SATCOM for Net-Centric Warfare

MilsatMagazine

FEBRUARY 2019

MILSATCOM, SmallSats and More...

A Defense Intelligence Agency (DIA) Analysis & Report

2019 National Intelligence Strategy (NIS)

A Shift in Military Satellite Strategies

Thermal Management in High Performance RF and Microwave PCBs

AI for Africa: Opportunities for Government

Dispatches

FEATURES

ADVERTISER INDEX

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

Advantech
Satellite Networks

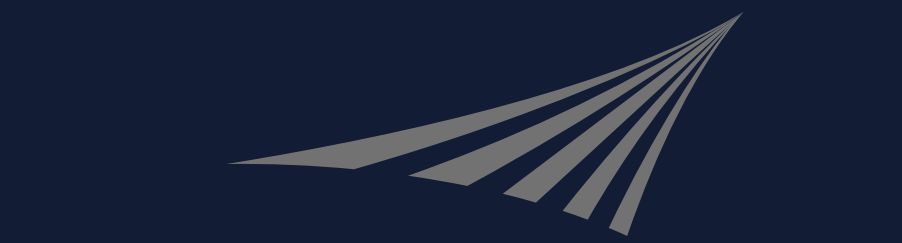
New name, New adventure.

Advantech Satellite Networks, formerly Advantech Wireless Inc., is now

SPACEBRIDGE

We thank all our partners, clients and suppliers for helping us significantly grow our business and we remain committed to the same degree of excellence, spirit of innovation and customer delight. Above all, we commit to reward our customers with unsurpassed technologies and solutions developed by our talented and loyal team that has earned your trust over the past 30 years.

A new journey has begun.



SPACEBRIDGE (Advantech Wireless Inc., doing business as Advantech Satellite Networks)
Tel.: +1.514.420.0045 • Fax: +1.514.420.0073 • spacebridge.com • info@spacebridge.com

DISPATCHES

Comtech Telecommunications' latest satellite modem board ordered by defense contractor

Comtech Telecommunication's DMD-1050TS L-Band Satellite Modem Board.

Comtech Telecommunications Corp. (Nasdaq: CMTL) has revealed that, during the firm's second quarter of fiscal 2019, the company's Tempe, Arizona-based subsidiary, Comtech EF Data Corp., which is part of Comtech's Commercial Solutions segment, received a $1.0 million equipment order from a defense contractor — the equipment will be deployed to support a United States Air Force (USAF) program.

The order specified the ***DMD1050TS L-Band Satellite Modem Board***.

The DMD1050TS is Comtech EF Data's latest generation modem board set targeted at critical government and military applications.

The product complies with the widest possible range of U.S. Government (USG) and commercial standards and is compatible with the largest number of satellite modems in the industry.

This modem board is fully compliant with MIL-STD-188-165A, STANAG 4486 Edition 3 (EBEM), and the IESS–315 commercial standards at data rates up to 37 Mbps.

Additionally, the DMD1050TS has successfully completed Phase I of Army Forces Strategic Command (ARSTRAT) WGS certification and is scheduled for final Joint SATCOM Engineering Center (JSEC) evaluation.

The DMD1050TS L-Band Satellite Modem board offers a complete modem with FIPS certified TRANSEC on a compact PCB daughter board.

The embedded TRANSEC capability is fully compatible with the TRANSEC capabilities in Comtech EF Data's DMD2050E and SLM-5650A Satellite Modems.

The extensive list of integrated hardware and software options allows the user to integrate the modem on many platforms and provide an upgrade path for future networks.

Options may be purchased with the product or easily upgraded in the field through the web browser or terminal port.

Download the product's PDF data sheet at this direct link: ***www.comtechefdata.com/files/ds-DMD1050TS.pdf***

DISPATCHES

Mercury Systems ships prototype solid state drive that tolerates high radiation for satellites and high altitude aircraft

Mercury Systems has announced the first prototype shipments of the company's 3U TRRUST-Stor VPX RT space-qualified secure solid-state drives (SSD) to two leading suppliers of LEO satellites.

Mercury Systems' TRRUST-Stor VPX RT space-qualified secure solid-state drive is the first commercial SSD to leverage VITA 78 SpaceVPX standards. Photo is courtesy of the company.

Designed to operate reliably in high radiation environments, this device is the first commercial SSD leveraging VITA 78 SpaceVPX standards to reduce customer cost and mitigate program risk. In addition to commercial satellite applications, this device is ideally suited for high-altitude aircraft, airborne weapons and mission-critical ground computing systems.

At the heart of the SSD is Mercury's proprietary NAND controller with BuiltSECURE error correcting code (ECC) algorithms. These ECC algorithms mitigate radiation-induced byte errors, thereby enabling sustainable reliability and fault tolerance that are not available with competing storage solutions. As Mercury maintains 10 percent authority over the controller and its implementation, this device is readily customizable for non-traditional use cases when deemed critical to a customer's program.

Honored with a Platinum award in the category of Trusted Computing in the 2018 Military & Aerospace Electronics Innovators Awards program, Mercury's TRRUST-Stor VPX RT device provides long-term data integrity.

Engineered into an open standards platform, customers can seamlessly integrate this device into the SpaceVPX ecosystem of processing boards and chassis without sacrificing affordability. As the need for radiation-tolerant devices for LEO satellites proliferates, system development around the SpaceVPX open standard architecture will be integral in supporting the growth of the space market.

Flight units are scheduled to ship in the first half of calendar year 2019.

www.mrcy.com

ENABLING COMMUNICATIONS IN ANY SITUATION

AvL'S FAMILY OF INTEGRATED TERMINALS (FIT)

- Ultra lightweight - meets IATA requirements for carry-on or checked baggage
- One person set-up in less than 10 minutes
- Carbon fiber reflectors - sizes range from 45cm to 1.35M
- All-in-one positioner system & switchable manual or motorized operation
- Quick change tri-band feed and RF kits
- AvL AAQ computer-assisted pointing and acquisition
- Beacon receiver, ODU/modem integration and BUC/LNB integration
- Watch the video at avltech.com/media

DISPATCHES

Evolution of global military comms studied in Market and Technology's just-published forecast

The nation's military communications efforts have shifted toward better situational awareness, which was previously skewed toward asset capability — the combination of inputs from various forces helps headquarters make tactical decisions based on data driven inputs.

Military communication also focuses on ear marking friendlies apart from marking enemy positions.

The IFF (*Identification, Friend or Foe*) systems help in ID'ing the friendlies, thereby reducing friendly fire situations.

The communications have evolved from runners to SATCOM which has eased the transfer of information to a faster and more reliable form.

However, supporting this communication infrastructure for defense applications was becoming a costly challenge.

Currently, defense departments across major countries are in the process of increasing the COTS (*Commercial-Off-The-Shelf*) adoption for defense applications.

The estimate is that more than 70 percent of the defense communication was through commercial bandwidth.

The commercial satellite companies are also ensuring that commercial satellites meet military standards to cater to the needs of defense.

The military communications market is expected to grow at a CAGR of around 4 percent during the forecast period and reach approximately $41 billion by 2027.

The key drivers for the market include the soldier modernization program, need for increased situational awareness and the NATO driven program upgrades.

The key challenge is the lack of direct benefit to better military communication systems, unlike tangible military assets that can be exhibited with specific requirements.

The average spending on military communications was around 1 to 2 percent of total military budgets during the 2012-2017 period.

The military communications market is poised to grow during the next few years; however, there are certain market segments that are expected to experience decrease in spending.

The market intelligence report ***Global Military Communications – Market and Technology Forecast to 2027*** covers the key technologies, current market overview, a market analysis, and a forecast to 2027.

The market analysis chapter covers the key market dynamics that are expected to shape the market during the forecast period, the PEST analysis and the Porter's five forces (Porter's five forces model is an analysis tool that uses five industry forces to determine the intensity of competition in an industry and its profitability level).

The country analysis chapter covers around 21 country level programs which is further segmented, based on the three forces.

The country analysis also covers the future trends based on historical spending.

The market forecast chapter covers three main segments which are — Region wise, Equipment wise and Sub-System wise — which are then further sub-segmented.

The report features more than 143 tables and more than 200 figures.

The Market Forecast infosite may be accessed via this direct link:
www.marketforecast.com/

The advantages of

Advantech Wireless **Technologies** *are clear*

- Deployments in over 150 countries
- New state-of-the-art research and manufacturing facility
- Broadest SATCOM RF product portfolio in the industry
- Part of the Baylin Technologies Group of Companies

ADVANTECH
Wireless Technologies

Solid State Power Amplifiers | **Satellite Frequency Converters** | **Satellite Antennas** | **Radar GaN Amplifiers** | **Terrestrial Microwave Radios**

advantechwireless.com

DISPATCHES

Smallsat constellation bus for DARPA to be developed by Airbus Defense and Space

DARPA has awarded a contract, called the *Blackjack* program to Airbus Defense and Space — the company will develop a satellite bus to support this program.

Defense Advanced Research Projects Agency (DARPA) describes the Blackjack program as an architecture demonstration intending to show the military utility of global LEO constellations and mesh networks of lower size, weight and cost.

DARPA's intentions are to purchase commercial satellite buses and pair them with military sensors and payloads.

The bus drives each satellite by generating power, controlling attitude, providing propulsion, transmitting spacecraft telemetry, and providing general payload accommodation including mounting locations for the military sensors.

Tim Deaver, Director of U.S. Space Programs at **Airbus Defense and Space, Inc**. said that Airbus has previously co-invested hundreds of millions of dollars in high-rate manufacturing technology and supply chain logistics to build large constellations of small satellites.

He added that Airbus is committed to growing manufacturing capability in the U.S. and their government customers can leverage this commercial capability to develop LEO constellations to complement large, existing systems.

This contract positions Airbus Defense and Space, Inc., of Herndon, Virginia, and its strategic joint venture partner, **OneWeb Satellites**, of Exploration Park, Florida, as the ideal service providers for Blackjack.

High production rates and design-to-cost management techniques enable OneWeb Satellites to offer low cost constellation solutions for the U.S. government and current customers.

Constellations of inexpensive satellites permit wide scale disaggregated architectures enhancing survivability across many different mission areas.

OneWeb Satellites is designing and manufacturing ultra-high performing satellites at high-volumes.

Tony Gingiss, CEO, OneWeb Satellites, said that the company has created a game changer with their overall design, supply chain and production system. Their team is transforming the space industry and they are in the midst of demonstrating they can deliver on their promises.

According to Gingiss, OneWeb Satellites brings to bear capabilities which dramatically lower the cost and shorten acquisition timelines for customers thanks to a modular design and agile serial production of satellites.

The OneWeb Satellites satellite manufacturing facility in Florida is the latest step in Airbus' continued commitment to growth in U.S. manufacturing, job creation and investment.

This facility, which will ultimately support thousands of jobs and follows the opening of U.S. Manufacturing Facility for A320 aircraft in Mobile, Alabama, from which the company delivered their first aircraft in 2016. An A220 assembly line on the same site in Alabama broke ground in a ceremony on January 16, 2019.

With their network of U.S. suppliers, Airbus is the largest consumer of U.S. aerospace and defense goods in the world, and the company has invested $16.5 billion with U.S. companies in 2017, supporting a total of 275,000 American jobs, according to the firm.

www.darpa.mil

airbus.com

onewebsatellites.com

Artistic rendition is courtesy of OneWeb Satellites.

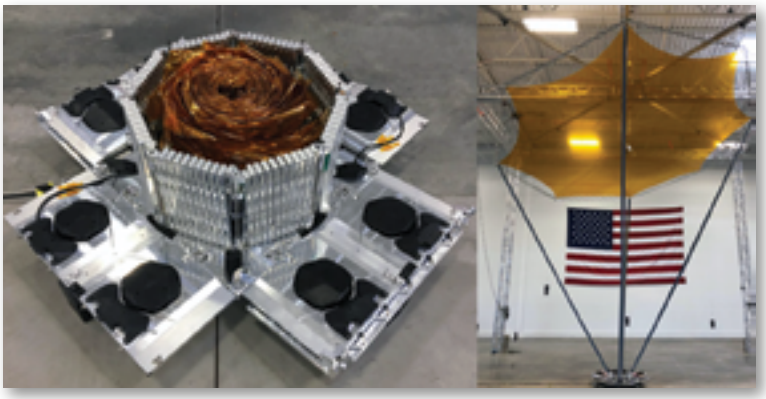
Additionally, DARPA's Radio Frequency Risk Reduction Deployment Demonstration (R3D2) is set for launch in late February to space-qualify a new type of membrane reflectarray antenna.

The antenna, made of a tissue-thin *Kapton* membrane, packs tightly for stowage during launch and then will deploy to its full size of 2.25 meters in diameter once it reaches LEO.

R3D2 will monitor antenna deployment dynamics, survivability and radio frequency (RF) characteristics of a membrane antenna in LEO. The antenna could enable multiple missions that currently require large satellites, to include high data rate communications to disadvantaged users on the ground.

A successful demonstration also will help prove out a smaller, faster-to-launch and lower cost capability, allowing the *Department of Defense* (DoD), as well as other users, to make the most of the new commercial market for small, inexpensive launch vehicles.

Satellite design, development, and launch took approximately 18 months.



MMA Design successfully completes deployment testing of its innovative high-compaction ratio reflectarray antenna in its Louisville, Colorado facilities.

"*The Department of Defense has prioritized rapid acquisition of small satellite and launch capabilities. By relying on commercial acquisition practices, DARPA streamlined the R3D2 mission from conception through launch services acquisition,*" said ***Fred Kennedy***, director of DARPA's Tactical Technology Office.

Kennedy added, "*This mission could help validate emerging concepts for a resilient sensor and data transport layer in low Earth orbit — a capability that does not exist today, but one which could revolutionize global communications by laying the groundwork for a space-based internet.*"

The launch will occur on a **Rocket Lab USA *Electron*** rocket from the company's launch complex on the Mahia Peninsula of New Zealand.

Northrop Grumman is the prime contractor and integrated the 150 kg. satellite; **MMA Design** designed and built the antenna. **Trident Systems** designed and built R3D2's software-defined radio, while **Blue Canyon Technologies** provided the spacecraft bus.

Rocket Lab will host a webcast and provide coverage of the launch via a live stream at this direct link:
www.rocketlabusa.com/live-stream

www.northropgrumman.com

mmadesignllc.com

www.tridsys.com

bluecanyontech.com

DISPATCHES

The Arrow 3 weapon system successfully tested by Israel's MDO and the U.S. MDA

The Israel Missile Defense Organization (IMDO) of the Directorate of the Defense Research and Development (DDR&D) at Israel's Ministry of Defense, together with the U.S. Missile Defense Agency (MDA), have successfully completed a test of the 'Arrow 3' Weapon System.

The Arrow-3 is a unique weapon system, designed to defend against ballistic missiles by targeting the threat outside of the atmosphere.

The test was conducted at a test site in central Israel and was led by Israel Aerospace Industries (IAI) in collaboration with the Israeli Air Force.

Once the target was launched, the Arrow Weapon System radars detected it and transferred the data to the Battle Management Control (BMC) which then established a defense plan.

At the correct moment, the Arrow-3 interceptor was launched toward the target and successfully completed the mission.

The Arrow Weapon System is a major part of Israel's multi-layered defense array.

This array is based on four layers: Iron Dome Defense System, David's Sling Weapon System, Arrow-2 and the Arrow-3 Weapon Systems.

The success of this test is a major milestone in the operational capabilities of the State of Israel and the nation's ability to defend itself against current and future threats in the region.

According to a September 6, 2018, posting at the ***Defense Industry Daily*** infosite, "*Because missile defenses are so important, states like India and Israel have taken steps to ensure that they have the ability to build many of the key pieces. The Arrow project is a collaboration between Boeing and IAI to produce the missile interceptors that accompany the required radars, satellites, command and control systems.*"

MDA Director Lt. General ***Samuel Greaves*** said that this successful test provides confidence in Israel's capability to protect itself from existing threats in the region. Congratulations to the Israel Missile Defense Organization, the Israeli Air Force, the MDA team, and industry partners.

The General added that the MDA is committed to assisting the government of Israel in upgrading its national missile defense capability against emerging threats.

משרד הביטחון
MINISTRY OF DEFENSE

www.mod.gov.il

U.S. DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY

mda.mil

Introducing the

WALTON DE-ICE Portable Radome

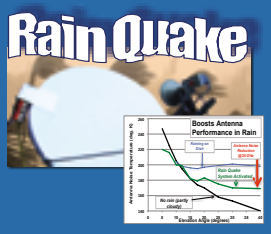
Unleash new SATCOMS capabilities in extreme conditions

NOW AVAILABLE
Call for details!

Whether the mission demands staying on-air in a 85 mile-per-hour (136 kph) wind storm, a sandstorm, a blizzard, hail, or torrential rains – the **Portable Radome** helps make satellite networks more survivable and deployable into extreme or harsh environments. Gain significant cost saving vs. conventional radomes for military or civilian networks. Heating and air-conditioning options.

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.

Call / email to meet at: NABSHOW Where Content Comes to Life

+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

Dispatches

MUOS comms upgrades contract awarded to Harris by the U.S.M.C.

The U.S. Marine Corps (USMC) has awarded Harris Corporation (NYSE:HRS) a $75 million order to provide MUOS (Mobile User Objective System) narrowband satellite communication upgrades to the service's Falcon III® AN/PRC-117G manpack radio fleet.

This order is part of the Navy Portable Radio Program five-year IDIQ contract received in 2017.

Harris has continued to invest in the development and deployment of MUOS and other advanced waveforms to add capability to the widely deployed ***AN/PRC-117G*** family of radios, as well as its next generation of tactical radios.

As a *software defined radio* (SDR), the AN/PRC-117G was developed to be easily upgradable with new waveforms such as MUOS, enabling customers to increase capabilities economically.

The MUOS software upgrade will allow Marines to access the new, advanced MUOS satellite constellation that provides next-generation satellite communications, enabling them to talk and more easily share data anywhere in the world.

The AN/PRC-117G MUOS software upgrade will also provide the Marines with a greater number of SATCOM users, enhanced voice and data communication, and robustness in disadvantaged environments where they operate, such as urban and high/low latitude locations.

In addition to the MUOS upgrades, Harris will deliver ancillary devices for the AN/PRC-117G radios currently fielded by the USMC.

These include antennas that enable the Harris radios to support SATCOM-On-The-Move (SOTM) while connected to the MUOS satellites.

Dana Mehnert, President, Harris Communication Systems, said that adding this capability to the 117G will enable the Marines to leverage the proven radios they have already deployed, fought and trained with to access the advanced capabilities and capacity of the MUOS satellites with a simple software upgrade. The MUOS upgrade also will enable interoperability with other U.S. Department of Defense and allied users who deploy this advanced capability in the future.

www.marines.mil

www.harris.com

The Harris AN/PRC-117G(V)1(C) Multiband Networking Manpack Radio.

WAVESTREAM

AMPLIFYING MISSION-CRITICAL SATELLITE COMMUNICATION

Industry leading efficiency and reliability for the world's harshest environments

INTRODUCING

The new 60W Ku-Band GaN BUC

www.wavestream.com

A KRATOS CONSTELLATIONS PODCAST EXCERPT: MILSATCOM, SMALLSATS & MORE...

NSR Analyst Brad Grady joins Kratos Constellations for a Q&A

The Constellations podcast by Kratos connects the listener to the innovators, entrepreneurs and policy makers who are making and remaking today's satellite and space industries.

A recent Constellation guest was ***Brad Grady***, Senior Analyst with **Northern Sky Research** (NSR).

The company recently released their ***15th edition*** of their ***Government and Military Satellite Communications*** report.

After several years of stagnation, the MILSATCOM market is growing, with the $5 billion revenue in 2017 expected to double over the next decade.

What's causing this change, and what are the key factors driving the military market are the topics of discussion for the Constellations podcast — the original interview has been edited for brevity and format.

— Listen to this and 40 other podcast interviews on Constellations —
www.kratoscomms.com/constellations-podcast?utm_source=MilSat&utm_medium=email&utm_campaign=Feb2019

John Gilroy for Constellations
Brad, the DOD doesn't seem ready to adopt LEO or large constellation architectures for future DOD-owned constellations.

Do you think the nascent LEO mega constellation such as OneWeb will be successful in proving out that model?

Brad Grady, NSR (BG)
When we talk about adopting mega LEO constellations or non-GEO HTS constellations there are lots of challenges, and not just in flying them.

When you look at players such as **OneWeb**, **SpaceX** or **Telesat**, one of the surprising things that we found in our latest report, and what's come out of the DoD's wideband *Analysis of Alternatives* (AoA) study, is how many issues are happening on the ground. There are 17,000 terminals and trying to build and consolidate those terminal programs is a difficult task.

Constellations
So, the non-GEO world is affecting the ground market as well?

BG
Yes, in both commercial and government. On the commercial side, there are evolving business models, and on the government side, they've never been an early adopter. It's always been a let's wait and see, and there are various reasons for that. We expect to see the same behavior on the non-GEOs.

Constellations
What is the role for non-GEO satellites in the military market?

BG
It's important to make the distinction between the LEO players that are coming and MEO. O3b by SES, which is MEO, is providing connectivity and services to the DoD across a variety of applications and doing things that you wouldn't necessarily expect, like airborne communications and other applications. So, it's a question of how LEO is going to be integrated into that network design.

Constellations
When you look at the technologies on the ground – the terminals, the waveforms, the command and control, even policy – are these lagging and putting obstacles in front of the space segment?

BG
Yes, and it's not just a DOD trend. It's across the satellite sector in general of how we take advantage of next generation networks and new space technologies and integrate that into our network.

We're seeing this emergence of multi-band antennas being able to integrate multiple frequencies, multiple architectures into the antenna itself and build that network and simplify the ground infrastructure.

For example, you don't want an antenna farm of four or five bespoke antennas each doing just one thing on a Navy ship with limited space.

Constellations

Is it a matter of financial considerations or are there too many new choices now with all these advances?

BG

A bit of both. On the investment side, the challenge is you've already invested in the 17,000 terminals for the U.S. DOD and others across the world. What do you do with them when you're talking about adding new things into the network that weren't designed for them?

There may be some additional investments or additional problems to migrate those terminals to new technologies and new infrastructures. How do you bring the old into new networks and new architectures? But with the new, you have a real chance for innovation in those technologies.

Constellations

Is the addition of more MILSATCOM wideband capacity adding to the confusion?

BG

Absolutely. If you're a commercial player and you hear the recent allocation from Congress for WGS 11 and 12, you worry if that's a sign of things to come with the U.S. government investing in more wideband capabilities.

I think the answer is probably not. If there's one trend that we've seen, bandwidth demand goes up, not down, and even with the creation of the WGS program, commercial SATCOM leasing is continuing to go up.

Another result from the wideband AoA is the need to design in next generation architecture from day zero, not as an add-on later.

Constellations

It seems that the commercial and the federal worlds are each trying to learn from each other and take their cue from who the leaders are.

For example, there's now greater capacity being offered from GEO HTS Ka band for the overall market, but is it changing the military?

BG

What's interesting is that WGS uses Ka. In certain countries it's a dedicated military frequency, and in other countries it's just Ka-band.

If you look at a system such as ***Global Xpress*** from **Inmarsat** or **Viasat**, there's some compatibilities on the terminal side designed to operate in Ka-band. If you're a DoD customer, you can bring some of your existing ground infrastructure onto these new commercial systems. That's a great selling point for a commercial satellite operator, meaning you don't have to buy my terminal, you can bring yours onto my network and migrate.

Another point is that integrating networks used to require stitching together widgets from company A and company B, whereas now they're focused much more on the IP layer. Commercial providers can now say, '*I'll bring everything up to that IP ethernet port, and you can manage everything on the other side.*'

Artistic rendition of WGS satellites.

Constellation

Are there examples of the commercial and government markets engaging in a sort of public-private partnership?

BG

The best example of a public-private partnership in the government SATCOM world is ***Skynet 5*** from the UK.

There was a partnership between the UK government and **Airbus** to have a fully managed proprietary military system delivered as a service. There were some challenges, but many saw Skynet as one of the better-managed PPP programs.

The flipside of that outsourcing is the brain drain. If you ever want to go back to "*sovereign capabilities,*" you need to hire new staff to learn to fly a satellite, to operate the RF layer, to manage the cyber security posture and more.

Government customers need to walk that line and manage what can be outsourced. Now that we're focused a lot more on IP, that brings more opportunities to focus on network services and throughput, not just whether your terminal operates with this waveform or this specific capability.

Constellations
What other significant changes do you see?

BG
The pace of innovation in government SATCOM today is faster than ever before.

WGS 11 and 12 are proposed to deliver on commercial timeframes, which if believed, would be in 36 months or so. It's yet to be determined whether 11 and 12 will be another version of the WGS constellation that they've done, or if they are bringing next generation capabilities. That will shape a lot of direction.

Constellations
Commercial SATCOM providers want to offer managed services to the government, much like consumers who buy internet service. However, DoD wants the flexibility to buy from different vendors. How is the DoD addressing this push pull?

BG
On the surface, there are two ways. One is the DoD is still what I would call a service provider. When they buy raw capacity, they go to a satellite operator and say, '*Give me a percentage of airtime, and I'll build the network and connect the people.*' They're acting like a service provider.

Traditionally, this bulk leasing market has been in decline, but we're seeing a resurgence. Even with falling capacity prices and other market dynamics, in our recent report we've seen more optimism because there are certain inherent benefits of security, ownership, and sovereignty that you can't get away from.

Constellations
Given its requirements, the government wants satellite networks and enterprise architecture with resilience, while on the other side commercial providers want steady cash flow and indemnification. How are they working together to make long-term plans for DoD SATCOM?

BG
There's a meeting in the middle. The government is agreeing to change acquisition and to consolidate approaches across military systems, and commercial is making certain investment choices.

Procurement is a challenge to work through, but on a technical level there's optimism in terms of flexible modem interfaces and other new hardware integration capabilities between military systems and various commercial systems. That's what's required to go forward.

Constellations
The U.S. Air Force study identified various types of wideband terminals across military inventory that are not compatible with commercial networks. Isn't this a problem?

BG
Yes, it surprised many people, and not just the 17,000 terminals out there, but the 100 different programs and staff for acquiring these capabilities.

If you were a commercial provider, a cruise ship company or an oil and gas operator, you would not operate this way. There's still friction and inertia behind that mindset, but there's also a great deal of positive change.

Constellations
Two words that get many people upset is acquisition reform. What's the military doing about this incompatibility?

BG
One of the first steps is that they've decided to put the people who buy MILSATCOM systems alongside the people who buy COMSATCOM systems.

The people building WGS are sitting alongside the people who are buying transponders and managed services and those things, which implicitly helps the problem. If you have people sitting in the same room, they can talk to each other.

The next is designing in commercial capabilities from day zero. If providers see that you're going to invest in these new technologies, then they can bring commercial best practices in to solve government problems. They'll focus on integrating at that IP layer rather than the RF layer or the hardware level.

Constellations
This will help government better deal with change in the future?

BG
One of the buzzwords is software defined... fill in the blank. Whether it's terminals or software defined networks it's a hot topic for a lot of reasons. It brings a lot of flexibility into the equation.

You can imagine a warfighter in the field, with only one terminal, one modem, and the satellite they need to talk to is not available. If they can upload a new waveform, a new capability, that's the holy grail for resiliency and redundancy.

We're seeing that on the commercial side with flexible satellite architectures and infrastructures and the amazing power that software can bring to redefining networks on the fly. Government is looking to take advantage of that.

Constellations
Along those lines, we hear terms like 'networks of networks.' Is there really something to that?

BG
It gets back to the warfighter scenario, where you need to figure out how to talk from Network 1 to Network 2. It's hybrid networks, networks of networks, and systems of systems, and creating that flexible ground infrastructure to not care what the transport path is.

Maybe I need security around my ISR information and that needs to go over a proprietary network, otherwise it can go over a public network.

With networks of networks, we're talking about best routing, least cost routing, those technical capabilities of matching the requirement of the application to the dynamics of the network.

Constellations
So it seems more and more is being driven by what's happening on the ground.

BG
The next 12 to 18 months are going to be key in deciding whether these reforms are just the typical Washington dog and pony show or if there's something really there.

We found in our NSR report many positive aspects to believe the story this time, and not just from the U.S. We see lots of people outside the U.S. investing in the technologies, capabilities, and services that are pushing the market forward.

Constellations
Thank you, Brad.

Want to hear from more movers and shakers?
Listen to the Constellations podcast.
Subscribe at:
www.kratoscomms.com/constellations-podcast?utm_source=MilSat&utm_medium=email&utm_campaign=Feb2019

Have a topic you'd like us to discuss?
Email Kratos at:
Podcast@KratosComms.com

NABSHOW®

Where Content Comes to Life

APRIL 6–11, 2019 | LAS VEGAS

Register Today: NABShow.com

Free* Exhibits Pass with Code MP01

No one knows Media, Entertainment and Technology like us.

Industry convergence is powering the stories the world consumes. This is where you need to be. Surrounded by new gear, impressive tech and big thinking. NAB Show® is the real deal. And where deals are done.

Join our global community finding inspiration, discovering solutions, building audiences and growing profits. Together, we advance the art, science and business of storytelling.

your story will never be the same.

**Offer expires March 24, 2019. Starting March 25, a $50 fee will be applied.*

A DEFENSE INTELLIGENCE AGENCY ANALYSIS & REPORT

China — Military Power (Report excerpts that focus on Space/Counterspace, republished with DIA permission)

Lt. Gen. Robert P. Ashley, Director, Defense Intelligence Agency.

The following article contains excerpts from Lieutenant General *Robert P. Ashley*, Jr.'s, preface to, as well as the report itself, authored by the Defense Intelligence Agency's (DIA) and are republished with permission of the DIA...

"Chinese leaders characterize China's long-term military modernization program as essential to achieving great power status. Indeed, China is building a robust, lethal force with capabilities spanning the air, maritime, space and information domains which will enable China to impose its will in the region. As it continues to grow in strength and confidence, our nation's leaders will face a China insistent on having a greater voice in global interactions, which at times may be antithetical to U.S. interests.

"With a deeper understanding of the military might behind Chinese economic and diplomatic efforts, we can provide our own national political, economic, and military leaders the widest range of options for choosing when to counter, when to encourage, and when to join with China in actions around the world.

"This report offers insights into the modernization of Chinese military power as it reforms from a defensive, inflexible ground-based force charged with domestic and peripheral security responsibilities to a joint, highly agile, expeditionary, and power-projecting arm of Chinese foreign policy that engages in military diplomacy and operations across the globe."

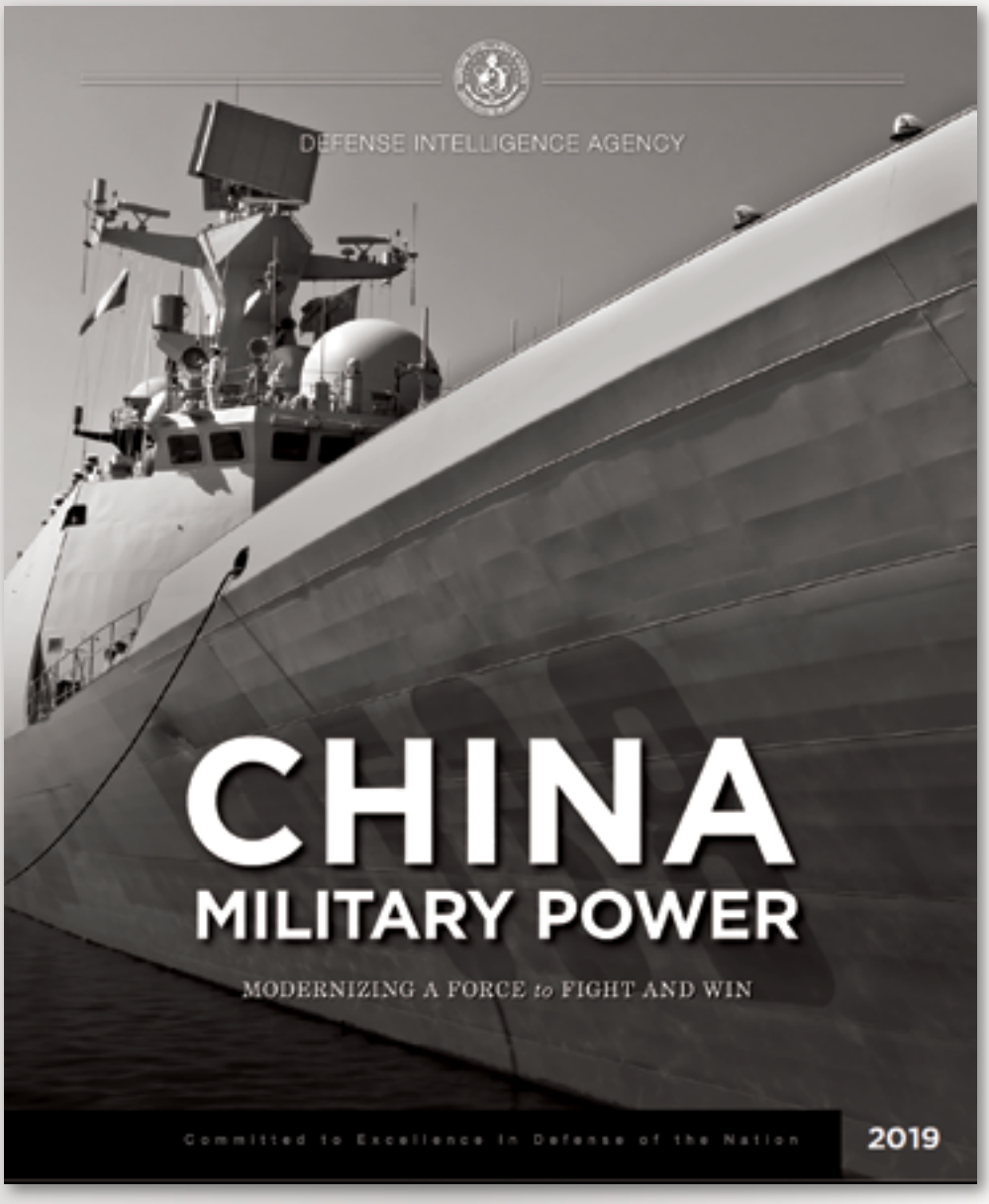
Space/Counterspace

Outer space has become a commanding height in international strategic competition. Countries concerned are developing their space forces and instruments, and the first signs of weaponization of outer space have appeared. China has all along advocated the peaceful use of outer space, opposed the weaponization of and arms race in outer space, and taken an active part in international space cooperation. China will keep abreast of the dynamics of outer space, deal with security threats and challenges in that domain, and secure its space assets to serve its national economic and social development, and maintain outer space security. ***— Excerpt from China's Military Strategy, May, 2015***

The Chinese *People's Liberation Army* (PLA) historically has managed China's space program and continues to invest in improving China's capabilities in space-based ISR, satellite communication, satellite navigation, and meteorology, as well as human spaceflight and robotic space exploration.[1]

China uses its on-orbit and ground-based assets to support national civil, economic, political, and military goals and objectives.

Strategists in the PLA regard the ability to use space-based systems and deny them to adversaries as central to enabling modern, informatized warfare.



As a result, the PLA continues to strengthen its military space capabilities despite its public stance against the militarization of space.

Space operations probably will form an integral component of other PLA campaigns and serve a key role in enabling actions to counter third-party intervention during military conflicts.

China continues to develop a variety of counterspace capabilities designed to limit or prevent an adversary's use of space-based assets during crisis or conflict. In addition to the research and possible development of satellite jammers and directed-energy weapons, China has probably made progress on kinetic energy weapons, including the anti-satellite missile system tested in July 2014.[2]

China is employing more sophisticated satellite operations and probably is testing on-orbit dual-use technologies that could be applied to counterspace missions. The PLA's ***Strategic Support Force*** (**SSF**), established in December OF 2015, has an important role in the management of China's aerospace warfare capabilities.[3]

Consolidating the PLA's space, cyber, and electronic warfare capabilities into the SSF enables cross-domain synergy in "*strategic frontiers.*" The SSF may also be responsible for research, development, testing, and fielding of certain "*new concept*" weapons, such as directed energy and kinetic energy weapons.

The SSF's space function is primarily focused on satellite launch and operation to support PLA reconnaissance, navigation, and communication requirements. *[For more on the SSF, please see Appendix E.]*

Space and counterspace capabilities — such as missile forces, advanced air and seapower, and cyber capabilities — are critical for China to fight and win modern military engagements.

To support various requirements, China has built a vast ground and maritime infrastructure enabling spacecraft and ***space launch vehicle*** (**SLV**) manufacture, launch, C2, and data downlink.

— Satellites —

China employs a robust space-based ISR capability designed to enhance its worldwide situational awareness. Used for civil and military remote sensing and mapping,

Long March-3B SLV in midlaunch. Photo is courtesy of AFP.

A Chinese Space Operations Center. Photo is courtesy of AFP.

terrestrial and maritime surveillance, and military intelligence collection, China's ISR satellites are capable of providing electro-optical (EO) and synthetic aperture radar imagery, as well as electronic intelligence and signals intelligence data.[4]

China pursues parallel programs for military and ***commercial communications satellites*** (**COMSATs**), and owns and operates about 30 COMSATs that are used for civil, commercial, and military satellite communications. The PLA operates a small number of dedicated military COMSATs.[5]

China's civil COMSATs incorporate turnkey off-the-shelf, commercially manufactured components and China produces its military-dedicated satellites domestically.[6]

China continues to launch new COMSATs to replace its aging satellites and increase its overall satellite communications bandwidth, capacity, availability, and reliability. China uses its domestically produced ***Dongfanghong- 4*** (**DFH-4**) satellite bus—the structure that contains the components of the satellite— for its military COMSATs.[7]

Even though early satellites suffered mission-ending or mission-degrading failures, the DFH-4 has become a reliable satellite bus. The PLA and government continue to vigorously support the program and have signed numerous contracts with domestic and international customers for future DFH-4 COMSATs.

The DFH-4 bus has also allowed China to position itself as a competitor in the international COMSAT market, orchestrating many contracts with foreign countries to supply on-orbit satellites, ground-control systems, and training.

In 2008, China launched the first ***Tianlian*** data-relay satellite of its China Tracking and Data Relay Satellite constellation. As of December 2017, China had four Tianlian data-relay satellites on orbit, allowing China to relay commands and data to and from its satellites even when those satellites were not over Chinese territory.

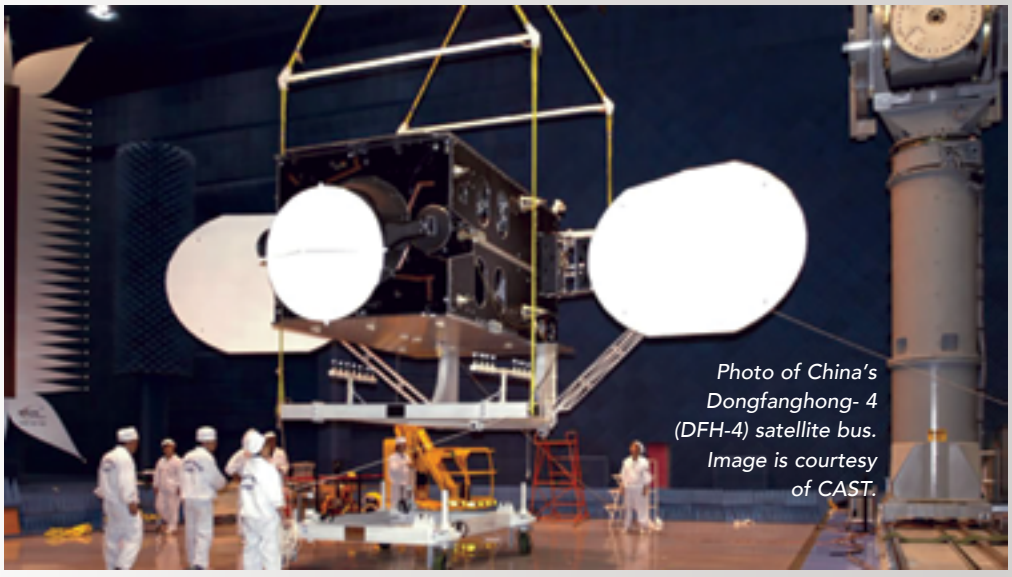


Photo of China's Dongfanghong- 4 (DFH-4) satellite bus. Image is courtesy of CAST.

In 2000, China launched its first Beidou satellites to test the development of a regional satellite navigation system. By 2012, China had established a regional satellite navigation constellation consisting of 10 Beidou satellites and had initiated testing of a global constellation similar to the U.S. Global Positioning System (GPS).[8]

As Beidou satellites continue to be placed in orbit, by 2020 China will complete its global constellation of 27 Beidou satellites while maintaining a separate regional constellation providing redundant coverage over Asia.[9]

Artistic rendition of a Chinese Beidou satellite. Image is courtesy of CAST.

China owns and operates 10 domestically produced ***Fengyun*** and ***Yunhai*** meteorological satellites.[10] The *China Meteorological Administration* supports civilian and military customers with the delivery of meteorological data and detailed weather forecasts. The newer satellites house almost a dozen all-weather sensors concerning atmospheric conditions as well as maritime terrain data for military and civilian customers. China's membership in the World Meteorological Organization grants it free access to global meteorological data from the international organization's 191 members.[11]

Artistic rendition of China's Fengyun satellite.

— Counterspace —

The PLA is acquiring a range of technologies to improve China's counterspace capabilities. China is developing anti-satellite capabilities, including research and possible development of directed-energy weapons and satellite jammers, and probably has made progress on the anti-satellite missile system that it tested in July 2014. China is employing more sophisticated satellite operations and probably is testing dual-use technologies that could be applied to counterspace missions.[12]

China has not publicly acknowledged the existence of any new programs since it confirmed it used an anti-satellite missile to destroy a weather satellite in 2007. PLA writings emphasize the necessity of "*destroying, damaging, and interfering with the enemy's reconnaissance… and communications satellites,*" suggesting *that such systems, as well as navigation and early warning satellites, could be among the targets of attacks designed to "blind and deafen the enemy."*[13,14]

— Human Spaceflight + Space-Exploration Probes —

China became the third country to achieve independent human spaceflight in 2003, when it successfully orbited the crewed ***Shenzhou-5*** spacecraft, followed by space laboratory ***Tiangong- 1*** and ***-2*** launches in 2011 and 2016, respectively. China intends to assemble and operate a permanently inhabited, modular space station capable of hosting foreign payloads and astronauts by 2022.[15]

China is the third country to have soft-landed a rover on the Moon, deploying the rover Yutu as part of the Chang'e-3 mission in 2013. China's Lunar Exploration Program plans to launch the first mission to land a rover on the lunar far side in 2018 (Chang'e-4), followed by its first lunar sample-return mission in 2019 (Chang'e-5).[16,17,18]

Artistic rendition of China's Tiangong-2 space lab docked with a crewed Shenzhou spacecraft. Image is courtesy of China Aerospace Science and Technology Corporation (CAST).

— Space Launch —

China has a robust fleet of launch vehicles to support its requirements. The ***Chang Zheng***, or ***Long March***, and ***Kuaizhou*** SLVs can launch Chinese spacecraft to any orbit.

China's space launch sites. Image source: DIA, D3 Design.
All locations are approximate. Boundary representation is not necessarily authoratative. Depiction of claims on this map is without prejudice to U.S. non-recogntiion of any such claims.

System	Propellant	Generation	Outlook
LM-2, LM-3, LM-4 series	Liquid	Legacy	Phase out by 2025
LM-5 series	Liquid	Next	Heavy-lift for the proposed space station and other payloads
LM-6	Liquid	Next	Light-lift for low Earth and sun-synchronous orbit
LM-7	Liquid	Next	Medium-lift for human spacefight and resupply to the future space station
LM-11 and Kuaizhou series	Solid	Next	Lift for emergency response

China's space launch fleet[19,20,21.]

— Cyberspace —

Authoritative PLA writings identify controlling the "*information domain*"—sometimes referred to as "**information dominance**"—as a prerequisite for achieving victory in a modern war and as essential for countering outside intervention in a conflict.[22]

The PLA's broader concept of the information domain and of information operations encompasses the network, electromagnetic, psychological, and intelligence domains, with the "network domain" and corresponding "network warfare" roughly analogous to the current U.S. concept of the cyber domain and cyberwarfare.[23]

The PLA *Strategic Support Force* (SSF) may be the first step in the development of a cyberforce by combining cyber reconnaissance, cyberattack, and cyberdefense capabilities into one organization to reduce bureaucratic hurdles and centralize command and control of PLA cyber units.

Official pronouncements offer limited details on the organization's makeup or mission. China's President ***Xi*** simply said during the SSF founding ceremony on December 31, 2015, that the SSF is a "*new-type combat force to maintain national security and [is] an important growth point for the PLA's combat capabilities.*"[24]

The SSF probably was formed to consolidate cyber elements of the former PLA ***General Staff Third*** (Technical Reconnaissance) and ***Fourth*** (Electronic Countermeasures and Radar) ***Departments and Informatization Department***.[25,26]

Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces.

Being one of the major victims of hacker attacks, China is confronted with grave security threats to its cyber infrastructure. As cyberspace weighs more in military security, China will expedite the development of a cyberforce, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability. — Excerpt from China's Military Strategy, May, 2015

The PLA could use its cyberwarfare capabilities to support military operations in three key areas.

First, cyber reconnaissance allows the PLA to collect technical and operational data for intelligence and potential operational planning for cyberattacks because the accesses and tactics, techniques, and procedures for cyber reconnaissance translate into those also necessary to conduct cyberattacks.

Second, the PLA could employ its cyberattack capabilities to establish information dominance in the early stages of a conflict to constrain an adversary's actions or slow mobilization and deployment by targeting network-based C2, C4ISR, logistics, and commercial activities.

Third, cyberwarfare capabilities can serve as a force multiplier when coupled with conventional capabilities during a conflict. PLA military writings detail the effectiveness of information operations and cyberwarfare in modern conflicts, and advocate targeting an adversary's C2 and logistics networks to affect the adversary's ability to operate during the early stages of conflict

One authoritative source identifies an adversary's C2 system as "*the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield.*"[27]

China's cyberwarfare could also focus on targeting links and nodes in an adversary's mobility system and identifying operational vulnerabilities in the mobilization and deployment phase.

The PLA also plays a role in cyber theft. In May 2014, the ***U.S. Department of Justice*** indicted five PLA officers on charges of hacking into the networks of U.S. companies for commercial gain.

Beijing maintains that the Chinese government and military do not engage in cyber-espionage and that the United States fabricated the charges.[28,29]

— Denial and Deception —

The PLA uses military deception to reduce the effectiveness of adversaries' reconnaissance and to deceive adversaries about the PLA's warfighting intentions, actions, or major targets.[30]

PLA tradition emphasizes deception and psychological manipulation to create asymmetric advantages and enable surprise.

The PLA has a longstanding doctrine for deception, and claims that it regularly practices deception during training.

PLA sources describe military deception as a form of combat support, on par with ISR, meteorological support, missile calculation, engineering, and logistic support.

Denial and deception activities include:[31]

- *Concealing and camouflaging.*
- *Blending false or misleading military movements with actual deployments and war preparations.*
- *Employing counter-reconnaissance: understanding and evading, jamming, or destroying the whole spectrum of enemy reconnaissance activities against PLA units and facilities.*
- *Using deceptive maneuvers, psychological ploys, and unorthodox schemes to deceive, confuse, or otherwise manipulate an adversary into a militarily disadvantageous position.*[32]

Skillfully employed, deception can paralyze an enemy force and achieve decisive results. Options range from no-warning strikes, violent multi-axis strikes, and envelopment to a less ambitious attempt to confuse the adversary regarding the exact timing, nature, direction, or scope of a PLA operation.[33,34]

The complete DIA China Military Power report is available at:
www.dia.mil/Military-Power-Publications

References

[1]*Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017, Office of the Secretary of Defense; May 2017.*

[2]*Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017, Office of the Secretary of Defense; May 2017.*

[3]*Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017, Office of the Secretary of Defense; May 2017.*

[4]*Harvey, Brian, China in Space: The Great Leap Forward; 2013; Springer Science + Business Media; New York.*

[5]Report; Stokes, Mark A. and Dean Cheng; Project 2049 Institute for the U.S.-China Economic and Security Review Commission; China's Evolving Space Capabilities: Implications for U.S. Interests; 26 April 2012; http://project2049.net/documents/ uscc_ china-space-program-report_april-2012.pdf.

[6]Report; Stokes, Mark A. and Dean Cheng; Project 2049 Institute for the U.S.-China Economic and Security Review Commission; China's Evolving Space Capabilities: Implications for U.S. Interests; 26 April 2012; http://project2049.net/documents/ uscc_ china-space-program-report_april-2012.pdf.

[7]White Paper; The State Council Information Office of the People's Republic of China; China's BeiDou Navigation Satellite System; June 2016; http://www.scio.gov.cn/zxbd/ wz/ Document/1480433/1480433.htm.

[8]White Paper; The State Council Information Office of the People's Republic of China; China's BeiDou Navigation Satellite System; June 2016; http://www.scio.gov.cn/zxbd/ wz/ Document/1480433/1480433.htm.

[9]Internet; Xinhua; China To Launch 30 Beidou Navigation Satellites In Next 5 Years; 19 May 2016; http://english.cas.cn/ newsroom/china_research/201605/ t20160523_163363.shtml.

[10]Report; Stokes, Mark A. and Dean Cheng; Project 2049 Institute for the U.S.-China Economic and Security Review Commission; China's Evolving Space Capabilities: Implications for U.S. Interests; 26 April 2012; http://project2049.net/documents/ uscc_ china-space-program-report_april-2012.pdf.

[11]World Meteorological Organization; Satellite Status; accessed 17 October 2016; www.wmo.ing/pages/prog/sat/ satellitestatus.php.

[12]Annual Report to Congress; Military and Security Developments Involving the People's Republic of China 2017; Office of the Secretary of Defense; May 2017.

[13]Peng Guangqian, Yao Youzhi, eds; 2001; Science of Strategy. 132 Li Bingyan, 27 Jan 2016; Beijing Guangming Ribao: General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War.

[14]China Manned Space Engineering Office Website; Space Station Project Development Progress; 23 April 2016; http://www.cmse.gov.cn/uploadfile/news/uploadfile/ 201604/20160427104809225.pdf.

[15]Internet; Xinhua; Chang-E 5 To Launch Sometime in 2017 -- China's Latest Secret Lunar Exploration Project Uncovered; 1 March 2014; http://news.xinhuanet.com/ tech/2014- 03/01/c_119562037.htm.

[16]Xinhua: China To Land On Dark Side Of Moon In 2018; 14 January 2016; http:// news.xinhuanet.com/english/ 2016-01/15/ c_135010577.htm.

[17]Internet, NASASpaceFlight, Chang'e-5 Lunar Sample Return, CZ-5 - Wenchang - NET 2017, http:// forum.nasaspaceflight. com/index. php?action=dlattach;topic=33431.0;attach= 1440126, Accessed 28 July 2017.

[18]Report; Stokes, Mark A. and Dean Cheng; Project 2049 Institute for the U.S.-China Economic and Security Review Commission; China's Evolving Space Capabilities: Implications for U.S. Interests; 26 April 2012; http://project2049.net/documents/ uscc_ china-space-program-report_april-2012.pdf.

[19]Briefing; Zhou, Yuanying; China Great Wall Industry Corporation; China's Space Industry: Achievement, Future Planning and International Cooperation; presented by Zhou Yuanying for China Great Wall Industry Corporation at the 4th International Space Conference, Vilnius, Lithuania 18 Sept. 2012; updated 27 Sept. 2013.

[20]China Space Flight; Chinese Rocket service time; 12 March 2016; http:// www.chinaspaceflight.com/rocket/China-launchers-timeline.html.

[21]Kevin Pollpeter and Kenneth Allen ed; 26 AUG 2015; DGI; The PLA as Organization: Reference Volume v2.0; pp 401.; http:// www.andrewerickson.com/2015/12/a-classic-reference- with-renewed-relevance-download-the-pla-as-organization- v2-0/.

[22] Joe McReynolds; 17 APR 2016; Jamestown Foundation China Brief; China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy; pp 6; https://jamestown.org/ program/chinas-evolving-perspectives- on-network-warfare-lessons-from-the-science-of-military- strategy/.

[23]Lincoln Davidson; 'China's Strategic Support Force: The New Home of the PLA's Cyber Operations?'; CFR. org; Net Politics; January 20, 2016; http://blogs.cfr.org/ cyber/2016/01/20/chinas-strategic-support-force-the-newhome- of-the-plas-cyber-operations/.

[24]John Costello; 'The Strategic Support Force: China's Information Warfare Service'; The Jamestown Foundation; China Brief Vol. 16 Issue 3; February 8, 2016; https:// jamestown. org/program/the-strategic-support-force-chinas-information- warfare-service/.

[25]John Costello; 'China Finally Centralizes Its Space, Cyber, Information Forces'; TheDiplomat.com; January 20, 2016. 145 Peng Guangqian, Yao Youzhi, eds; 2001; Science of Strategy; pp 311.

[26]Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage;" May 19, 2014; URL: http:// www.justice.gov/opa/pr/2014/May/14- ag-528.html.

[27]Lesley Wroughton, Michael Martina, "Cyber spying, maritime disputes loom large in U.S.-China talks," Reuters, July 8, 2014, URL: https:// www.reuters.com/article/ china-usa/cyber-spying-maritime-disputes-loom-large-in-u-schina- talks-idUSL4N0PJ0MT20140708.

[28]Zhang Yuliang (ed.), Science of Campaigns (National Defense University, Beijing, 2006; ISBN 7-5626-1407-0) p. 155-66.

[29]Zhang Yuliang (ed.), Science of Campaigns (National Defense University, Beijing, 2006; ISBN 7-5626-1407-0) p. 155-66.

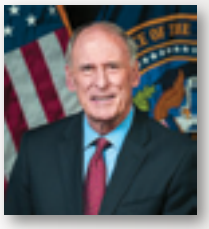
[30]Zhang Xingye and Zhang Zhanli ed., Campaign Stratagems, (PLA National Defense University, Beijing, 2002), p. 1-2, 26-8

[31]Zhang Yuliang (ed.), Science of Campaigns (National Defense University, Beijing, 2006; ISBN 7-5626-1407-0) p. 96-7.

[32]"Theories of the Initial Period of War" in Tiao Youzhi, ed., Theories of War and Strategy, PLA Press, Beijing, 2005 p. 564.

[33]Zhang Yuliang (ed.), Science of Campaigns (National Defense University, Beijing, 2006; ISBN 7-5626-1407-0) p. 96-7.

[33]"Theories of the Initial Period of War" in Tiao Youzhi, ed., Theories of War and Strategy, PLA Press, Beijing, 2005 p. 564.



Daniel R. Coats, Director of National Intelligence.

The **Director of National Intelligence** — *Daniel R. Coats* — recently unveiling the ***2019 National Intelligence Strategy*** (**NIS**) report.

The NIS is the guiding strategy for the ***U.S. Intelligence Community*** (**IC**) and will drive the strategic direction for the Nation's 17 IC elements for the next four years.

The 2019 strategy is the fourth iteration for the NIS and seeks to make our nation more secure by driving the IC to be more integrated, agile, resilient, and innovative.

"*This strategy is based on the core principle of seeking the truth and speaking the truth to our policymakers and the American people in order to protect our country*," said Director Coats. "*As a Community, we must become more agile, build and leverage partnerships, and apply the most advanced technologies in pursuit of unmatched insights. The 2019 NIS provides a roadmap to achieve this end.*"

The NIS is one of the most important documents for the IC, as it aligns IC efforts to the National Security Strategy, sets priorities and objectives, and focuses resources on current and future operational, acquisition, and capability development decisions.

Also, the NIS provides the IC with the opportunity to communicate those national priorities to the IC workforce, partners, oversight, customers, and fellow citizens.

The 2019 NIS focuses on:

- *Integration — harnessing the full talent and tools of the IC by bringing the right information, to the right people, at the correct time.*
- *Innovation — making the IC more agile by swiftly enabling the right people and leveraging the right technology and using them efficiently to advance the highest priorities.*
- *Partnerships — leveraging strong, unique, and valuable partnerships to support and enable national security outcomes.*
- *Transparency earning and upholding the trust and faith of the IC's customers and the American people.*

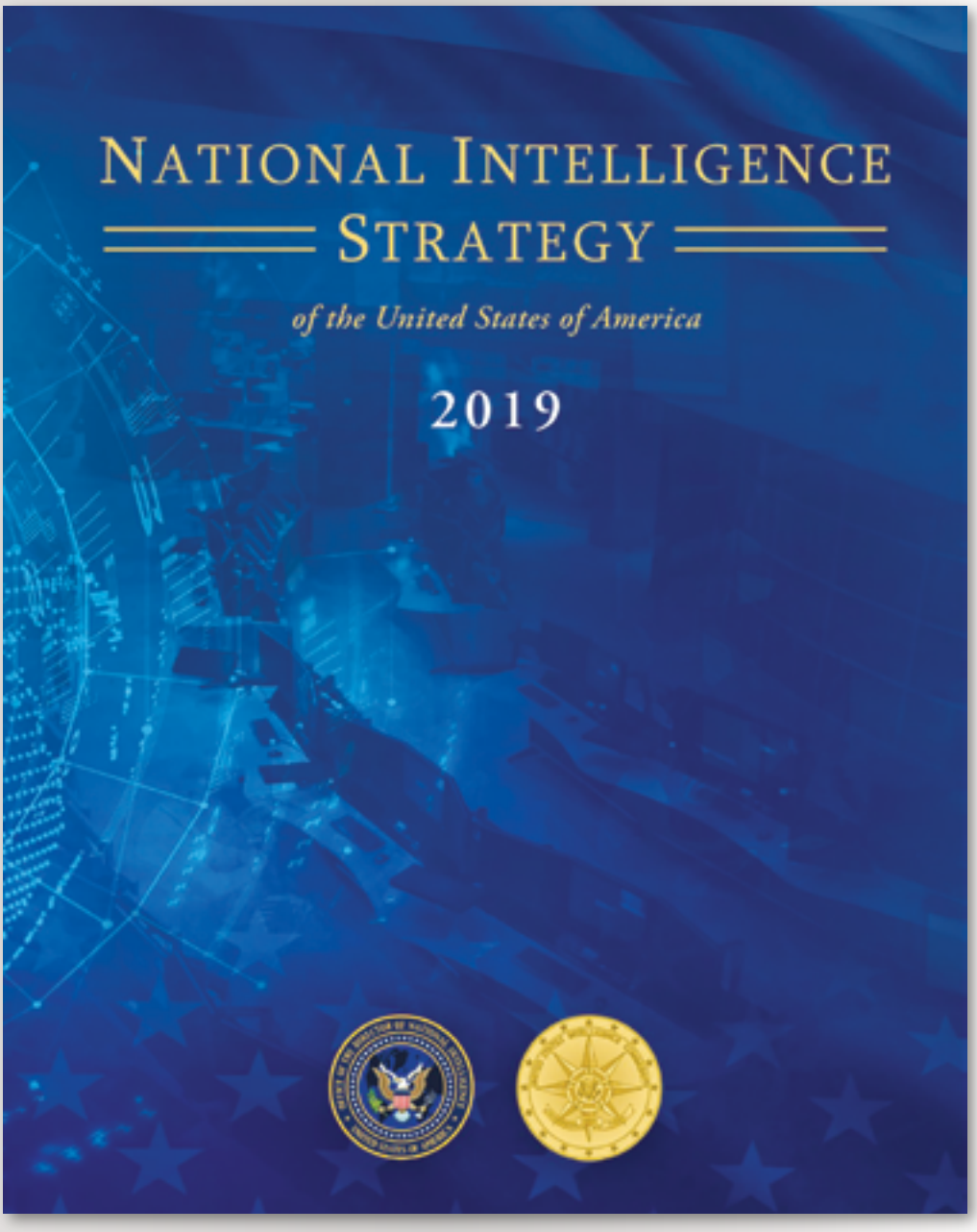
The NIS was developed in response to rapid advances made by our adversaries and the ODNI's recognition that the IC needs to change to more effectively respond to those challenges.

In his 2019 NIS opening message, the DNI stated, "*We face a significant challenge in the domestic and global environment; we must be ready to meet 21st century challenges and to recognize emerging threats and opportunities. To navigate today's turbulent and complex strategic environment, we must do things differently.*"

To guide the IC in facing these challenges, the NIS identifies and explains the IC's objectives — both what the Community must accomplish (mission objectives) and what capabilities the Community must build in order to do so (enterprise objectives).

The seven mission objectives are...

1) strategic intelligence
2) anticipatory intelligence
3) current operations intelligence
4) cyber threat intelligence
5) counter-terrorism
6) counter-proliferation
7) counterintelligence and security.



The seven enterprise objectives are...

1) integrated mission management
2) integrated business management
3) people
4) innovation
5) information sharing and safeguarding
6) partnerships
7) privacy, civil liberties, and transparency.

"*These objectives will allow the IC to continue the crucial work of supporting our senior policymakers, warfighters, and democracy while increasing transparency and protecting privacy and civil liberties,*" said Director Coats. "*Transparency will be our hallmark, and I cannot stress this enough - this is not a limitation on us. Transparency will make us stronger. It is the right thing to do, across the board. This is the reason we publish the NIS at the unclassified level.*"

The Office of the Director of National Intelligence oversees the coordination and integration of the 17 federal organizations that make up the Intelligence Community (*see the infographic on the following page*).

The DNI sets the priorities for and manages the implementation of the National Intelligence Program, which is the IC's budget.

Additionally, the DNI is the principal advisor to the President and the National Security Council on all intelligence issues related to national security.

In this report, within the ***Strategic Environment*** section, the authors note:

Traditional adversaries will continue attempts to gain and assert influence, taking advantage of changing conditions in the international environment—including the weakening of the post-WWII international order and dominance of Western democratic ideals, increasingly isolationist tendencies in the West, and shifts in the global economy.

These adversaries pose challenges within traditional, non-traditional, hybrid, and asymmetric military, economic, and political spheres.

Russian efforts to increase its influence and authority are likely to continue and may conflict with U.S. goals and priorities in multiple regions.

Chinese military modernization and continued pursuit of economic and territorial predominance in the Pacific region and beyond remain a concern, though opportunities exist to work with Beijing on issues of mutual concern, such as North Korean aggression and continued pursuit of nuclear and ballistic missile technology.

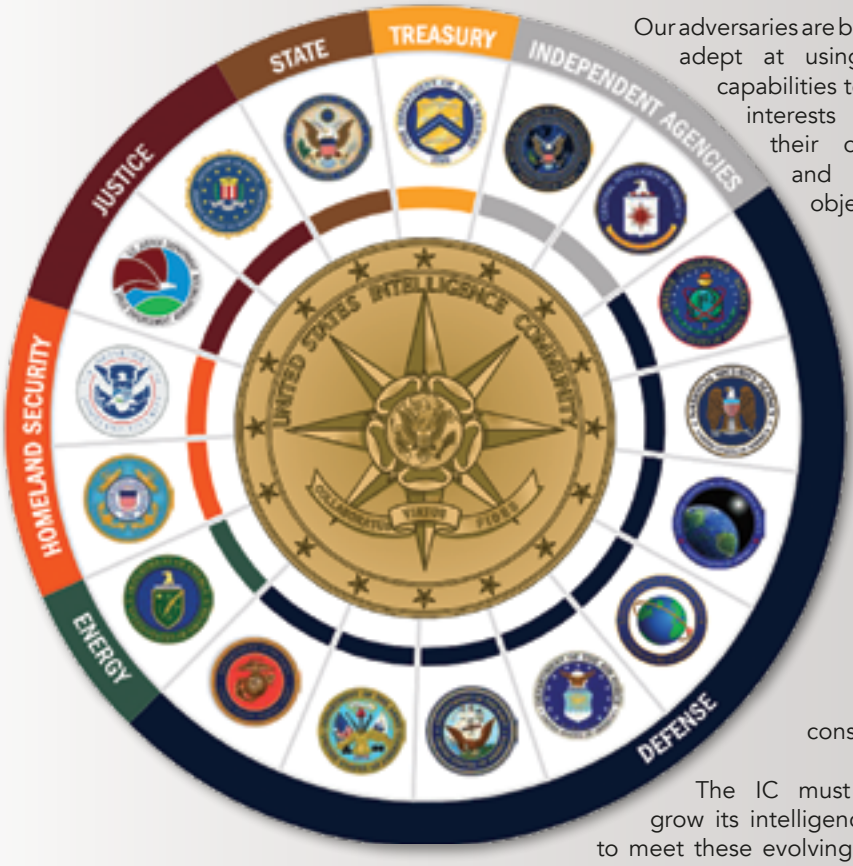
Despite its 2015 commitment to a peaceful nuclear program, Iran's pursuit of more advanced missile and military capabilities and continued support for terrorist groups, militants, and other U.S. opponents will continue to threaten U.S. interests.

Multiple adversaries continue to pursue capabilities to inflict potentially catastrophic damage to U.S. interests through the acquisition and use of ***weapons of mass destruction*** (WMD), which includes biological, chemical, and nuclear weapons. In addition to these familiar threats, our adversaries are increasingly leveraging rapid advances in technology to pose new and evolving threats — particularly in the realm of space, cyberspace, computing, and other emerging, disruptive technologies.

Technological advances will enable a wider range of actors to acquire sophisticated capabilities that were previously available only to well-resourced states.

No longer a solely U.S. domain, the democratization of space poses significant challenges for the United States and the IC. Adversaries are increasing their presence in this domain with plans to reach or exceed parity in some areas.

For example, Russia and China will continue to pursue a full range of anti-satellite weapons as a means to reduce U.S. military effectiveness and overall security.



Increasing commercialization of space now provides capabilities that were once limited to global powers to anyone that can afford to buy them.

Many aspects of modern society — to include our ability to conduct military operations — rely on our access to and equipment in space. Cyber threats are already challenging public confidence in our global institutions, governance, and norms, while imposing numerous economic costs domestically and globally.

As the cyber capabilities of our adversaries grow, they will pose increasing threats to U.S. security, including critical infrastructure, public health and safety, economic prosperity, and stability.

When analyzing cyber threats, the National Intelligence Agency reports that Detect and understand cyber threats from state and non-state actors engaged in malicious cyber activity to inform and enable national security decision making, cybersecurity, and the full range of response activities.

Despite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come.

Our adversaries are becoming more adept at using cyberspace capabilities to threaten our interests and advance their own strategic and economic objectives.

Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices.

The IC must continue to grow its intelligence capabilities to meet these evolving cyber threats as a part of a comprehensive cyber posture positioning the Nation for strategic and tactical response.

Daniel Coats introduced this report with an opening statement...

"*As the Director of National Intelligence, I am fortunate to lead an Intelligence Community (IC) composed of the best and brightest professionals who have committed their careers and their lives to protecting our national security. The IC is a 24/7/365 organization, scanning the globe and delivering the most distinctive, timely insights with clarity, objectivity, and independence to advance our national security, economic strength, and technological superiority.*

"*This, the fourth iteration of the National Intelligence Strategy (NIS), is our guide for the next four years to better serve the needs of our customers, to help them make informed decisions on national security issues, and to ultimately keep our Nation safe.*

"*The NIS is designed to advance our mission and align our objectives with national strategies, and it provides an opportunity to communicate national priority objectives to our workforce, partners, oversight, customers, and also to our fellow citizens.*

"*We face significant changes in the domestic and global environment; we must be ready to meet 21st century challenges and to recognize emerging threats and opportunities. To navigate today's turbulent and complex strategic environment, we must do things differently. This means we must:*

- *Increase integration and coordination of our intelligence activities to achieve best effect and value in executing our mission,*
- *Bolster innovation to constantly improve our work,*
- *Better leverage strong, unique, and valuable partnerships to support and enable national security outcomes, and*
- *Increase transparency while protecting national security information to enhance accountability and public trust.*

"*This National Intelligence Strategy increases emphasis in these areas. It better integrates counterintelligence and security, better focuses the IC on addressing cyber threats, and sets clear direction on privacy, civil liberties and transparency.*

"*We have crucial work before us. Our customers depend on us to help them to make wise national security decisions, and Americans count on us to help protect the Nation, all while protecting their privacy and civil liberties.*

"*We must provide the best intelligence possible to support these objectives; doing so is a collective responsibility of all of our dedicated IC professionals and, together with our partners, we can realize our vision.*

"*Our ongoing goal is to continue to be the very best intelligence community in the world. Thank you for your service and for bringing your talent and commitment to the work of keeping our Nation safe each and every day.*"

www.dni.gov

EXHIBITION PREVIEW (INVITE ONLY): 20 MAY, 2019 EXHIBITS AND CONFERENCE: 21 MAY - 22 MAY, 2019 | PASADENA, CA, USA

SPACE TECH EXPO
USA

AMERICA'S ENGINEERING AND MANUFACTURING MEETING PLACE FOR SPACE TECHNOLOGY

- **Cutting-edge** solutions
- **Innovative** technologies
- **Global** perspectives
- **Unlimited** networking

SPACE SYSTEMS // COMPONENTS, PARTS & ASSEMBLIES // TESTING // INDUSTRY 4.0 TECHNOLOGIES

REGISTER ONLINE FOR A **FREE** EXHIBITS PASS AT **WWW.SPACETECHEXPO.COM**

Contact us: **info@spacetechexpo.com** | +1 855 436 8683 (US and Canada toll free)

THE GOVERNMENT SATELLITE REPORT

A shift is underway in military satellite strategies

By Ryan Schradin, Executive Editor, GSR, and MilsatMagazine Senior Columnist

The satellite industry and global government decision makers came together for the largest military satellite conference in Europe in the fall of last year — the *Global MilSatCom Conference*.

The *Government Satellite Report* kept an eye on the news coming out of that conference and highlights in this article some of the major themes produced at this event.

Across the board, militaries are in the process of reevaluating and changing how they conduct "*business as usual*" when it comes to space. Much of that has to do with the fact that space — itself — has changed as a domain.

Space is no longer a benign domain, thanks to the reemergence on near-peer adversaries capable of challenging and denying space resources and capabilities in theater.

Simultaneously, the space and satellite domain have been revolutionized by the introduction of new commercial players and massive innovation from industry partners.

This innovation has come in the form of a new generation of satellites that are being launched and coming on-line in new orbits, the emergence of commercial space launch and even the advancement of on-orbit refueling and servicing.

Together, these trends have led to global militaries — including the United States military — needing to rethink how they gain access to space capabilities, how they acquire space resources and even how they fundamentally architect and build their space infrastructure.

This has led to some drastic decisions and changes across governments, as well as some head scratching. All of which was on display at *Global MilSatCom*.

Ground segments are getting more attention in military space programs, according to U.S. leaders.

Historically, government customers have met their satellite requirements in a piecemeal fashion — leasing bandwidth on the spot market to fill gaps in coverage and availability, using a mix of MILSATCOM and COMSATCOM resources and purchasing ground terminals for specific requirements.

Unfortunately, this piecemeal approach has led to interoperability issues and challenges within the military's ground infrastructure.

As this article discusses, there were multiple discussions about ground infrastructure at Global MilSatCom about the interoperability challenges and problems with aging ground terminals facing today's military.

One of the proposed solutions was a more holistic approach to satellite acquisition — taking both the space and ground segment into consideration when evaluating and implementing new satellite resources and infrastructure.

However, industry could have another solution in the form of satellite managed services. In this instance, the industry partner is hired as a service provider — effectively on the hook for all of the hardware and services needed to deliver a capability to the end customer.

This means that everything from the ground terminal to the bandwidth needed would be included in the managed service.

It's a system that has become increasingly popular in the satellite industry and that could begin to make its way more into the military and government space.

That being said, it's clear that ground terminals are, and will continue to be, a challenge and area of focus for global militaries and the approach to acquiring ground terminals will most likely change. However, that was not the only change in acquisition that was a topic at this show.

U.S. Air Force Space Command is taking over the procurement of satellite communications — and that's big news.

Air Force Space Command is poised and ready to take on a big responsibility that was originally owned by the ***Defense Information Systems Agency*** (DISA) — the acquisition of commercial satellite services for the entire *Department of Defense* (DoD).

The impetus for this change has a lot to do with concerns about the speed of acquisitions and if operator's needs are being met.

The feeling is that this change in acquisition authority will help make necessary COMSATCOM services more readily available to the military at the speed of war.

Another change that could be precipitated by this interesting shift in acquisition authority is a move away from ***Lowest Price Technically Acceptable*** (LPTA) contracting —— which bought satellite service based on its price — making it much like a commodity.

With Air Force Space Command at the helm, there is an expected shift towards more innovative acquisition models and a movement to award contracts by more criteria than just cost.

While this change is certainly a positive step for the government, it wasn't the only change that was floated to the acquisition process during Global MilSatCom…

U.S. Air Force satellite communications buyers would like to see commercial vendors team up into a consortium.

While the above shift is on the government side, there was also a proposed change to the industry side of the acquisition equation.

Due to concerns about vendor lock-in and terminal interoperability, militaries have been reticent to embrace the "*satellite as a managed service*" model that was discussed above.

In an attempt to make it more palatable to the government, some speakers at the show came up with a somewhat interesting proposal — team up.

Tom Becht, the interim director of the military satellite communications directorate at the ***U.S. Air Force Space and Missile Systems Center*** (SMC), called for industry leaders to team up in a consortium that could offer satellite services across companies and constellations to the military as a unit.

There is certainly some uncertainty as to how "*open*" satellite companies would be toward this kind of tag team, but it certainly is a new and innovative approach to satellite acquisitions.

This article first appeared on GovSat. To read additional, informative articles, please visit ***ses-gs.com/govsat/#***

Ryan Schradin is the Executive Editor of GovSat Report. A communications expert and journalist with more than a decade of experience, Ryan has edited and contributed to multiple popular online trade publications focused on the satellite, unified communications and network infrastructure industries.

In addition to editing content and establishing editorial direction, Ryan also contributes articles about satellite news and trends, and also conducts both written and podcast interviews for the GovSat Report. Ryan also contributes to the publication's industry event and conference coverage, providing in-depth reporting from leading satellite shows. Ryan is a Senior Columnist for MilsatMagazine.

THERMAL MANAGEMENT...

In high performance RF and microwave PCBs

By John Priday, Chief Technical Officer, Teledyne Labtech

As new RF and microwave systems evolve, we are seeing a greater need for effective thermal management and significantly higher RF performance from Printed Circuit Boards (PCB's) and subsystems; at the same time these systems are required to decrease in mass and still offer greater functionality than ever before.

Constraints such as these are often most acute in applications where ***Size, Weight and Power*** (SWaP) are high priorities, such as military and aerospace, and typically include RF power amplifiers and phased array TxRx modules.

This article reviews the various methods of thermal management and reviews in detail the advantages of "***Coin***" technology versus traditional thermal via technology.

High density active power devices, such as GaN power transistors, can dissipate significant heat. One of many roles that the PCB has to perform is to channel heat from the underside of the semiconductor device through to the chosen heatsinking scheme as efficiently and effectively as possible.

The design challenge is how best to accomplish this while achieving the other trade- offs required such as RF performance, manufacturability and cost.

Methods of Thermal Management

Traditionally, designers have simply added *plated through holes* (PTHs) to thermal/ ground pads under components to take heat away through the circuit to a thermal sink such as a cold wall.

Unless the assembly process includes a step to pre-fill these PTHs with solder, there is a high risk that solder will be robbed from under the component into the holes leading to a poor and potentially unreliable connection.

Another solution often used is to have these PTHs under the components filled with a proprietary via plugging paste and plated over the top to give an uninterrupted ground pad.

The plugging pastes typically used are electrically non-conductive and offer a relatively low thermal conductivity of around 0.6 W/mK compared to a conductivity of copper of 400 W/mK, so do not contribute much to the thermal transfer.

Electrically and thermally conductive paste, for example silver (Ag) loaded epoxy, can be used to fill the thermal PTHs but even with Ag epoxy the thermal conductivity of these pastes is typically in the range of 4 to 30 W/ mK depending upon type — still very low. (***See figure 1a***) shows an example of a cross section though a filled and over- plated via. (***See Figure 1b***) shows a typical application with filled thermal vias within the ground pad. Look closely and you will notice subtle outlines of the thermal vias in the central large ground pad.

To improve thermal conductivity, one option is to increase the plated wall thickness of the PTHs from the standard 25um, to 100um, for example. Often a greater number of smaller PTHs within a ground pad can provide a more effective thermal path than fewer larger PTHs.

There are limits to the effectiveness of heat transfer using a traditional ground pad with PTHs.

Figure 2 on the next page shows the results of calculations of four different cases, with detailed calculations shown in *Appendix 1*.

Starting with a typical case of PTHs with 0.1 mm thickness of wall plating[1], it examines the overall thermal conductance with vias filled with a non-conductive filler (***see Figure 2a***).

Using this as the base case, it then examines increasing the number of vias (***see Figure 2b***), then changes the filling from non-conductive to conductive silver epoxy of two different thermal conductivities (***Figure 2c and d***).

As can be seen, the benefit of using Ag epoxy instead of standard, non-conductive plug paste to fill the vias is limited and generally not worth the additional expense.

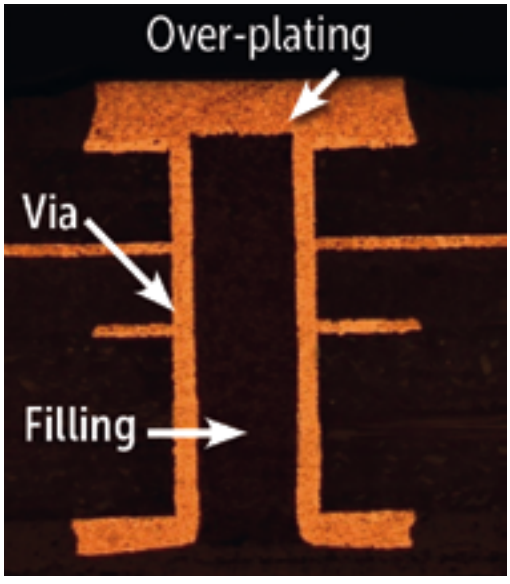


Figure 1a. Cross-section of filled via.

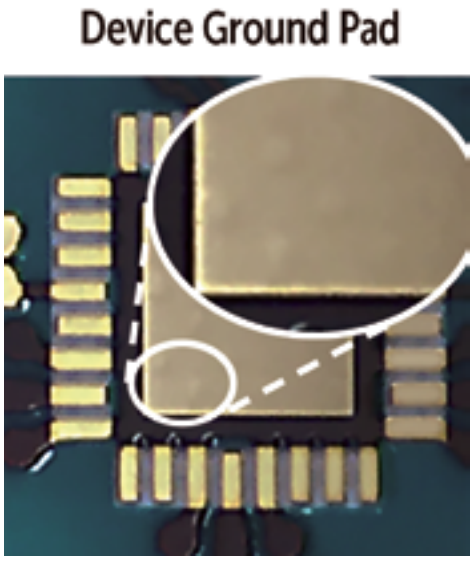


Figure 1b. Photo of typical device ground pad with over-plated vias just visible

[1]*While a through-hole wall thickness of 0.025mm is standard in non-thermally challenged applications, we usually recommend 0.1mm where heat transfer is important. Note that if standard 0.025mm plating was used for case 2a, then thermal conductance would only be 0.96 W/°C.*

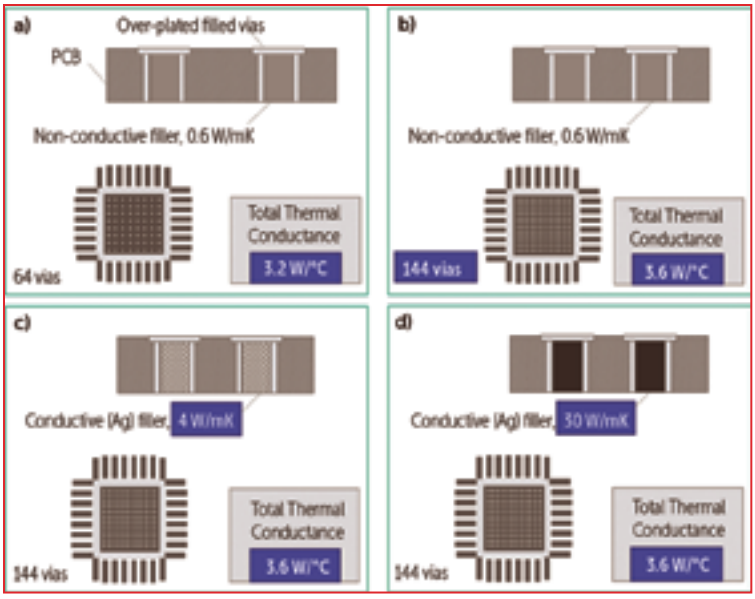


Figure 2: Comparison of total thermal conductance of different filled vias

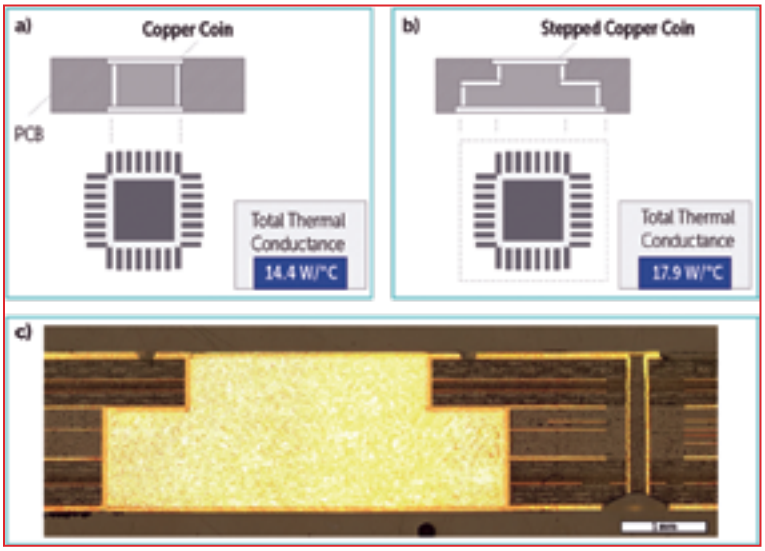


Figure 3: Examples of the use of copper coins

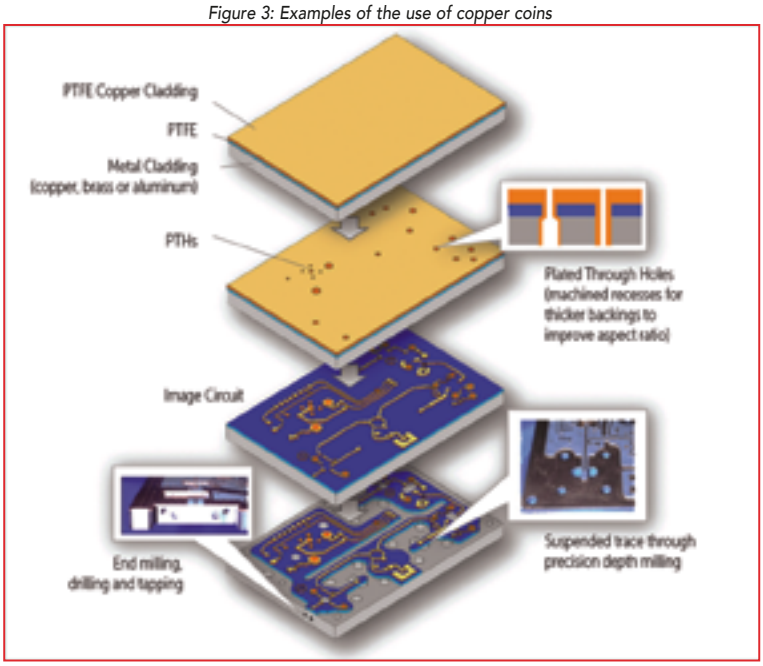


Figure 4: construction of metal-backed circuits.

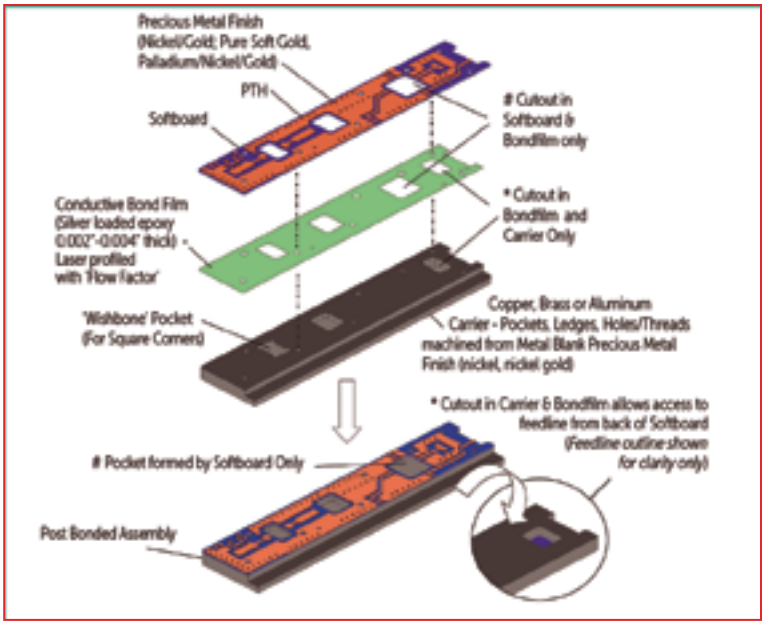


Figure 5: The assembly of post-bonded circuits.

For many leading edge applications the total thermal conductances shown on previous page are not up to the task. A more effective approach is to use copper coins that are integrated into the circuit's structure.

For ease of comparison, a simple approach is shown in (***see Figure 3a***), where a 6mm x 6mm square coin is modeled. A more frequently used approach is to have the coin stepped so that heat is not only efficiently conducted away but also spread.

This is modeled in (*Figure 3b*), and a cross sectional photograph of a real stepped copper coin shown in (*Figure 3c*). The larger area of copper provides a larger surface area in contact with the cold wall, providing improved thermal transfer. More calculations are given in *Appendix 2*. Ultimately metal backed circuits offer an ideal solution where large amounts of thermal energy need to be dissipated, as shown in *Figure 4*.

The metal backing can be copper, aluminum or brass as this type of circuit is typically used for solid state power amplifiers (SSPA) and can be of either pre-bonded or post bonded structure.

In the case of pre-bonded circuits this is where the substrate is supplied pre-bonded to a thick metal backer. This does limit tracking to a single layer and presents issues during processing as invariably machining operations have to take place after the circuit traces have been formed.

Great care needs to be taken to avoid damaging critical circuit features. The advantage is that this provides an excellent ground plane reference.

The post bonded alternative is easier to manufacture in so much as the circuit is produced and verified before being attached to a pre-machined and plated metal backer as shown in *Figure 5*.

Post bonded circuits can have more than a single layer of conductors. Generally the circuit is bonded to the metal backer using a conductive adhesive layer.

For both pre- and post-bonded circuits the components that require heat to be transferred away are mounted directly onto the metal backer through openings within the circuit.

A more complex solution is metal-cored circuits. These can be usefully employed where space is limited and high isolation between RF and control is required in addition to thermal management. Heat being transferred from components to the core can either be through thermal vias or by direct contact through cavities within the circuit that the components are mounted on.

Consideration must be given to removing heat from the core. Typically circuit substrate is machined away from two edges to expose the core so it may be clamped within the chassis to transfer heat.

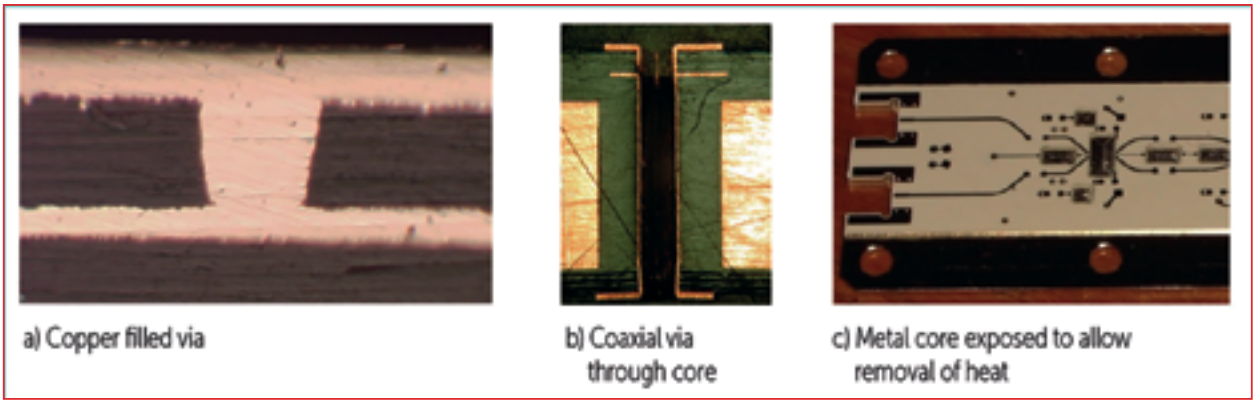


Figure 6: Examples of metal-cored circuits.

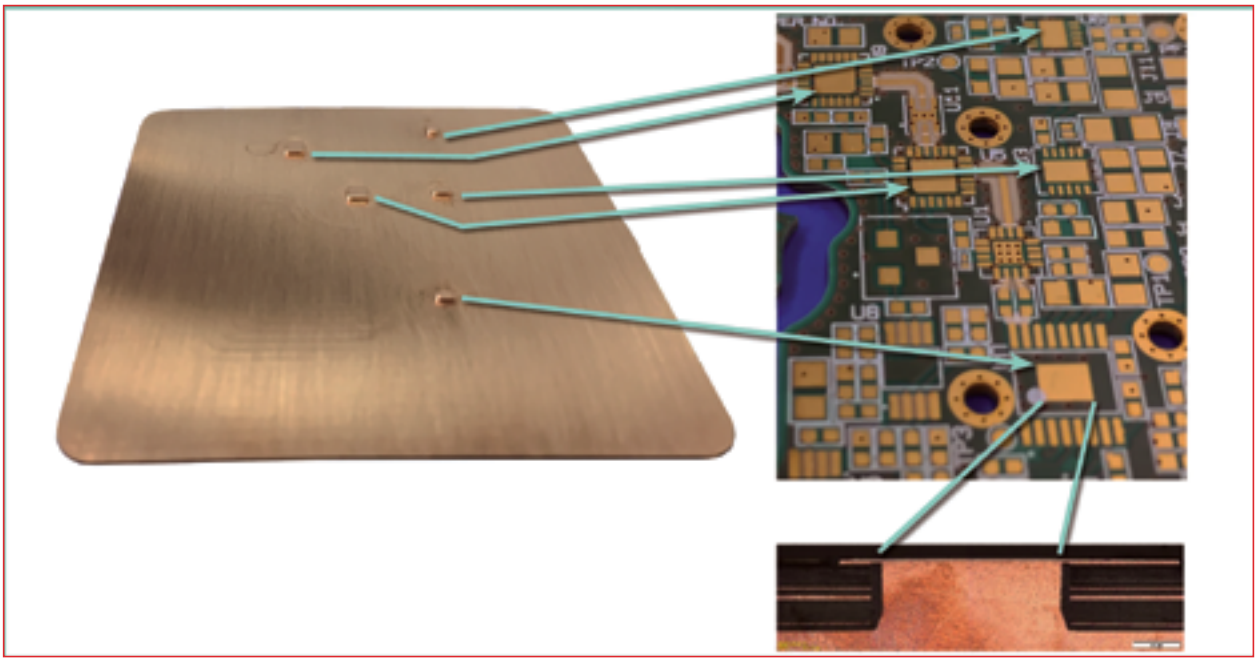


Figure 7: Machined copper plane with up-stands, applicable for small circuits.

In the case of thermal vias where holes are blind with diameters <0.2mm and depths <0.3mm the holes can be filled with copper using a blind hole plating process. *Figure 6* shows examples.

Another technique developed by Teledyne Labtech for thermal management on small circuits (<25cm2) and where the overall thickness is limited, yet several devices require thermal management is to employ a machined copper plane with up-stands (pillars). This provides an excellent thermal path way and the heat can be distributed efficiently through the thermal plane for transmission to a cold wall. An example is shown in *Figure 7*.

Summary

For very high power applications, metal backed circuits currently offer the best solution for high power solid state RF devices that are flange mounted; they do not cater well for SMT components requiring thermal management.

Where SMT components with high dissipation requirements are used, coins provide an effective solution for thermal management.

If the required power dissipation is lower, thick walled filled vias offer a lower cost alternative to coins.

Metal core and machined copper planes are generally only employed where space is limited and cost is not the overriding factor. There are thermally conductive substrates available for RF applications but even these generally have rather modest thermal conductivity of typically 1.0 to 1.5 W/mK

For additional information, or for inquiries regarding a specific application, please email ***ptn_sales@teledyne.com***.

www.teledynedefelec.com

Appendix 1 – Modelled PTHs

The following simplified calculations relate to Figure 2.

a) Thermal Vias assuming non-conductive filler

Drill @	0.500	
Plate through with	0.100	
Via Length	1.000	mm
Pitch	0.700	
Area for thermal vias	6.000	long
	6.000	wide
Number vias	64.000	
Total area of copper through vias	8.042	mm^2
Thermal conductivity of Cu	400	W/m.K
Non-conductive filler	0.6	W/m.K
Total area of epoxy in vias	4.524	
Thermal resistance copper Rth=L/kA	0.311	°C/W
Thermal resistance Epoxy Rth=L/kA	368.414	°C/W
Total Thermal resistance	**0.311**	°C/W
Total Thermal conductance	3.220	W/ °C

b) Thermal Vias assuming non-conductive filler

Drill @	0.300	
Plate through with	0.100	
Via Length	1.000	mm
Pitch	0.500	
Area for thermal vias	6.000	long
	6.000	wide
Number vias	144.000	
Total area of copper through vias	9.048	mm^2
Thermal conductivity of Cu	400	W/m.K
Non-conductive filler	0.6	W/m.K
Total area of epoxy in vias	1.131	
Thermal resistance copper Rth=L/kA	0.276	°C/W
Thermal resistance Epoxy Rth=L/kA	1473.657	°C/W
Total Thermal resistance	**0.276**	°C/W
Total Thermal conductance	3.620	W/ °C

c) Thermal Vias assuming conductive filler 4W/mK

Drill @	0.300	
Plate through with	0.100	
Via Length	1.000	mm
Pitch	0.500	
Area for thermal vias	6.000	long
	6.000	wide
Number vias	144.000	
Total area of copper through vias	9.048	mm^2
Thermal conductivity of Cu	400	W/m.K
Thermal filler Ag epoxy	4.0	W/m.K
Total area of Ag epoxy in vias	1.131	
Thermal resistance copper Rth=L/kA	0.276	°C/W
Thermal resistance Ag Epoxy Rth=L/kA	221.049	°C/W
Total Thermal resistance	**0.276**	°C/W
Total Thermal conductance	3.624	W/ °C

d) Thermal Vias assuming conductive filler 30W/mK

Drill @	0.300	
Plate through with	0.100	
Via Length	1.000	mm
Pitch	0.500	
Area for thermal vias	6.000	long
	6.000	wide
Number vias	144.000	
Total area of copper through vias	9.048	mm^2
Thermal conductivity of Cu	400	W/m.K
Thermal filler Ag epoxy	30.0	W/m.K
Total area of Ag epoxy in vias	1.131	
Thermal resistance copper Rth=L/kA	0.276	°C/W
Thermal resistance Ag Epoxy Rth=L/kA	29.473	o°C/W
Total Thermal resistance	**0.274**	°C/W
Total Thermal conductance	3.653	W/ °C

Appendix 2 – Modelled Copper Coins

The following simplified calculations relate to Figure 3.

a) Solid Copper Coin non-stepped

Dimensions of coin	6.000	long
	6.000	wide
Thickness of coin	1.000	mm
Total area of copper coin	36.000	mm^2
Thermal conductivity of Cu	400	W/m.K
Total Thermal resistance Rth=L/kA	**0.069**	°C/W
Total Thermal conductance	**14.400**	W/°C

b) Solid Copper Coin stepped

Dimensions of coin Top	6.000	long
	6.000	wide
Thickness of coin to step	0.300	mm
Area of copper coin Top	36.000	mm^2
Thermal resistance Top Rth=L/kA	**0.021**	°C/W
Dimensions of coin Base	8	long
	8	wide
Tickness of Base	0.7	mm
Area of copper coin Base	64.000	mm^2
Thermal resistance Base1 Rth=L/kA	**0.035**	°C/W
Thermal conductivity of Cu	400	W/m.K
Total Thermal resistance	0.056	°C/W
Total Thermal conductance	17.910	W/ °C

*Assumes only 50% of increased base area is effective (50mm^2)

AI FOR AFRICA: OPPORTUNITIES FOR GOVERNMENT

An opportunity for growth, development and democratization

The rapidly developing set of Artificial Intelligence (AI) technologies has the potential to solve some of the most pressing challenges that impact Sub-Saharan Africa and drive growth and development in core sectors:

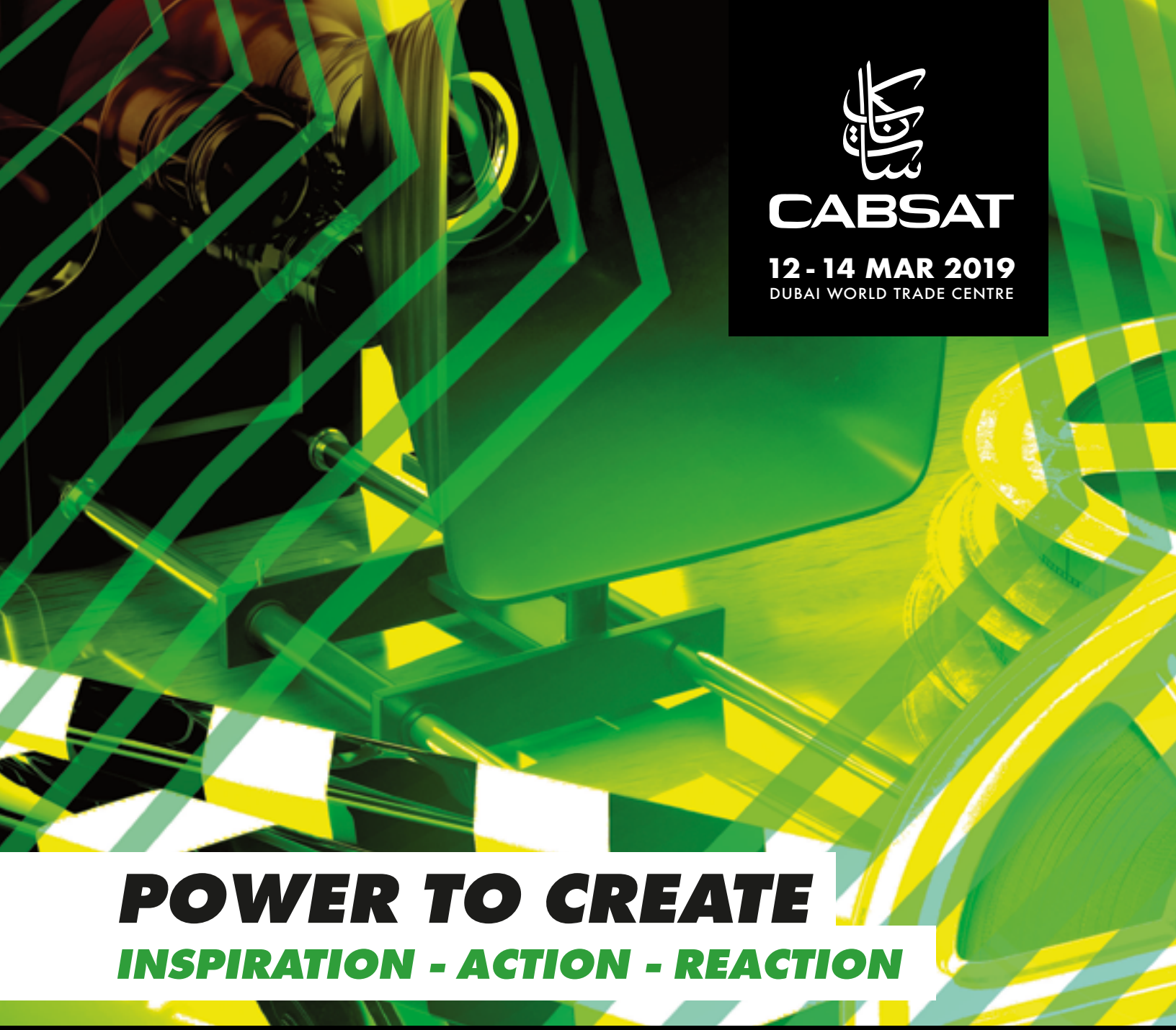
- *Agriculture will be done more efficiently and effectively, raising yields.*
- *Healthcare will be better tailored, higher quality, and more accessible, improving outcomes.*
- *Public services will be more efficient and more responsive to citizens, enhancing impact.*
- *Financial services will be more secure and reach more citizens who need them, expanding access.*

Forward thinking policy-makers, innovative startups, global technology partners, civil society groups, and international global stakeholders are already mobilizing to promote the growth of a vibrant AI ecosystem in Africa.

However, there remain structural challenges that can hamper the development of a healthy AI ecosystem in Africa:

- *Education systems will need to adapt quickly, and new frameworks need to be created for workers and citizens to develop the skills they need to thrive.*
- *Broadband coverage will need to expand rapidly — specifically in rural areas — in order for all citizens and businesses to reap the benefits.*
- *Ethical implications regarding the fair, secure, and inclusive use of AI applications also must be addressed through collaboration and engagement to ensure AI systems earn trust.*

- *Ensuring a deeper, broader, and more accessible pool of data is available will also be key to enable researchers, developers, and users to drive AI.*
- *As with other transformative and revolutionary technologies, there are challenges inherent in the development of AI.*
- *Governments can embrace these challenges and benefit from AI by creating clear roadmaps to guide the adoption of this technology.*
- *They should recalibrate their laws and legal frameworks to support data-driven technologies and innovation-*



CABSAT

12 - 14 MAR 2019
DUBAI WORLD TRADE CENTRE

POWER TO CREATE

INSPIRATION - ACTION - REACTION

25TH EDITION LEADING THE NEW WAVE OF BROADCAST ENTERTAINMENT

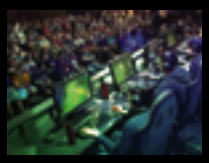
The global broadcast and media industry is scrambling for consumer attention in a recalibrated digital world, so how will you stay ahead? Find out at the leading event for broadcast, satellite, digital media and film - CABSAT 2019!

- Content Creation
- Content Production & Post-Production
- Content Delivery & Distribution

LIVE THE FULL BROADCAST & TECH EVOLUTION IN REAL-TIME

- Digital & Over The Top (OTT) Technologies
- E-Sports Pavillion
- GVF Satellite Hub Summit
- Global Networking & Meetings Programmes
- Photography Workshops





IF YOU'RE IN FILM, TV, AUDIO, SATELLITE, DIGITAL MEDIA, PHOTOGRAPHY OR E-SPORTS, YOU'VE GOT TO BE AT CABSAT 2019!

Organised by
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

REGISTER TODAY TO VISIT AT WWW.CABSAT.COM

FOLLOW US **@cabsatofficial #cabsat #cabsat2019**

driven growth; strengthen the supporting infrastructure for development; and set the tone of a collaborative approach that allows all stakeholders to share their expertise, insights, and build trust.

- *With the correct mix of policies, Africa and its citizens can reap the benefits of the transformations in the years to come.*

The following information is excerpted from the ***Artificial Intelligence for Africa*** whitepaper, with permission from the authors at **Access Partnership**.

The entire, informative paper that discusses the opportunities and challenges for AI in Africa may be downloaded at this direct link: ***www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf***

Government (Public Services) citizens' experience with public services can often be challenging. Delivery is characterized by backlogs; redundant tasks; lack of accuracy; slow response times; and generally poor quality, which leads to low levels of citizen satisfaction.

Governments' ability to ensure efficient use of resources in the delivery of public services is impaired due to factors such as corruption and lack of transparency, as well as public service delivery modes that struggle to respond to present day needs. Thus, while delivery of public services commonly accounts for a large proportion of government budgets, increased spending is often not matched by improvements in outcomes.

Through automation, AI technologies can significantly streamline process es and reduce costs: it can ease administrative burdens, paperwork, and backlogs, increasing public sector efficiency and the speed at which public services can be delivered. This will allow public sector managers to resolve resource allocation constraints, redirecting the staff where they can be most productive.[1]

In addition to making the delivery of existing services more efficient, AI will drive innovation, enabling new and better types of public services. AI's predictive capabilities are a game - changer for how government services and policies can respond to society's needs: from pre-emptive social service interventions to help children and struggling students to better crime reporting and emergency response.

AI tools can also better administer infrastructure, anticipating the need for repairs and better managing cyberattacks that threaten critical systems.[2]

Finally, AI tools will enhance citizen participation. They can provide new platforms for citizens to assess the quality, adequacy, and effectiveness of public services as well as express their needs and preferences. This provides government with more information to improve their services and make more informed policy decisions.[3]

African governments could help demonstrate AI's potential benefits and foster public trust in the technology.[4] Governments can also help the development of the local AI industry by seeking solutions that use AI to address various governmental needs and thereby creating demand of this technology.

AI Solutions for Government

Spatial Wave

The **Microsoft *CityNext* Partner** designed ***SANSTAR*** for the *Los Angeles Bureau of Sanitation* (LASAN) using Microsoft ***Azure*** cloud services.

The smartphone application is used by truck drivers to map and record their daily routes and by citizens to report clean-up issues. The mobile app allows drivers to complete their routes faster and respond to more customer requests.[5]

Veritone

This platform enables federal, state , and local government agencies in the United States to seamlessly and automatically process, transform, and analyze their data. The discovery of mission-critical information is expedited across content silos by cognitively processing and searching for faces, objects, spoken words, logos and more.[6]

Many governments in Africa have begun to take steps to promote AI in their countries:

The government of Nigeria has taken steps to promote partnerships and stakeholder engagement towards leveraging AI's benefits. The **Ministry of Science and Technology** has announced the formation of a *National Agency for Research in Robotics and Artificial Intelligence* (NARRAI).[7]

The new institute will collaborate with international research bodies, enhance instruction on AI topics for thousands of students, and promote Nigeria's ability to leverage these technologies for economic growth. In March 2018, Minister of Communications ***Adebayo Shittu*** also restated his ministry's commitment to support AI stakeholders, engage in conversations to manage and explore the implications of AI, and share best practices.[8]

Kenya was the first African country to launch an open-data portal to make information on education, energy, health, population, poverty, and water and sanitation, which was previously very hard to access, available to citizens.[9]

Application development in Kenya is high, and the government wanted to support the industry's growth. The open-data portal was created in response to requests for data by local tech incubators and co-working facilities for Nairobi programmers, such as ***iHub***[10], which led the government to recognize that access to public datasets is crucial for developing locally relevant AI solutions and services. So far, data from this governmental portal has been key in the development of about 100 apps.

The *South African Department of Trade and Industry* formed a *Chief Directorate for Future Industrial Production and Technologies* (FIP&T) in 2017 to examine the impacts of emerging digital technologies, including the Internet of Things, big data, AI, robotics, and new materials.

The unit aims to build government capacity to address these challenges and partner with industry to enhance South Africa's readiness.[11] Science and Technology Minister ***Mmamoloko Kubayi-Ngubane*** has also said that the government aims to boost its investment in research and development, support for entrepreneurs, and skills development[12].

Reaching All Citizens

AI depends on high quality broadband. This creates an obvious problem for Africa: given the continent's many connectivity challenges, people must be brought online before they can fully leverage the benefits of AI.

There are an estimated 267 million individuals not using the Internet in Africa, and approximately 53 million households[13]. Within these numbers, there are substantial

inequalities: while approximately 22 percent of urban populations have access to the Internet, this number falls to just 10 percent for rural populations. There are also similar divides between men and women, the youth and mature populations, and upper versus lower income groups[14]. Without sufficient connectivity, entire regions will be excluded from all that this technology can to offer.

The inter-related issues of insufficient infrastructure and lack of affordability are the key obstacles. An estimated 30 percent of Sub-Saharan Africa's population is beyond the reach of even the backbone network, let alone last mile links to access the Internet[15].

African countries also have the most expensive broadband in the world. According to the ***Alliance for Affordable Internet*** (A4AI), the first gigabyte of mobile data cost 9.3 percent of the average income in 2016, compared to 3.7 percent for Latin America and 2.5 percent for Asia. Of the 59 developing countries studied, African countries occupied 9 of the 10 lowest slots regarding affordability, with costs ranging from 12 percent to 44 percent of income[16].

Governments should seek to develop and implement policies to enhance connectivity and affordability. This is especially urgent in rural areas, where the lack of broadband is most pressing, but also where applications in the agricultural sector have significant potential.

While in some cases public support and direct investment may be needed, private investment is critical to ensure adequate infrastructure is in place and should be encouraged.

Enabling new wireless technologies may also be an important piece of the puzzle to connect users as quickly and cheaply as possible, bypassing in some cases expensive terrestrial infrastructure.

Government's should improve the accuracy of data they collect and share in key sectors — for example, with the use of technology (such as cloud computing) by national statistical agencies to improve efficiency in the gathering, structuring and analysis of data. However, policies must also encourage the private sector and civil society to do the same.

Governments can help support this by encouraging voluntary adherence to industry standards for data that facilitate interoperability of data sets, promoting data publishing principles (for example Sir ***Tim Berners-Lee***'s *'five-star maturity model'*[17] and incentivizing automated collection and sharing of certain non-proprietary data by the private sector.[18]

Encouraging data sharing platforms, for example for publicly funded academic and scientific research institutions, will also help deepen the pool of data available to all stakeholders.

Regulatory and Policy Framework

Policy can be a powerful tool for African governments to promote technological development by encouraging innovation and investment. At the same time, as leading countries have shown, government engagement and experimentation with nascent technology can also be a powerful signal of trust and support local companies. According to African stakeholders, low government engagement, particularly at the policy level, has been a hindrance, and a stronger focus will encourage an early adoption of AI.[19]

African governments should take a proactive approach and implement AI-friendly regulation, policies, and initiatives. There are several areas relevant to the development and AI and robust digital economies where policy - makers should focus:

- *Data privacy and security — A data privacy and security framework that individuals can trust encourages and empowers them to use AI-based solutions that require their data to work. Data privacy and security laws should aim to protect users' data without restricting the ability to move data across borders. In drafting these laws, African regulators should look to learn from international best practice, which includes avoiding burdensome requirements which would foreclose the benefits of AI and put African companies at a disadvantage.*

- *Cybersecurity — African governments should adopt cybersecurity laws that provide for meaningful deterrence, incentivize investment, clarify legal responsibilities, and create effective and reasonable enforcement mechanisms. Additionally, authorities should help users understand and properly manage the risks inherent in using AI technology.*

- *Digital strategies and cloud adoption initiatives — Governments should develop national digital strategies and policies that foster widespread cloud adoption to democratize the use of advanced technologies.*

- *Intellectual property — Intellectual property laws that provide for clear protection and enforcement against misappropriation and infringement of technological developments, including proprietary algorithms, are indispensable to promote continued innovation and advancement in AI.*

- *Procurement policies — Public procurement regulations should enable the use of AI solutions for the provision of public services. By investing in public sector innovation, African governments will demonstrate their trust in AI and support the growth of local developers.*

- *Industry-led standards and international harmonization of rules — IT organizations worldwide are developing international standards to ensure data portability, interoperability, and a smooth data flow. African governments should remain abreast of developments in this area and seek t o adopt international standards and harmonization rules as they become applicable.*

By drawing from international best practice, African governments can develop national strategies and create a flourishing legal environment for AI. Leading actors — both other governments and the private sector — have valuable experiences to share regarding the advantages, uses and risks of AI, as well as policy approaches they have taken to address challenges and create an environment to fully benefit from this technology.

Creating a Collaborative Environment

Following the example of leading countries in AI, African governments should increase cooperation and exchange of information between diverse stakeholders: academia; industry (including startups and entrepreneurs), civil society (including NGOs and think tanks); policymakers and regulators. These actors must work together — not in silos.

Such a collaborative approach encourages the sharing of expertise and perspective on AI. African government can gain a deeper understanding on the technology and rely on international best practice to address specific local and regional needs. This approach ensures that policy and regulatory action protects citizens and supports the technology's development.

Governments worldwide are concerned about the major intellectual, technological, political, ethical, and social questions that will arise as AI become deeply integrated into our lives.[20] Local, national, regional, and international collaboration can address these concerns as governments share knowledge and experience.

Collaboration is as much an orientation towards openness as it is a specific policy program. African governments can pursue many types of measures to foster the local and regional AI industry, including:

- *Integrate national and regional AI Councils with leading figures from industry, academia and government to advise on the development of AI strategies and oversee their implementation.*
- *Adopt open data initiatives as a way of using technology to support distributed innovation, and to make AI development more participatory and transparent.[21]*
- *Develop frameworks that enable government and industry to work together in technology projects, including public-private partnerships.*
- *Create national and regional "AI labs" that gather top researchers and thought leaders working in the development of the technology as well as on its implications for policy and law-making purposes.[22]*
- *Adopt policies in partnership with universities and the private sector to attract and retain people with AI skills.*
- *For example, African governments could:*
  - » *Work with industry and academia to develop and run specialized fellowships and programs (such as Masters in AI) that prepare the national workforce to respond to businesses current and future skills needs.*
  - » *Create incentives for industry to fund educational programs at all levels, from basic skills to masters and doctoral programmes.*
  - » *Consider modifications to visa allowances to allow foreign nationals to work in jobs in science and digital technology.[23]*
  - » *Work with other stakeholders to organise networking events that allow experts to share knowledge and collaboration across countries. Some countries in the region are already doing this, such as Nigeria (Data Science Lagos), Kenya (Data Science Nairobi) and South Africa (Machine Intelligence Institute of Africa).[22] These will also be key to ensure Africa's young, ambitious, and entrepreneurial-minded population find what they need in Africa, rather than go to other countries to achieve their goals.*
- *Consider joining international initiatives and partnerships that gather experts in the field and thought leaders to contribute to the development of AI for the benefit of humanity (such as Partnership On AI[24] or City.AI).[25]*

AI for Good

AI can drive both economic and social progress and help countries achieve national objectives like inclusive growth and development. But to achieve this, the technology must be developed in a way that is human-centred. African governments should consider the wider impacts of AI and implement policies accordingly. Responsible AI systems must be aligned with ethical values while empowering consumers.

There is a role for policy in ensuring that data and algorithms are used responsibly, and governments should support the collaborative development of codes of conduct by many stakeholders. Such codes should be cross-sector and based on shared, consensus principles. A recent report of the UK House of Lords suggests some principles that can form such a basis:

> *i. AI should be developed for the common good and benefit of humanity*
>
> *ii. AI should operate on principles of intelligibility and fairness*
>
> *iii. AI should not be used to diminish the data rights or privacy of individuals, families or communities*
>
> *iv. all citizens should have the right to be educated to enable them to flourish mentally, emotionally and economically alongside artificial intelligence*
>
> *v. the autonomous power to hurt, destroy or deceive human beings should never be vested in artificial intelligence.[26]*

Further, governments should ensure that transparency, liability, accountability, justification, and redress for decisions are at the heart of the development and application of AI. These principles are essential to foster trust in AI and ensure its true potential can be realised by all.

This is in line with the African Union's aspirations set in Agenda 2063 to build an Africa whose development is people driven, relying on the potential offered by people, especially its women and youth and caring for children.[27]

Artificial intelligence is an important opportunity for the continent of Africa. If governments can successfully navigate the challenges, AI can be a driver of growth, development, and democratisation. It has the potential to enhance productivity growth by expanding opportunities in key sectors for Africa's development, including agriculture, healthcare, financial services, and government services.

By empowering them with access to high-quality digital tools, AI will equip workers, entrepreneurs, and businesses compete at a global level and be at the forefront of economic transformation.

However, the obstacles in the way require serious policy responses. AI will mean substantial adjustments for workers and business and opens new ethical questions that require thoughtful responses.

Labor and ethical questions are compounded by higher hurdles specific to Africa, stemming from gaps in connectivity, the readiness of education systems, and the availability of digital data.

Africa needs to take decisive steps to overcome its unique challenges, but if it can, it has the opportunity to catch up to those countries that have already taken steps to advance AI.

These efforts will not be easy, but the path forward is clear. Success will depend on the ability of governments to foster collaboration among all stakeholders — state and civil society, academia, industry, and national and international stakeholders.

If the challenges and opportunities of AI are embraced, Africa will reap the benefits of a vibrant AI ecosystem.

Download the entire, informative whitepaper to learn more about the opportunities and challenges for AI in Africa at this direct link: www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf

References

[1]*If used effectively, AI can lead to important savings in public money. For example, in the UK, just the use of AI virtual agents across Government departments and the public sector is expected to save an estimated £4 billion a year. For more information, see techUK – Written evidence (AIC0203):* ***data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/artificial-intelligence-committee/artificial-intelligence/written/70492.html***

[2]*Hila Mehr, Artificial Intelligence for Citizen Services and Government (****ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf****), Harvard Kennedy School, ASH Centre for Democratic Governance and Innovation, 2017*

[3]*Dina Ringlod, Citizens and Service Delivery: Assessing the Use of Social Accountability Approaches in Human Development Sectors, December 2011, The World Bank.*

[4]*The report also notes that the big challenge for these countries — and globally — is scarcity of AI developer talent. Governments need to re - think education for a future workplace redefined by AI and start building a healthy, collaborative, and open AI ecosystem to attract and retain competitive AI talent. According to a report by IDC, spending on cognitive and AI systems in the Middle East and Africa (MEA) region will reach USD 114.22 million by 2021, with the market expected to represent a compound annual growth rate of 32 percent for the 2017 to- 2021 period*

[5]*For more information on SANSTAR, see the Microsoft website (****customers.microsoft.com/en-us/story/la-improves-sanitation-services-with-a-cloud-based-spatially-enabled-mobile-solution****).*

[6]*For more information on Veritone, visit the company website at* ***www.veritone.com/ai-solutions/government/***

[7]*For more information on NADER and NARRAI, see the Federal Ministry of Science and Technology website:* ***scienceandtech.gov.ng/2018/08/01/fg-to-establish-two-new-agencies/***

[8]*For more information on Nigeria's commitment to support AI, see the Federal Ministry of Communications website located at:* ***www.commtech.gov.ng/news-and-media/daily-news-report/187-shittu-charges-private-sector-to-lead-in-artificial-intelligence.html***

[9]*Kenya OpenData. Kenya has also signed on to the Open Government Partnership:* ***www.opengovpartnership.org/***

[10]*For more information on iHub, see the iHub website:* ***ihub.co.ke/***

[11]*For more information on South Africa's AI program, see Department of Trade and Industry website:* ***www.dti.gov.za/industrial_development/fipt.jsp***

[12]*For more information on South Africa's investments, see the government website:* ***www.gov.za/speeches/minister-mmamoloko-kubayi-ngubane-netrepreneurs-rise-africa%20percentE2%20percent80%20percent99s-digital-lions-workshop-8-aug***

[13]*Philbeck, "Working Together to Connect the World by 2020: Reinforcing Connectivity Initiatives for Universal and Affordable Access, Broadband Commission, p.8*

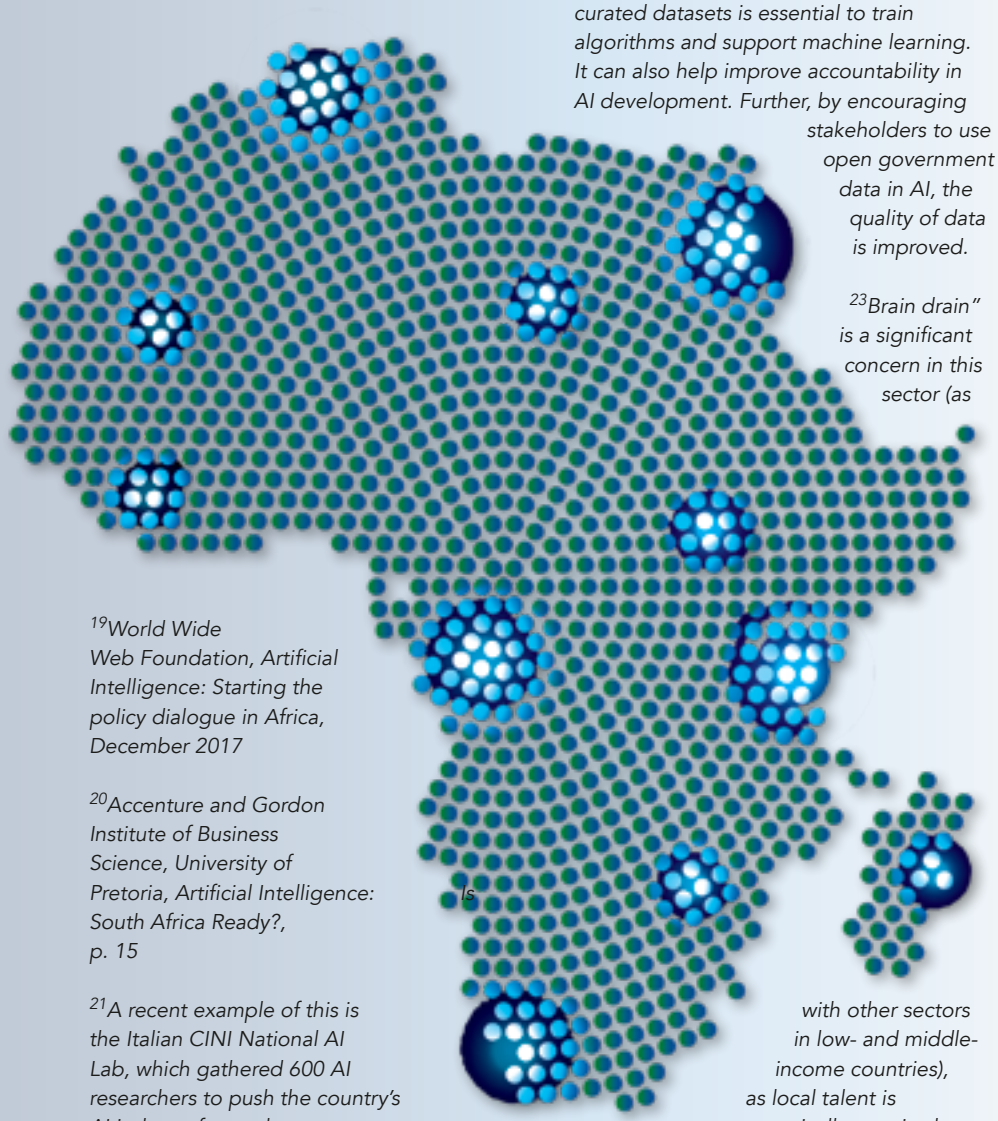
[14]*"World Development Report 2016: Digital Dividends," World Bank, 2016, p. 9*

[15]*J.M. Garcia and T. Kelly, "The Economic and Policy Implications of Infrastructure Sharing and Mutualisation in Africa," World Bank Group, p.16*

[16]*For more information on New Broadband Pricing Data, see A4AI website:* ***https://a4ai.org/broadband-pricing-data-2017/***

[17]*Tim Berners-Lee. 2009. Linked Data (****www.w3.org/DesignIssues/LinkedData.html****) ("Five Stars").*

[18]*For additional recommendations targeted to the agricultural sector, see Global Open Data for Agriculture and Nutrition (GODAN), "A Global Data Ecosystem for Agriculture and Food," August 2016, at* ***https://www.godan.info/sites/default/files/documents/Godan_Global_Data_Ecosystem_Publication_lowres.pdf***



[19]World Wide Web Foundation, Artificial Intelligence: Starting the policy dialogue in Africa, December 2017

[20]Accenture and Gordon Institute of Business Science, University of Pretoria, Artificial Intelligence: South Africa Ready?, p. 15

[21]A recent example of this is the Italian CINI National AI Lab, which gathered 600 AI researchers to push the country's AI industry forward.

[22]Access to free, open, and anonymized, curated datasets is essential to train algorithms and support machine learning. It can also help improve accountability in AI development. Further, by encouraging stakeholders to use open government data in AI, the quality of data is improved.

[23]Brain drain" is a significant concern in this sector (as is with other sectors in low- and middle-income countries), as local talent is systematically recruited by large U.S. and European companies working on AI, including Google, Facebook, and Apple. World Wide Web Foundation, Artificial Intelligence: Starting the policy dialogue in Africa, December 2017

[24]Partnership on AI: **https://www.partnershiponai.org/partners/**

[25]City.AI. For more information on the Tech in Ghana Conference, see event website at **http://techinghanaconference.com/#overview**

[26]Austin Clark, "Government 'must play central role in AI development'" (**www.govtechleaders.com/2018/04/16/government-must-play-central-role-in-ai-development/**), GovTech Leaders, 16 April 2018.

[27]The Agenda 2063 (**au.int/en/agenda2063**) is a strategic framework for the socio-economic transformation of the continent over the next 50 years. Its builds on, and seeks to accelerate the implementation of past and existing continental initiatives for growth and sustainable development.

Excerpts from this paper are courtesy of Access Partnership and are published with their permission.

Access Partnership is a leading public policy firm that provides market access for technology. The company monitors and analyzes global trends for the risks and opportunities they create for technology businesses and identify strategies to mitigate those risks and drive the opportunities to our clients' advantage.

The company's team mixes policy and technical expertise to optimize outcomes for companies operating at the intersection of technology, data and connectivity.

www.accesspartnership.com/artificial-intelligence-for-africa-an-opportunity-for-growth-development-and-democratisation/

TOGETHER

We Will Define the Future of Space!

Top Global Space Networking Event of the Year

The Latest Space Technologies

Featured Targeted Tracks

- Cyber 1.9 Classified
- New Generation Space Leaders
- Tech Track
- Space Law

Global Space Leaders

James Bridenstine
Administrator
NASA

VADM Brian B. Brown, USN
Commander
Naval Information Forces
U.S. Navy

Prof. Dr. Pascale Ehrenfreund
Chair of the Executive Board
German Aerospace Center (DLR)

Gen. David L. Goldfein, USAF
Chief of Staff
U.S. Air Force

Gen. John W. "Jay" Raymond, USAF
Commander
Air Force Space Command

35TH SPACE SYMPOSIUM
SPACE FOUNDATION

The Broadmoor Hotel, Colorado Springs, Colorado USA

Join Us April 8 - 11, 2019!

Official Media Partner
satnews
Satellite News · SatMagazine · MilsatMagazine

Register Today – There's Still Time to Save! • SpaceSymposium.org • +1.800.691.4000