reporting in FY18. DCSA identified entities from East Asia and the Pacific region in 39 percent of the reports of targeting of PNT.



Targeted Positioning, Navigation, and Time	
Inertial Measuring Units	Gyroscopes
Global Positioning System (GPS)	Accelerometers
Navigational Aids	GPS Alternative Systems
Radio Frequency & other Beacon-Based Navigation Technology	

Sensor (Acoustic)

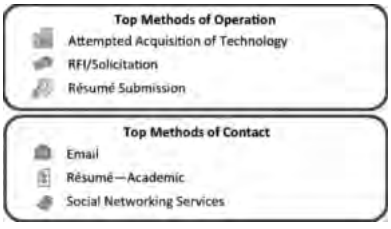
Reported targeting of sensors (acoustic) technology increased by 122 percent in FY18 over FY17. Entities from East Asia and the Pacific accounted for 63 percent of reporting relating to sensors.



Targeted Sensor (Acoustic)	
Acoustic Sensor Products	Active Sonar
Sonobouys	Seismic Ground
Acoustic, Sensors, and Displays	

Materials: Raw and Processed

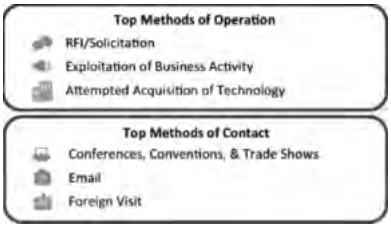
In FY18 reporting, the number of incidents of targeting of materials: raw and processed, dropped by 40 percent from FY17. Entities from East Asia and the Pacific accounted for 58 percent of the reports.



Targeted Materials: Raw and Processed	
Fiber-based Materials	Alloys
Plastic—Unique or Advanced	Structural Foam
Chemicals	

Ground Systems

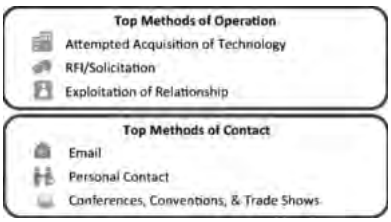
Reported targeting of ground systems was up 7 percent from FY17. Entities from the Near East were the most active collectors identified in 28 percent of the SCRs.



Targeted Ground Systems
Light Armored Vehicles & Designs
Medium Tactical Vehicles & Designs
Unmanned Ground Systems
Cargo Systems
Transport Vehicles & Designs
M1 Abrams Variations of Heavy Tanks & Designs

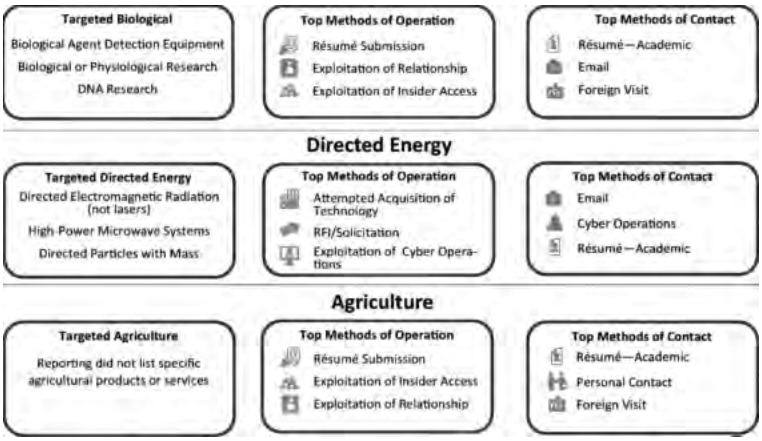
Lasers

In FY18 the reported targeting of lasers decreased 27 percent from FY17. East Asia and the Pacific region entities were identified in 47 percent of the reports of targeting technologies and information relating to lasers.



Targeted Lasers	
Solid State Lasers	Gas Lasers
High Energy Laser Weapons	Fiber Lasers

Biological



Part Two of the DCSA's "Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry" will be presented in the May issue of MilsatMagazine.

www.dcsa.mil

SATELLITE INNOVATION

2020 SILICON VALLEY

THE MEETING PLACE FOR SATELLITE EXECUTIVES AND PROFESSIONALS

75+
EXHIBITORS / SPONSORS

125+
SPEAKERS

800+
ATTENDEES

SATINNOVATION.COM

The ***Satellite Innovation*** Conference has become the premier meeting place for innovative Satellite Executives and Professionals. Subject-matter experts focus on imminent changes and the market forces that will propel their implementation. Meet the market leaders and pioneers of the shifting landscape of our industry.

October 6th - 8th, 2020