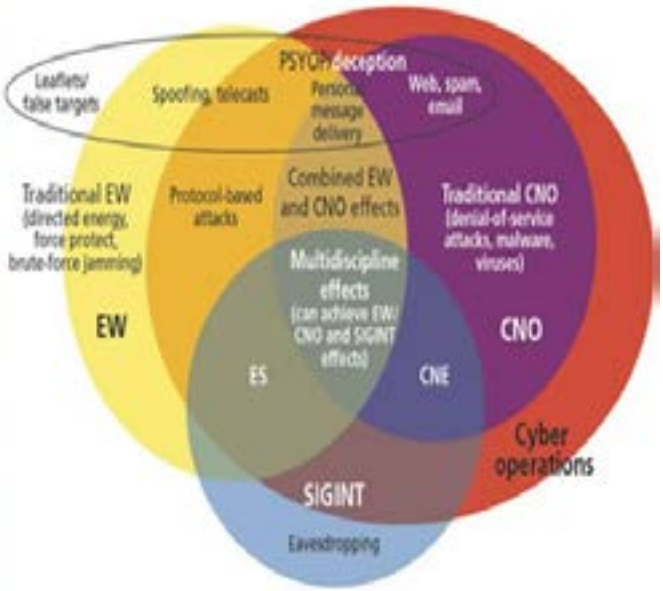
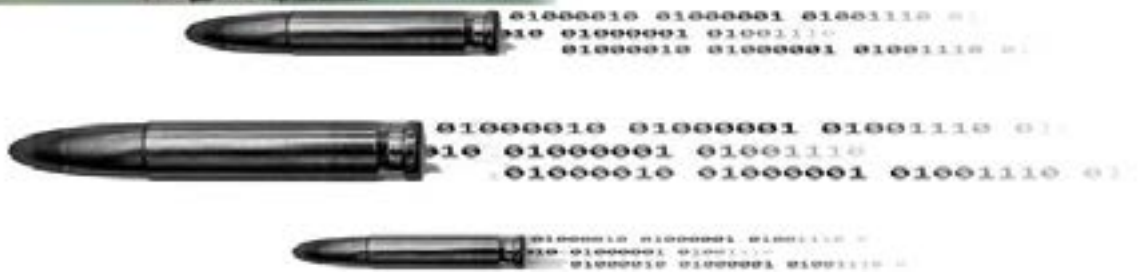
Cyber, Communications, EW & Technology (C2ET) Digest

By Maj Gen P K Mallick, VSM (Retd)





Website : http://www.strategicstudyindia.com/
https://indianstrategicknowledgeonline.com/

PUBLISHED BY STRATEGIC STUDY INDIA

Contents

CYBER

China-Russia links in cyberspace are a source of concern, says America's top cyber warrior

General Paul Nakasone, the head of the US Cyber Command and director of the National Security Agency, told The Straits Times that "What we see with both China and Russia is a close association of being able to share information." Interactions between China and Russia have been under sharper scrutiny since US Secretary of State Antony Blinken said in February that Chinese firms were already providing "non-lethal, dual-use-type support" to Russia. China has flatly denied any weapons deals with Russia

Source: https://www.strategicstudyindia.com/2023/04/china-russia-links-in-cyberspace-are.html

Chinese State-sponsored Hacking Group Highly Active

Insikt Group, a private American cybersecurity firm, said it found evidence that A Chinese hacking group RedGolf that is likely state-sponsored and has been linked previously to attacks on U.S. state government computers is still "highly active" in a wide range of countries and industries, "targeting aviation, automotive, education, government, media, information technology and religious organizations."

Following up on previous reports of APT41 and BARIUM activities and monitoring the targets that were attacked, Insikt Group said it had identified a cluster of domains and infrastructure "highly likely used across multiple campaigns by RedGolf" over the past two years.

Source: https://www.strategicstudyindia.com/2023/04/report-chinese-state-sponsored-hacking_037188147.html

Secret trove offers rare look into Russian cyberwar ambitions

An anonymous person provided the documents from the contractor, NTC Vulkan. The documents detail a suite of computer programs and databases that would allow Russia's intelligence agencies and hacking groups to better find vulnerabilities, coordinate attacks and control online activity. The documents suggest the firm was supporting operations including both social media disinformation and training to remotely disrupt real-world targets, such as sea, air and rail control systems.

The cache of more than 5,000 pages of documents, dated between 2016 and 2021, includes manuals, technical specification sheets and other details for software that Vulkan designed for the Russian military and intelligence establishment. It also includes internal company emails, financial records and contracts that show both the ambition of Russia's cyber operations and the breadth of the work Moscow has been outsourcing.

Officials from five Western intelligence agencies and several independent cybersecurity companies said they believe the documents are authentic, after reviewing excerpts at the request of The Washington Post and several partner news organizations.

Source: https://www.strategicstudyindia.com/2023/04/secret-trove-offers-rare-look-into.html

Yes, TikTok is a threat to America. But so are U.S. social media companies.

The difficult question of to ban or not to ban confronts the U.S. government as it struggles to figure out how to handle TikTok, the wildly popular Chinese social media platform that has at least 150 million active users in the United States.

Most of the complaints about TikTok — that it is harmful to children, that it spreads misinformation and that it collects private data — are just as applicable to U.S. competitors. For example, Facebook, the company now known as Meta that also owns Instagram, agreed in 2019 to pay a record $5 billion fine after the Federal Trade Commission alleged that it violated users' privacy. Facebook was also used by Russian trolls to influence the 2016 election. Now Meta has been quietly lobbying to turn the public against TikTok, because Instagram and Facebook have been losing ground to TikTok, especially among teens.

FBI Director Christopher A. Wray has also raised "national security concerns" about TikTok: "They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so chose, or to control software on millions of devices, which gives it an opportuni-

ty to potentially technically compromise personal devices."

Source: https://www.strategicstudyindia.com/2023/04/yes-tiktok-is-threat-to-america-but-so.html

Hackers probing contractors for path to Pentagon, DISA chief says

Lt. Gen. Robert Skinner, Director of the Defense Information Systems Agency on March 29 told Congress **that hackers backed by China, Russia and other adversaries are applying "very high" levels of effort to digitally infiltrate,** surveil and make off with plans or intelligence closely held by suppliers to the Department of Defense.

"Some of them see the defense industrial base as a soft underbelly," In October, the National Security Agency, FBI and other federal entities said hackers managed to infiltrate a defense industrial base organization, maintain "persistent, long-term" access to its network and abscond with sensitive data. Years prior, Chinese-sponsored cyberattacks breached a Navy contractor's computers, jeopardizing info tied to secret work on an anti-ship missile, Defense News reported.

Source: https://www.strategicstudyindia.com/2023/04/hackers-probing-contractors-for-path-to.html

Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences

Despite expectations to the contrary, cyber defence, not offence, has been the story of Russia's war against Ukraine as it enters its second year. Shattering concepts of offence dominance, Kyiv's cyber-defensive effort has shown that a strong and layered cyber defence can be mounted against a well-resourced and highly capable adversary.

Careful examination of the available evidence would suggest that the primary lessons lie less in what Ukraine has done and more generally in its superior capacity to adjust to various aspects of Russia's cyber offensive. Institutional adaptations such as legislative change in Ukraine and measures taken to garner public- and private-sector support have driven much of Kyiv's defensive success.

Kyiv has deftly marshalled its defensive resources and orchestrated diverse forms of external support to stem the Russian cyber offensive. However, concerns of 'fatigue' setting in are just as consequential to Ukraine's cyber defence as they are in other domains of war. Competing priorities or emerging crises elsewhere in the world could divert attention and resources away from the Ukraine front. Changing economic conditions could also stem crucial private-sector support for Ukraine's cyber defence.

Source: https://www.strategicstudyindia.com/2023/04/russias-war-in-ukraine-examining.html

From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point

The third quarter of 2022 marked a turning point in cyber-attacks related to the conflict in Ukraine, with a clear transition from a cyber-war focused on Ukraine and Russia to a high-intensity hybrid cyber-war across Europe. The cyber-war is targeting Poland and the Baltic and Nordic countries in particular, with an increasing focus on critical national infrastructure in sectors including aviation, energy, healthcare, banking and public services.

At the very beginning of the conflict, the majority of incidents only affected Ukraine (50.4% in the first quarter of 2022 versus 28.6% in the third quarter), but EU countries have seen a sharp increase in conflict-related incidents in the last six months (9.8% versus 46.5% of global attacks).

Pierre-Yves Jolivet, VP Cyber Solutions, Thales said: "Cyber is now a crucial weapon in the arsenal of new instruments of war, alongside disinformation, manipulation of public opinion, economic warfare, sabotage and guerrilla tactics. With the lateralisation of the conflict from Ukraine to the rest of Europe, Western Europe should be wary of possible attacks on critical infrastructure in the short term if the conflict continues to accelerate."

Source: https://www.strategicstudyindia.com/2023/04/from-ukraine-to-whole-of-europe-cyber.html

US military needs 7th branch just for cyber, current and former leaders say

A national association of current and former military digital security leaders is calling on Congress to establish a separate cyber service, arguing that the lack of one creates an "unnecessary risk" to U.S. national security.

"For over a decade, each service has taken their own approach to providing United States Cyber Command forces to employ and the predictable results remain inconsistent readiness and effectiveness," according to the group, which boasts around 3,700 members.

Only a service, with all its trappings, can provide the level of focus needed to achieve optimal results in their given domain. Cyberspace, being highly contested and increasingly so, is the only domain of conflict without an aligned service. How much longer will our citizenry endure this unnecessary risk?

The creation of a Cyber Force would follow the arrival of the Space Force in 2019.

Source: https://www.strategicstudyindia.com/2023/03/us-military-needs-7th-branch-just-for.html

What cyber attack risks do the railways face?

The European Union Agency for Cybersecurity (ENISA) finds in its first cyber threat landscape report dedicated to the transport sector that DDoS attacks have increased in the past year, mainly targeting railways, and ransomware is the most common type of cyber attacks. The majority of the attacks observed in railway targeted the IT systems of railways, relating to passenger services, ticketing systems, mobile applications and display boards, for example. These caused some disruptions due to the unavailability of these services, but mostly did not cause train operations itself to be shut down.

The report makes clear that there are different types of cyber attacks that can negatively impact railways, and they are likely to increase, warns ENISA. The agency deems that the significant increase in hacktivist activity, and the increasing rate of DDoS attacks are highly likely to continue. Though currently, most cyber attacks had little impact on train services itself, it also foresees that ransomware groups will likely target and disrupt Operational Technology (OT) systems in the foreseeable future, partly due to the ongoing digital transformation in the transport sector and the increased connectivity between IT and OT networks.

Source: https://www.strategicstudyindia.com/2023/03/what-cyber-attack-risks-do-railways-face.html#more

Ukraine War Shows Difficulty of Large-Scale Cyberattacks, NSA Director Says

National Security Agency Director Gen. Paul Nakasone said, U.S. adversaries have become more capable of carrying out sophisticated cyberattacks, but the Ukraine war shows how difficult it is to conduct large-scale operations against critical infrastructure. America's rivals are seeking ways to penetrate business and government networks, databases and weapons systems. Large cyberattacks need synchronizing, intelligence, tools and the capacity to carry them out. "If you don't have one of those elements, then I think as we saw in February and beyond, it's been much more difficult for the Russians to operate in this domain of cyberspace,"

Source: https://www.strategicstudyindia.com/2023/03/ukraine-war-shows-difficulty-of-large.html

The 'Clop' Gang's Latest Ransomware Spree May Have Hit More Than 100 Targets

A vulnerability in file transfer software from Fortra known as GoAnywhere has been repeatedly exploited by the notorious, Russia-based Clop ransomware group to target dozens or possibly more than a hundred victims in recent days. The cybercrminal group has added entries on numerous organizations to its dark web site, where Clop attempts to extort money from victims by publishing samples of data they've stolen and threatening to leak more if targets don't pay.

TechCrunch confirmed that the City of Toronto is one of the victims of the spree. TechCrunch has also uncovered details about problems with Fortra's response to the discovery of the vulnerability.

Source: https://www.strategicstudyindia.com/2023/03/security-news-this-week-india-shut-down.html

At least 50 U.S. government employees targeted with phone spyware overseas

At least 50 U.S. government employees in at least 10 countries overseas have had their mobile phones targeted with commercial spyware, a number that is expected to grow as the investigation continues.

The revelation comes as the White House announces a new executive order to ban the use by the U.S.

government of commercial spyware that poses a risk to national security and human rights. The order follows in the wake of a long-running controversy over the misuse of a powerful spyware, Pegasus, by foreign governments to hack journalists, rights activists and dissidents around the world. It also comes as the administration this week co-hosts the second global Summit for Democracy.

In late 2021, Apple alerted roughly a dozen U.S. Embassy employees in Uganda that their iPhones had been hacked using Pegasus, military-grade spyware developed by NSO Group, an Israel-based company with government clients in dozens of countries. The tool allows its users to steal digital files, eavesdrop on conversations and track the movements of targets — often activated through "zero-click" malware that doesn't even require the target to click on a link.

But the latest figure of at least 50 government employees shocked the Biden administration. The effort to identify additional targeted personnel continues. Measures were being taken to mitigate the risks posed by the tools.

The executive order comes more than a year after the Commerce Department placed NSO Group on a trade blacklist known as the Entity List, a significant move that barred export of any hardware or software from the United States to NSO, choking off a vital source of technology and sending a signal to would-be investors.

The order bars federal agencies from using commercial spyware if it has been used to hack or target U.S. government devices or personnel — or if it has been used to abuse human rights, such as by targeting dissidents. It applies to spyware built by foreign or American companies, a measure to avoid creating a "perverse incentive" for companies to relocate to the United States to bypass restrictions, the official said.

There's an exception for spyware that might be needed for helping U.S. agencies develop defensive cyber measures or testing countermeasures to defeat hackers.

Source: https://www.strategicstudyindia.com/2023/03/at-least-50-us-government-employees.html

Military Organizations in Pakistan Targeted With Sophisticated Espionage Tool

Tracked as NewsPenguin, the adversary has been observed sending phishing emails that use the upcoming Pakistan International Maritime Expo & Conference (PIMEC-2023) as bait and which carry weaponized documents to deliver an advanced espionage tool.

Running February 10-12, PIMEC is an initiative of the Pakistani Navy that helps private and public organizations showcase products and develop relationships.

NewsPenguin's malicious documents, which pose as an exhibitor manual that appears to target PIMEC visitors, carry embedded Visual Basic for Applications (VBA) macros to execute malware. Once opened, the lure document uses a remote template injection technique to fetch the next stage from a remote server that only serves the payload to Pakistani IP addresses.

The researchers discovered that the malware waits five minutes between commands, likely another attempt to bypass sandboxes, which typically have a time limit of fewer than five minutes per sample. Based on received commands, the malware collects and sends information about the machine, runs an additional thread, copies or moves files, deletes files, creates directories, sends the content of files to the server, executes files, and uploads or downloads files from the server.

The threat actor's targets include military technology companies, nation-states, and military organizations in Pakistan, including PIMEC organizers, exhibitors, and visitors.

Source: https://www.securityweek.com/military-organizations-in-pakistan-targeted-with-sophisticated-espionage-tool/

Phishing Campaign Targets Chinese Nuclear Energy Industry

Intezer has been tracking activity targeting the energy sector and noted a campaign with techniques that align with those of Bitter APT, operating in the Asia-Pacific region. Bitter APT is a South Asian threat group that commonly targets energy and government sectors; they have been known to target Pakistan, China, Bangladesh, and Saudi Arabia.

We have made the connection to Bitter APT through tactics, techniques, and procedures (TTPs) that have been observed in other publications, such as

the use of Microsoft Office exploits through Excel files, and the use of CHM and Windows Installer (MSI) files. Bitter APT are continuing to target organizations in China in an espionage campaign. For some of the payloads we have corresponding phishing emails that were used as lures to deliver the files, allowing analysis of the social engineering techniques used.

Bitter APT have been conducting espionage campaigns for years using many tactics, including phishing, to achieve their goals. It is advised that entities in government, energy, and engineering especially those in the Asia-Pacific region should remain vigilant when receiving emails, especially those claiming to be from other diplomatic entities. None of the social engineering techniques used are novel and it is imperative that employees of companies should have a good standard of security awareness about phishing emails.

Source: https://www.intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/

Google Rolls Out Its Bard Chatbot to Battle ChatGPT

GOOGLE ISN'T USED to playing catch-up in either artificial intelligence or search, but today the company is hustling to show that it hasn't lost its edge. It's starting the rollout of a chatbot called Bard to do battle with the sensationally popular ChatGPT.

Bard, like ChatGPT, will respond to questions about and discuss an almost inexhaustible range of subjects with what sometimes seems like humanlike understanding.

Eli Collins, a vice president of research at Google working on Bard said "Bard's an early experiment, it's not perfect, and it's gonna get things wrong occasionally."

Google says early users of Bard have found it a useful aid for generating ideas or text. Collins also acknowledges that some have successfully got it to misbehave, although he did not specify how or exactly what restrictions Google has tried to place on the bot.

Bard and ChatGPT show enormous potential and flexibility but are also unpredictable and still at an early stage of development. That presents a conundrum for companies hoping to gain an edge in advancing and harnessing the technology. For a company like Google with large established products, the challenge is particularly difficult.

Both the chatbots use powerful AI models that predict the words that should follow a given sentence based on statistical patterns gleaned from enormous amounts of text training data. This turns out to be an incredibly effective way of mimicking human responses to questions, but it means that the algorithms will sometimes make up, or "hallucinate," facts—a serious problem when a bot is supposed to be helping users find information or search the web.

ChatGPT-style bots can also regurgitate biases or language found in the darker corners of their training data, for example around race, gender, and age. They also tend to reflect back the way a user addresses them, causing them to readily act as if they have emotions and to be vulnerable to being nudged into saying strange and inappropriate things.

Collins of Google says one reason the company is launching Bard now, when the bot is far from perfect, is because of the valuable data generated when people interact with the system. OpenAI and Microsoft already have that streaming in after their own launches. "Human feedback is a really important part of why we're launching Bard," Collins says. "We want to broaden [it] beyond what we've gotten internally."

"Google's core existence has been threatened by Microsoft." Tools like Bard may improve dramatically in the coming years, what Google is gambling that it won't suffer reputational damage in the short term when Bard gets things wrong. "People may no longer take it for granted that Google is always right," he says. "It's very tricky for them."

Source: https://www.strategicstudyindia.com/2023/03/google-rolls-out-its-bard-chatbot-to.html

'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, say experts

It is one of China's most popular shopping apps, selling clothing, groceries and just about everything else under the sun to more than 750 million users a month. But it can also bypass users'

cell phone security to monitor activities on other apps, check notifications, read private messages and change settings. And once installed, it's tough to remove.

Pinduoduo, which boasts a user base that accounts for three quarters of China's online population and a market value three times that of eBay (EBAY), wasn't always an online shopping behemoth. Founded in 2015 in Shanghai by Colin Huang, a former Google employee, the startup was fighting to establish itself in a market long dominated by e-commerce stalwarts Alibaba (BABA) and JD.com (JD).

It succeeded by offering steep discounts on friends-and-family group buying orders and focusing on lower-income rural areas.

While many apps collect vast troves of user data, sometimes without explicit consent, experts say e-commerce giant Pinduoduo has taken violations of privacy and data security to the next level. Multiple experts identified the presence of malware on the Pinduoduo app that exploited vulnerabilities in Android operating systems. Company insiders said the exploits were utilized to spy on users and competitors, allegedly to boost sales.

Evidence of sophisticated malware in the Pinduoduo app comes amid intense scrutiny of Chinese-developed apps like TikTok over concerns about data security. The revelations are also likely to draw more attention to Pinduoduo's international sister app, Temu, which is topping US download charts and fast expanding in other Western markets. Both are owned by Nasdaq-listed PDD, a multinational company with roots in China.

There is no evidence that Pinduoduo has handed data to the Chinese government. But as Beijing enjoys significant leverage over businesses under its jurisdiction, there are concerns from US lawmakers that any company operating in China could be forced to cooperate with a broad range of security activities.

PDD didn't reply to CNN's repeated requests for comment on the team.

Sergey Toshin, the founder of Oversecured, said Pinduoduo's malware specifically targeted different Android-based operating systems, including those used by Samsung, Huawei, Xiaomi and Oppo. Toshin described Pinduoduo as "the most dangerous malware" ever found among mainstream apps.

Toshin found Pinduoduo to have exploited about 50 Android system vulnerabilities. Most of the exploits were tailor made for customized parts known as the original equipment manufacturer (OEM) code, which tends to be audited less often than AOSP and is therefore more prone to vulnerabilities.

Source: https://www.strategicstudyindia.com/2023/04/ive-never-seen-anything-like-this-one.html

Uncovering the unheard: Researchers reveal inaudible remote cyber-attacks on voice assistant devices

Guenevere Chen, an associate professor in the UTSA Department of Electrical and Computer Engineering, recently published a paper on USENIX Security 2023 that demonstrates a novel inaudible voice trojan attack to exploit vulnerabilities of smart device microphones and voice assistants — like Siri, Google Assistant, Alexa or Amazon's Echo and Microsoft Cortana — and provide defense mechanisms for users.

The researchers developed Near-Ultrasound Inaudible Trojan, or NUIT (French for "nighttime") to study how hackers exploit speakers and attack voice assistants remotely and silently through the internet.

The researchers used NUIT to attack different types of smart devices from smart phones to smart home devices. The results of their demonstrations show that NUIT is effective in maliciously controlling the voice interfaces of popular tech products and that those tech products, despite being on the market, have vulnerabilities

Source: https://www.strategicstudyindia.com/2023/03/uncovering-unheard-researchers-reveal.html

COMMUNICATIONS

Opportunities and Risks of 5G Military Use in Europe

The fifth-generation (5G) technology standard for broadband cellular communications is expanding and will offer many more capabilities than the existing fourth generation long-term evolution standard. With this increase in capabilities comes opportunities for the U.S. Department of Defense (DoD) to integrate advanced technologies and improved communications into its operations. However, these opportunities come with inherent risks.

The trajectory of 5G in Russia is uncertain because of the hesitation of the Russian military to give up its rights to the contested 3.4 to 3.8 GHz bandRussia's 5G regulatory problems pose a challenge for such countries as Lithuania that are trying to cultivate 5G networks. North Atlantic Treaty Organization (NATO) governments feel the need to abide by international agreements governing spectrum usage in peacetime, and NATO militaries cannot take advantage of 5G infrastructure that remains unbuilt because of regulatory conflicts with the Russians.

If 5G technologies play some role in a conflict with Russia, Russia will attempt to counter 5G technologies in accordance with Russia's well-cultivated, holistic approach to radioelectronic struggle (radioelektronnaia bor'ba) or electronic warfare (EW). If these EW measures prove effective, the electromagnetic spectrum will potentially be a nonpermissive environment for 5G technologies during a conflict with Russia.

Source: https://www.strategicstudyindia.com/2023/03/opportunities-and-risks-of-5g-military.html

China's Approach to Military 5G Networks and Related Military Applications

China's pursuit of 5G technology for geopolitical ends has been well documented. 5G refers to the fifth generation of mobile networking technology. It offers increased data transmission speeds, lower latency, and greater connectivity enabled through the new capabilities that 5G technology brings, including enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine-type communications (mMTC).

China's development and rollout of Huawei 5G networks globally has created supply chain and network security risks for NATO and EU member states. In 2019, Chinese scholars and researchers linked to China's military, hereinafter also the People's Liberation Army (PLA), argued that 5G has 'strong military application value' and advocated for a comprehensive '5G technology development strategy' for military use. China's interest in 5G technologies for dualuse and military ends has advanced beyond mere discussions. The PLA has been working to integrate 5G and next-generation communication networks within its military modernization process. In one 'national defence mobilization' drill, the PLA used mobile 5G net-

works to maintain emergency communications during a network failure scenario. China's defence industry has also developed capabilities for 5Genabled military communications. As China's domestic rollout of 5G networks continues, the PLA and China's defence industry will continue to integrate nextgeneration communication networks to gain a military edge.

China's advancement of 5G for military use has important security implications. Unlike emerging technologies such as quantum technologies that may be years away from widespread military adoption and use, 5G and nextgeneration communication networks are already being developed and implemented by armed forces. 5G is likely to accelerate the adoption of technologies like artificial intelligence (AI) and enable new opportunities to coordinate technological assets on the battlefield. In many ways, 5G-enabled integration of these technologies will define the future of warfighting. As the DoD concluded in 2018, 'Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting'.

Despite the expected role for 5G in future military contexts, there has not yet been a comprehensive analysis of military 5G developments. Discussions of China's emerging and disruptive technologies have focused on AI and other technologies. Comprehensive analyses of China's military capabilities have often left 5G and next-generation communication networks behind. China's pursuit of 5G and next-generation communication networks for national security and military purposes has not yet been explored in detail. China's activities in the rollout of 5G represent a concerted effort to advance its military capabilities, support the mobilization of its armed forces, and compete for technological and military advantage.

This paper describes China's overall approach to 5G and the modernization of its military, contributing to a better understanding of how China's military and domestic security services might leverage 5G capabilities. As a 2020 report from the Brookings Institution explains, President Xi Jinping and other high-level government officials are unlikely to discuss specific technologies, and sensitive topics like the military applications of 5G are not discussed in government documents. No analysis of China's emerging technology sector can capture sensitive or classified activities, such as investments by China's military. Still, this paper aims to present available sources, which may reveal important insights about the current landscape of military 5G within China.

Source: https://www.strategicstudyindia.com/2023/04/chinas-approach-to-military-5g-networks.html

Army network plan will offset contested comms with multi-path transport-agnostic capabilities

A recent Army article quoted US Army Deputy Chief of Staff Lt. Gen. John Morrison as saying: "The Army's Unified Network is the Army's contribution to JADC2, and at the core of the unified network is space." The unified network almost sounds like a concept of operations like Joint All Domain Command and Control. But it's more than that. Describe what is meant by the "unified network."

The two main components of the Unified Network are the Integrated Tactical Network and the Integrated Enterprise Network, ITN and IEN. For ITN, we're fielding kit from the company up through the battalion and brigade to division, with other maneuver type elements sprinkled in.

That's supporting everything from the base band perspective for each of the enclaves that they need to support. We have our own transport network called the Unified Transport Network that is, essentially, colorless. That is what we're using to interconnect all of the DoD teleports, the regional hub nodes. It's the fabric that's stitching all this together. Then there's user enclaves that connect into that transport network.

The flexibility there is to drive toward being transport agnostic, where you can take a unit's base band component and plug it into commercial internet, a commercially provided terminal, or one of the program-of-record terminals that we field. It gives them flexibility to reach into tactical and strategic.

From an Army perspective, there are deliberate gaps from where we came from between those formation types. That puts a lot of complexity down at the user level. It also causes impacts when a unit goes from point A to point B. Depending on where point B is, it could result in them quite frankly having to sometimes even re-image their systems to be able to access the DODIN in that new location.

Where the Army is going is an attempt to converge those networks, both from a technical and policy perspective, so that a soldier using the system at post, camp, and station can also use that same system in a deployed environment. That is the impetus behind the Unified Network approach — common standards and policy. From a hardware perspective, it's routers, switches, encryptors.

What about the importance of space in the Unified Network? As a signaleer, one of your responsibilities is to develop what we call a PACE plan [primary, alternate, contingency, and emergency plans for resilient communications]. A signaleer is going to attempt to maximize all the options available to them, so space and terrestrial are key players.

I wouldn't necessarily prioritize one over the other in the aggregate; you probably would on specific missions where SATCOM would be your primary depending on where you're at. There are other missions where line of sight may be your primary. Other missions where fiber may be your primary. They're all key. Every one of those pathways — whether it be line of sight, beyond line of sight, fiber, host nation, 5G, SATCOM, and LEO, MEO, GEO — are part of this Unified Network approach.

The challenge for us is how we bring all that capacity and capability to the edge, seamlessly and simply. That's the impetus behind where we're going from a Unified Network approach.

Much of the emphasis of JADC2 is on the kill chain and precision fires, with less attention paid to the command and control aspect. How will the Unified Network let leadership not only command but also have control through communications — even in a contested environment?

One of the challenges historically and why there's been this bit of divide, whether artificial or not, between the strategic and the tactical, is the unique use case from a tactical environment that we used to call a DDIL [denied, degraded, intermittent, or limited] or DIL [disconnected, intermittent, limited] environment. You have to be able to operate with challenges to comms at times, whether it's jamming, lack of available fiber, geography impacting your line of sight, or host-nation spectrum restrictions. There are a lot of challenges in the tactical space. You have to create an architecture and a configuration that could mitigate the issues associated with that DIL environment.

As we move forward and start enabling things like cloud capabilities and get after the demand signal for constant transport, it hearkens back to our previous discussion about not putting all of our eggs in one basket. We're going to need all these different pathways.

We talk about PACE, but we need to add some letters at the end of that at some point because of the added links that we're trying to get in there. There's less of an acceptance of having a DIL environment in a tactical space. We have to up our game to enable assured, resilient transport in the tactical space.

It's still a term that's out there. You can have the best SATCOM system in the world but if an adversary puts up a certain type of jammer, you're not getting out. If the fiber gets cut or you've got geography limitations, you're not going to be able to use it.

There are unique challenges in the tactical space that we don't see on the enterprise side with posts, camps, and stations, and unique implementations that we have to pay attention to. Our goal is to give them enough options moving forward from the perspective of capability capacity and link aggregation perspective that we work our way away from that term.

We want to make it so that the soldiers can fight with the network versus fighting the network. They have other things they have to soldier and do. Working around DDIL or other scenarios shouldn't be something they have to worry about.

The challenge that we've given our engineering teams and industry partners is that we want to add all this capability and capacity, but we want you to do it with less kit and keep it simple. It's an opportunity for us to focus our limited resources on capabilities that add to everything that we've been talking about. But it doesn't do us any good if it comes with an extensive amount of training and complexity that soldiers won't be able to install, operate, and maintain.

Source: https://www.strategicstudyindia.com/2023/03/army-network-plan-will-off-set-contested.html

NORTHCOM chief: Homeland defense could be imperiled by commercial spectrum sale

The long-running battle over the Pentagon's hold on a portion of radio frequency spectrum coveted by telecommunications firms heated up. Gen. Glen VanHerck, commander of US Northern Command and the North American Aerospace Defense Command, and in charge of protecting the US homeland told the Senate Armed Services Committee, he is worried about his ability to detect incoming aircraft and missiles if access is lost. He said, "I am concerned about the potential national security impacts of auctioning or selling off that spectrum. It's my assessment there will be impacts, as you pointed, out to our domain awareness capabilities."

He explained,"There are multiple platforms to include maritime homeland defense platforms, airborne early warning platforms, ground-based early warning platforms that enable me to provide threat warning, attack assessment, and defend from potentially airborne assets, etc." that rely on the spectrum under debate.

That spectrum, 3.1-3.45 GHz, currently is allocated for Defense Department usage, primarily by ground-, air- and sea-based radars for detecting airborne and missile threats, in particular, the Navy's Aegis Combat System that is the heart of its ballistic defense capabilities. The Aegis's AN/SPY radar is one of the few US military systems able to track low flying, highly maneuverable hypersonic missiles.

But urged by the telecom industry chafing to develop 5G networks for mobile phones and internet services, the Federal Communications Commission (FCC) — as well as lawmakers are pushing to allow those RF frequencies to be made available to commercial firms. (The FCC regulates commercial spectrum usage inside US territory.)

This could be done by auction, which the FCC has favored for releasing other parts of DoD spectrum for commercial-only use, or by some sort of spectrum sharing scheme between military and commercial users. The telecoms and their supporters are pushing the FCC to be able to auction off the 3.1-3.45 band for commercial use as soon as possible.

While an auction of the segment for commercial use could drive wireless expansion and generate significant revenues, technical experts assert that reallocation of the band from federal to nonfederal use would require complex and high-cost modifications to DOD systems and would affect DOD operations. Aegis radar with one capable of using different frequencies would likely cost $120 billion.

Source: https://breakingdefense.com/2023/03/northcom-chief-homeland-defense-could-be-imperiled-by-commercial-spectrum-sale/

When we talk about what will enable JADC2, we're really talking about the Internet of Warfighting Things

If you think about what JADC2, or Joint All Domain Command and Control, is trying to achieve for the Department of Defense (DoD), it's the Internet of Warfighting Things. The reason I use the term "warfighting" versus "military" is because if you say "military" things what you get is Army, Navy, Air Force, and Marines. That's military.

Here's warfighting. When you go to war, four DoD defense agencies — National Geospatial Intelligence Agency (NGA), Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), and National Security Agency (NSA) — become Combat Support Agencies. They are part of the warfighting mechanism, so you need to include all the capabilities they bring to bear.

Space-based ISR needs to be integrated and accessible to the warfighter during a conflict. That means you need all of those space capabilities directly connected to the warfighter. Thus the Internet of Warfighting Things, not just military things.

We connect things in networks. If you look at a Link 16 network, it allows connectivity amongst a package of fighters. They can talk to each other and pass data but they still can't connect to space or many of the maritime systems. In the past, that would have been called a local area network. We're looking at broadening that to a wide area network where any data generated is available across all the domains: air, land, sea and space.

What's interesting about the Internet of Things is the ubiquity of data accessibility. The key is that the same data is accessible to everybody, but everybody uses it in different ways.

In the end, this is all about data and the movement of data, it's not about changing your platforms. It's about using non-organic data to make your platform more effective and ensuring that data generated by any platform is usable by other platforms.

So when looking at the commercial Internet of Things, cloud services have definitely been one of the key enablers for its success. The ability to not have data isolated on-premise, but to actually have it stored in a cloud for everyone to access has been game-changing. Data tagging will also allow the warfighter to make queries in such a way that if somebody says, "I'm fighting in this front area and I am looking for information on the adversary in these areas," it automatically populates just like it would with a Google search. Robust cloud storage and computing allows for these types of advances.

A combatant commander or any commander down the line always has command authority. It stays with them all the time. What they lack is control. A combatant commander may have a unit he has command authority over, but if he can't talk to them and connect to them, he doesn't have control.

What this Internet of Warfighting Things can do is connect you to everything just like your phone does. In the future, the idea is for commanders to have intimate knowledge over everything they command and have actual accessibility through comms and data to control those elements.

It's almost a duplicate of the Internet of Things. Integrating systems together doesn't mean all the services have to operate under the same CONOPS. If you're a naval vessel with your own CONOPS, a space system can now give you additional information over the horizon that you could normally not have gotten, or an airplane from the Air Force can give you information on the adversary that you could never have gotten organically. That doesn't change your CONOPS. It allows you to execute it more effectively. If Navy decides to do a joint operation with the Air Force and they have access to the same data, it helps them to transform their CONOPS to more effectively operate together when they choose to.

What makes the Internet of Things successful is communications capabilities. With fiber networks everywhere, data can transit to anywhere. With data storage centers like big tech you can access what you need in almost real time. The Space Development Agency is starting to build out what's called the SDA Transport Layer [a satellite constellation of several hundred satellites for assured, resilient, low-latency military data and connectivity worldwide to a range of warfighter platforms]. This comms transport layer in space is a recognition that large data requires robust communications paths.

For the Internet of Warfighting Things to be successful, it will be dependent on building resilient communications through space, air, and land and then ensuring that data is accessible both at the edge and in the rear. Data at the edge is critical for real-time operations. While these data hubs will likely be smaller, they provide real time fused data that's actionable to the warfighter. The balance between pushing data to the edge and pulling data from sources in the rear is a balance that is still being worked out.

Source: https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/

TECHNOLOGY

Pausing AI Developments Isn't Enough. We Need to Shut it All Down

An open letter published today calls for "all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4." The key issue is not "human-competitive" intelligence; it's what happens after AI gets to smarter-than-human intelligence. Key thresholds there may not be obvious, we definitely can't calculate in advance what happens when, and it currently seems imaginable that a research lab would cross critical lines without noticing.

On Feb. 7, Satya Nadella, CEO of Microsoft, publicly gloated that the new Bing would make Google "come out and show that they can dance. I want people to know that we made them dance." This is not how the CEO of Microsoft talks in a sane world. It shows an overwhelming gap between how seriously we are taking the problem, and how seriously we needed to take the problem starting 30 years ago. We are not going to bridge that gap in six months.

Many researchers working on these systems think that we're plunging toward a catastrophe, they think that they can't unilaterally stop the forward plunge, that others will go on even if they personally quit their jobs. And so they all think they might as well keep going. This is a stupid state of affairs, and an undignified way for Earth to die, and the

rest of humanity ought to step in at this point and help the industry solve its collective action problem.

Source: https://www.strategicstudyindia.com/2023/04/pausing-ai-developments-isnt-enough-we.html

Who's Winning the AI Race? It's Not That Simple.

China has long sought to dominate the AI landscape, laying out a plan to become a "global leader" in the sector by 2030 and pledging billions of state dollars for research and development. U.S. breakthroughs have been more organic, illustrated most recently by the rapid global uptake of chatbots made by American companies, such as Google, Microsoft, and OpenAI, with Chinese counterparts largely playing catch-up. Experts caution, however, that applying the "arms race" framework to the development of AI doesn't capture the global dynamics around the technology.

One fundamental distinction is the private sector's role at the forefront of developing new AI capabilities: There were no private-built rockets in the 1960s. During the Cold War, key technological advances in the nuclear and space sectors were characterized by a high barrier to entry and a near-monopoly by the state. AI is characterized by lower barriers to entry, democratized access, and the preponderance of the private sector in driving innovation.

So who's winning the AI race? Multiple rankings in recent years that consider metrics such as investment, talent base, and research—including the number of patents and publications—have the United States leading the field, with China close behind and gaining rapidly, followed by countries such as the United Kingdom, India, and Canada. But that doesn't paint the whole picture. AI isn't just patents but processes.

Source: https://www.strategicstudyindia.com/2023/03/whos-winning-ai-race-its-not-that-simple.html

A Chinese Perspective on the Pitfalls of Military Intelligentization

Intelligentization, also referred to as intelligent warfare, is the Chinese concept of applying machine speed and processing power of artificial intelligence (AI) to military planning, operational command, and decision support. According to an article published in the People's Liberation Army's official newspaper PLA Daily, the rate of developing intelligent weapons and systems is progressing at such a rapid pace, comes with potential risks, According to the article, the anti-jamming ability of current intelligent systems is too weak, making intelligent systems more vulnerable. For example, drone command and control relies on communication links that connect the drones to rear personnel. If the communication link is jammed, the operator will lose control of the drone. Therefore, improved anti-jamming capability is necessary to ensure communications links are not disrupted. The article also explains that the reliability of today's AI technology is questionable.While the AI systems' level of intelligence is superior to that of a human, there is not yet a reliable test to ensure theywill notfail in a complex combat scenario.

The article also warns that using intelligent weapons and equipmentincreases the risk oflosing control in a crisis. Military operations thatrely on intelligent weapons and equipment could surpass the speed of political decision making. This could weaken the decision-maker's ability to control the situation. The use of intelligent weapons and equipment in largescale combat could increase tension between countries as well as lead to changing the psychology of combatants, potentially causing them to become more desensitized to killing because of their greater distance from the battlefield and gradually reducing caution in decision-making.

Countries are increasingly pouring money into AI technology to gain military advantage, and this struggle for predominance could lead to a dangerous arms race. With current AI technology, the algorithms used to distinguish civilians from combatants are not yet reliable, thereby potentially putting the lives of civilians at risk. There is still a long way to go before China has perfected the software to not only drive AI weapons and equipment, but also to test them to ensure they are ready to meet all the demands of the battlefield.

Source: Luo Zhaocheng, "Pay Attention to Risks in Using Intelligentized Weapons and Equipment," PLA Daily (Official newspaper of the Chinese People's Liberation Army), 5 January 2023. http://www.81.cn/ll/2023-01/05/content_10209877.htm

The Age of AI has begun

Bill Gates writes

In my lifetime, I've seen two demonstrations of technology that struck me as revolutionary.

The first time was in 1980, when I was introduced to a graphical user interface—the forerunner of every modern operating system, including Windows. I sat with the person who had shown me the demo, a brilliant programmer named Charles Simonyi, and we immediately started brainstorming about all the things we could do with such a user-friendly approach to computing. Charles eventually joined Microsoft, Windows became the backbone of Microsoft, and the thinking we did after that demo helped set the company's agenda for the next 15 years.

The second big surprise came just last year. I'd been meeting with the team from OpenAI since 2016 and was impressed by their steady progress. In mid-2022, I was so excited about their work that I gave them a challenge: train an artificial intelligence to pass an Advanced Placement biology exam. Make it capable of answering questions that it hasn't been specifically trained for. I thought the challenge would keep them busy for two or three years. They finished it in just a few months.

I knew I had just seen the most important advance in technology since the graphical user interface. This inspired me to think about all the things that AI can achieve in the next five to 10 years.

The development of AI is as fundamental as the creation of the microprocessor, the personal computer, the Internet, and the mobile phone. It will change the way people work, learn, travel, get health care, and communicate with each other. Entire industries will reorient around it. Businesses will distinguish themselves by how well they use it.

Source: https://www.strategicstudyindia.com/2023/03/the-age-of-ai-has-begun.html#more

The Global War Over AI Already Started

AI's role in everyday life is set to increase exponentially and a global war over AI's national security applications is already underway.

China has been swift to react to these American-developed tools' rapid deployment. San Francisco-developed ChatGPT became the fastest-growing consumer app in history, blazing past 100 million users two months after launching. Beijing rapidly clamped down on access to ChatGPT and used state media to release pointed videos about "how the US uses AI to spread disinformation."

In parallel, a whole host of Chinese companies have stepped up their own conversational AI tools. The "Chinese Google," Baidu, said it would unveil its Ernie Bot in March after completing internal testing. Alibaba, China›s e-commerce leader, is also testing its own ChatGPT-style tool, while a plethora of smaller players are rushing to market their own solutions.

As this international AI competition heats up and positive applications for the technology abound, experts are also paying increasing attention to its potential nefarious uses. As the CEO of cyber defense company Check Point Software Gil Shwed underlined, generative AI makes writing malware very easy: "You can go to a tool like ChatGPT, ask it to develop a back-office application that collects information and then write a phishing email from that info that looks perfect. You can do all of that without knowing how to program or having the best English to write those emails." Within two months of its launch, ChatGPT has already been used in several cyberattacks.

While AI-assisted malware is certainly concerning, what remains the most alarming for the West is how artificial intelligence is changing the future of warfare—even faster than expected. The Chinese military has been investing heavily in intelligent warfare, making weapons systems and military operations more networked and autonomous. The People's Republic of China is already incorporating AI into its military strategy, including in autonomous vehicles, intelligence analysis, decision support, electronic warfare and cyber operations.

As the rift between Beijing and the West widens and tensions rise, it should seriously concern Western policymakers that China is among the leaders in AI research and development and uptake for military purposes, on top of its commanding lead in 37 out of 44 key technology fields, from defense to robotics and AI.

Under these circumstances, Brussels and Washington desperately need to step up their own investments into AI and similarly crucial technologies.

AI investment alone, however, won't be enough to stay competitive in this pivotal area—they also need to build the cutting-edge digital infrastructure base upon which AI advances can strive and be effectively implemented.

While security discourse in the West has been dominated over the past year by the more conventional warfare taking place in Ukraine, national security is far more than tanks and fighter jets. With AI becoming increasingly sophisticated and intertwined with our daily lives, the West needs to be prepared—technically and financially—to defend itself on that battlefield as well.

Source: https://www.strategicstudyindia.com/2023/03/the-global-war-over-ai-already-started.html

How to Describe the Future? Large-Language Models and the Future of Military Decision Making

The innovation of the smokeless rifle may not be as flashy as that of the aircraft and armored vehicles, but describing its impacts on the future of war required more than four-hundred pages of technical analysis in Jean de Bloch's The Future of War. A smokeless rifle not only increases visibility on the battlefield, but it also opens new possibilities for tactics and strategy.

Leaders across the world are seeing the early effects of another transformational technology: widely available large-language models.

Viewed as the first step in true artificial general intelligence, large-language models incorporate massive amounts of data from books and articles into training sets that allow them to recognize patterns between words and images. These models appear to be able to answer many questions by generating coherent responses in seconds and can perform menial tasks like summarizing articles or cleaning unstructured data. Across the internet, early adopters have demonstrated novel uses for OpenAI's chatbot, ChatGPT, that range from editing code to writing essays for college courses. These models are well regarded in the private sector, but they have not received much attention in military circles largely because they do not appear to have direct applications for combat. Large-language models will likely have a larger impact on the battlefield than autonomous drones due to their ability to automate the many aspects of staff work that prevent military leaders from focusing on tactics and strategy.

Large-language models will likely have a larger impact on the battlefield than autonomous drones due to their ability to automate the many aspects of staff work that prevent military leaders from focusing on tactics and strategy. The introduction of ubiquitous AI will have far-reaching consequences. The real transformation will occur in the offices that litter the headquarters of every echelon of the military.

The general trends of AI integration into staff functions like intelligence is inevitable. The fear that these models will completely pull humans out of the loop are unfounded; rather, they will create decision-making space by lessening the load of other tasks. These models will automatically create a common operating picture that will keep different staff sections synched even when they are not in face-to-face meetings. The timeline for this integration may be shorter than most analysts may think.

While the immediate effects are clear, the second and third order effects will take time to forecast. The adoption of large-language models by military staff will make war more deadly in ways that may be hard to predict. Yet despite this difficulty, it is necessary to take the time to try to describe the second-order effects of a technology that the world does not quite understand yet.

Source: https://www.strategicstudyindia.com/2023/03/how-to-describe-future-large-language.html

Pentagon, ODNI form 'joint team' to explore risks connected to mobility across cloud networks

Cloud services, which are essentially delivered on-demand via the internet, mark a major enabler of DIA's unfolding pursuit to modernize its legacy, secretive Joint Worldwide Intelligence Communication System, or JWICS, network. Through multi-vendor, multi-award contracts including the Pentagon-wide Joint Warfighting Cloud Capability (JWCC) and the intelligence community's Commercial Cloud Enterprise (C2E), DIA can choose from and is engaging with several large cloud service providers.

DIA is currently working with its various programs

offices to identify "efficiencies, where it makes sense" to set up different cloud access points globally. "It's kind of like a co-location of sorts, where customers can have better access to all of the different services that will be available — that way there is no confusion on having one service over here and another one over there."

DIA officials are aware of and accept risks associated with the agency's complex shift to the cloud.

With the enhanced mobility and more widely available network services DIA envisions in migrating to the cloud, surfacing information-governing issues must also be confronted in the near term.

"It goes beyond just a technical area, but it also goes into governance and policies. As you know, tactical systems have to be mobile, so they have to be able to work anywhere in the world."

However, "if you look at data governance" today, privacy laws differ across the world. This could essentially "mean that if you are in a certain area of a country, the laws in there, locally, mandate that that data can be reviewed by either the local government or someone else. One of the biggest challenges is understanding the policies and the laws that regulate the data at that location — the visibility, the security, and how do we protect it? How do we make sure that that is our data, and then no one else is going to look at it, and that whenever we need it, we can get it back?"

Source: https://www.strategicstudyindia.com/2023/03/pentagon-odni-form-joint-team-to.html

FIND IT, VET IT, SHARE IT: THE US GOVERNMENT'S OPEN-SOURCE INTELLIGENCE PROBLEM AND HOW TO FIX IT

When Russia launched its latest invasion of Ukraine early in the morning of February 24, 2022, we were serving as information operations planners for the US European Command Information Operations and Special Activities Division. Army reservists, we had arrived at EUCOM in September 2021 and soon after were assigned to help develop response plans in case of a Russian invasion. When that invasion occurred, our task shifted to rapidly operationalizing those plans. These efforts included working with interagency partners both before and after the invasion to combat Russian disinformation and help inform international audiences of Russian activities, in what some considered a "ramped up" US information warfare effort.

Throughout this process we routinely faced challenges in maximizing the value of open-source information. More specifically, we encountered problems in three areas: collection, vetting and analysis, and sharing content. We attempted several methods to address these deficiencies, with varying degrees of success, but our experiences laid bare a fundamental truth: better solutions are required to ensure US and ally information warfare capabilities are prepared for future crises.

As the war started, we worked with our partners to establish a method for sharing unvetted, possibly relevant content by email. Partners on the collection side (primarily intelligence organizations) would attach open-source content, tweets, images, or videos to emails; we would forward this content to partners on the messaging side. Then we removed ourselves as intermediaries and created an email distribution list that allowed both sides to directly interact.

The outbreak of the war also brought additional attention and offers of support from other US government and international partners. For this we were grateful, but it highlighted two key points: (1) there was a need for an easy-to-use, shareable content repository and (2) some organizations are unfortunately out of touch or uncomfortable when it comes to open-source content.

Overall, at this early stage, our main finding was the prescience of DoD's 2018 Joint Concept for Operating in the Information Environment. It described the US military as a force "hampered by its policies, conventions, cultural mindsets, and approaches to information," one that had built barriers that inhibit adaptation and synchronized approaches to information warfare. These were precisely the barriers we were running up against.

There is wide agreement, from RAND to the Center for Strategic and International Studies to others who have studied the problem, that improvements need to be made in open-source intelligence. The challenges we outlined above are neither new nor unique to Russia's invasion of Ukraine and the ongoing war.

In terms of open-source intelligence, many small, private organizations outperform US government entities with only a fraction of the funding avail-

able to DoD and the intelligence community. Traditional media organizations, often under the rubric of data journalism, also demonstrate capabilities that exceed those of the government, again with a fraction of the funding of government organizations.

Adapting how we approach open-source intelligence in the way outlined above is neither difficult nor expensive—private organizations conduct these activities cheaply and effectively every day. The signals are clear that changes are necessary. It's time to respond to them.

Source: https://www.strategicstudyindia.com/2023/03/find-it-vet-it-share-it-us-governments.html

How Open-Source Intelligence Is Changing Warfare

Open-source intelligence (OSINT) is the process of using publicly available information and tools to create (usually public) intelligence. While OSINT has been a subject of official study since at least the 1940s, it has become more privatized in the 21st century. Russia's conflict with Ukraine has resulted in a large-scale civilian effort to track Russian activities there and, in particular, to analyze the Russian invasion that began in early 2022. It is important for military professionals and the public to learn about OSINT, the threats it could pose, and how the United States can use this community as an asset for future conflicts.

OSINT is not just the information it produces or its capabilities. Three key "pillars" comprise it:

Data sources. OSINT researchers need data to analyze.

Information aggregation. OSINT researchers need references and places to store information obtained by investigation. They also need to be able to transfer this information to each other.

Communication. To employ "wisdom of the crowd"—the basis of OSINT—researchers need to be able to discuss and debate with one another.

Each pillar is critical. If any is compromised, OSINT cannot be conducted effectively.

OSINT in Ukraine

Before the invasion of Ukraine, researchers paying attention to tweets from Russian accounts showing Russian trains loaded with tanks and armored vehicles. By geolocating these photos and following the train tracks, OSINT researchers quickly identified the size and locations of a massive buildup occurring not just on the Russia-Ukraine border, but along parts of the Belarusian and Moldovan borders as well.

In the opening days of the invasion, Twitter exploded with records of the fighting. Videos emerged of tanks getting hit with rockets, armored vehicles fighting armored vehicles, and bodies in the streets. The OSINT community started to dig in. Researchers started identifying individual vehicles and tracking their status. Twitter users @Girkin-Girkin and @no_itsmyturn identified more than 400 vehicles in the first ten days of the invasion alone. Others began documenting the invasion as a whole.

The Russian government's reaction to the footage coming from Ukraine was to attempt to limit its own people's exposure. Roskomnadzor, Russia's media surveillance department, outright banned Facebook, and later in the year there were reports the agency had limited access to Twitter as well. This attempt at controlling the communication pillar was not very effective. Any citizen using a virtual private network (VPN) could evade the ban, and anonymous services such as Telegram resist limitation by such measures.

This action, however, also limited the distribution of pro-Russian sources, which created a pro-Ukrainian bias regarding what footage was available on social media. Combined with global public opinion, this led to an extremely one-sided OSINT community.

The unified global OSINT effort aimed at a single objective poses a critical question: how can the United States replicate the success of Ukraine and its supporters to ensure the OSINT community advantages the United States in a future conflict?

Controlling OSINT

Many prospective adversaries control certain pillars of OSINT in their countries, leaving them less vulnerable to integral threats posed by OSINT.

Russia. Russia's ability to limit internal communications, at least in part, is an obstacle to effective OSINT.

China. China's strong internal controls over every OSINT pillar makes conducting OSINT very difficult inside the country itself. However, China has little control of these pillars externally, leaving it vulnerable to some OSINT gathered from outside.

The United States. By average monthly users, the top four social media sites are all owned by companies in the United States. This could lead to a belief that the United States can gain control over the communication pillar at a moment's notice. However, if the United States attempted to suppress OSINT activities on these services, the community would be able to shift to others with relative ease.

Thus, it is difficult to argue that the United States has control over any of the OSINT pillars. This makes OSINT a unique threat to the United States relative to its adversaries.

Source: https://www.strategicstudyindia.com/2023/03/how-open-source-intelligence-is_01529445621.html

Space

Why Russian Space Satellites Are Failing in the Ukraine War

With more than 160 Russian satellites in orbit today, every Ukrainian city, tank, and howitzer should be exposed to the unrelenting gaze of orbital cameras. But that's not happening on the battlefield. While Ukraine's military is reaping enormous benefits from commercial communications and photographic satellites, Russia is only getting meager rewards from its huge investment in military spacecraft.

The Ukrainian army can use commercial systems to obtain images of any area in high detail at least twice a day in favorable weather conditions, whereas the Russian army can get an image of the same area approximately once in two weeks. Existing Russian satellites provide seriously inferior quality of imagery vis-à-vis American and European commercial satellites.

GPS satellites have enabled Ukraine's American-made HIMARS guided rockets to accurately target Russian supply depots and headquarters. SpaceX's Starlink—which uses numerous low earth orbit satellites to provide connectivity through backpack-sized ground stations—became indispensable for Ukrainian military communications.

Source: https://www.strategicstudyindia.com/2023/04/why-russian-space-satellites-are.html#more

Amazon is about to go head to head with SpaceX in a battle for satellite internet dominance

Elon Musk and Jeff Bezos are about to lock horns once again. Last month, the US Federal Communications Commission approved the final aspects of Project Kuiper, Amazon's effort to deliver high-speed internet access from space. In May, the company will launch test versions of the Kuiper communications satellites in an attempt to take on SpaceX's own venture, Starlink, and tap into a market of perhaps hundreds of millions of prospective internet users.

In the past few years, companies have been trying to expand access to the internet via satellite, both as commercial ventures and to supply internet to those in remote locations without otherwise easy access. Starlink, the mega-constellation of more than 3,500 satellites built by Musk's SpaceX, is the biggest of these ventures.

Amazon announced Project Kuiper in 2019, the same year Starlink began launching, leading Musk to tweet that Bezos, then the company's CEO, was a "copycat." The key competition is between SpaceX and Amazon.

There are riches to be had: SpaceX currently charges $110 a month to access Starlink, with an up-front cost of $599 for an antenna to connect to the satellites. Amazon is spending "over $10 billion" to develop Kuiper, with more than 1,000 employees working on the project. Kuiper has a chance of becoming a "fourth pillar" for the company, alongside its retail marketplace, Amazon Prime, and its widely used cloud computing service, Amazon Web Services.

Amazon is not yet disclosing the pricing of its service but has previously said a goal is to "bridge the digital divide" by bringing fast and affordable broadband to "underserved communities," an ambition Starlink has also professed. But whether costs will ever get low enough for that to be achievable remains to be seen. "Costs will come down, but to what extent is really the question."

There remain concerns, too, about space junk and the impact on ground-based astronomy. Before 2019 there were only about 3,000 active satellites

in space. SpaceX and Amazon by themselves could increase that number to 20,000 by the end of this decade. Tracking large numbers of moving objects in orbit—and making sure they don't collide with one another—is a headache.

Source: https://www.strategicstudyindia.com/2023/03/amazon-is-about-to-go-head-to-head-with_0784235564.html#more

OneWeb Launch an Important Success for India's Space Program

On March 26, the Indian Space Research Organization (ISRO) carried out a successful launch of 36 satellites, weighing 5,805 kg, into orbit. The satellites, belonging to the U.K.-based company, OneWeb, were launched using the LVM3 launch vehicle, what used to be called the Geosynchronous Satellite Launch Vehicle (GSLV) Mark III, a three-stage medium-lift launch vehicle developed by the ISRO.

An ISRO press release said that with this launch, NewSpace India Limited (NSIL), the commercial arm of the ISRO that entered into a contract with the OneWeb, has successfully executed the launch of OneWeb's 72 satellites to Low Earth Orbit. OneWeb later confirmed acquiring signals from the 36 new satellites. This is the second time that OneWeb has contracted the NSIL to launch its satellites. With the satellite launch in March, OneWeb's satellite constellation now has a total of 618 satellites. OneWeb notes the enormous ability of the LEO-based satellites to offer high-speed, low latency solutions across the world, involving not only business communities but "towns, villages, municipalities and schools, including the hardest-to-reach areas across the country."

OneWeb previously launched its satellites through Roscosmos, but since the February 2022 Russian invasion of Ukraine, its ties with Moscow have been cut. In March 2022, OneWeb signed an agreement with the Indian space agency to launch its satellites. This is the first-ever commercial launch of LVM3 with the heaviest payload to LEO. The LVM3 was conceived primarily for launching geostationary satellites with a payload capacity of 4T, which can be used for launching 6T payloads for LEO.

Sunil Bharti Mittal, executive chairman of OneWeb, called it "a significant milestone for OneWeb." The seamless manner in which all the stakeholders worked to make the mission a success, demonstrated ISRO's ability to attract foreign customers, including foreign commercial players. This will not only highlight the Indian space prowess, especially considering the small budget with which it operates, but also open up a new revenue stream for the ISRO.

Successive successful launches of LVM3 are remarkable for India in many ways. India is gaining a certain amount of self-sufficiency in launching medium-sized payloads. Gaining proficiency in LVM3 also opens up business and commercial possibilities. The cost-effectiveness of India's satellite launches along with a credible launch system offers India enormous opportunities. This is a pretty big achievement for a space program that is run on a shoestring budget compared to some of the other big space powers.

Source: https://www.strategicstudyindia.com/2023/04/oneweb-launch-important-success-for.html

Are We There Yet? The Artemis Accords, India, and the Way Forward

In the more than two years since the Artemis Accords were envisioned, announced, and executed, considerable progress has been made. Twenty-three countries, including a large number of spacefaring countries, have signed the accords, which lay out a framework for a new era of space exploration. Although certain countries with highly developed space programs, such as Russia and China, have refrained from joining and instead criticized the accords, the Artemis mission has continued without any major glitches. Getting India, a major spacefaring nation, to sign on to the accords has proven to be elusive so far.

India has signed an "implementation agreement" that is seen as a legal instrument related to the Artemis Accords. However, the Indian Space Research Organisation (ISRO) is still not a partner agency when it comes to any of the missions conceived under the Artemis Accords.

The reason space deserves to be treated as a major vertical in its own right is that India's capabilities in space affairs not only considerably outflank its budding know-how in other areas but compete with the best in the world. ISRO pivoted quickly when Russian space agency Roscosmos denied launch services to broadband satellite internet service OneWeb. ISRO managed to launch One-

Web's batch of satellites within a few months of Russia's denial. It is also readying itself to launch a solar scientific mission dubbed Aditya-L1 to study and observe the sun, and in doing so will utilize a high-quality coronagraph payload, which could potentially revolutionize solar astronomy. Lastly, ISRO is seeking to become one of the few space actors, alongside SpaceX and possibly China Aerospace Science and Technology Corporation, to test and use successfully a reusable heavy-lift rocket dubbed the Next Generation Launch Vehicle. While India's space know-how may trail that of the United States, there is still a need to elevate space cooperation to a status that reflects the capabilities of both India and the United States.

The problems with India's Chandrayaan-2 mission, its Small Satellite Launch Vehicle failure, pushed timelines for Gaganyaan (ISRO's human spaceflight mission), and the absence of a space law or an overarching space policy suggest scope for improvement. In recent years, India's trajectory in the space sector has undergone a shift due to regulatory tailwinds.

For example, in the time since the Artemis Accords were announced, India has liberalized its space sector, outsourced the production of its reliable and long-used Polar Satellite Launch Vehicle, and witnessed unusually high levels of commercial interest in its space sector at a time when global funding has been below usual levels. Although India's space economy is currently estimated at an abysmal 2 percent of the global space economy, which amounts to $7.6 billion these developments in India's space sector attest to a larger trend: a willingness on part of the powers that be—namely ISRO and the Indian National Space Promotion and Authorisation Centre (IN-SPACe)—to open up India's space sector and compete for a larger slice of the pie of the global space economy.

Not getting India to sign onto the Artemis Accords would be a missed opportunity. It could even risk accelerating the fragmentation of the global space regime into different blocs.

ISRO was stymied in its efforts to come up with a completely indigenous launch vehicle that could launch heavier payloads to the geosynchronous transfer orbit (GTO). This was due to an earlier stringent U.S. policy that discouraged the sale of cryogenic engines to countries that the United States feared could use them to power military projectiles. Despite this, ISRO was able to develop and launch the GSLV Mark III rocket, which catapulted India into the league of nations that have developed an indigenous launch vehicle capable of launching heavy payloads to the GTO. Thus India was able not only to get around the sanctions, but also to design an indigenous medium-lift launch vehicle.

Since the commercial sector is increasingly fostering many of these new technologies in both India and the United States, rather than the traditional defense industrial base, it is becoming important to ensure that these sensitive technologies are not subject to foreign influence—which underscores the need for like-minded nations like India and the United States to work together.

As India moves toward a range of international technology partnerships under the iCET, the I2U2 Group, and perhaps even AUKUS, smoothing of potential pain points will require clarity on internal policy positions. The United States, being the foremost global pioneer when it comes to space exploration, should consider how it can enhance the coalition of nations that may be interested in space exploration activities by addressing issues such as each participant's potential contribution, funding, and export control measures. Space has always captured and catapulted the imagination when it comes to achieving scientific breakthroughs. It may be time now to do the same in the policy realm.

Source: https://www.strategicstudyindia.com/2023/04/are-we-there-yet-artemis-accords-india.html

New 'Watch Center' to ring alarms on space-related cyber threats

Pentagon leaders have been increasingly concerned about cyber threats to both military and commercial space systems, fears only enhanced by Russia's cyber attacks on commercial providers in the ongoing war in Ukraine. Chief of Space Operations Gen. Chance Saltzman has asked for $700 million in fiscal 2024 to beef up cyber defenses.

Lockheed Martin is among a number of major defense, aerospace and space firms who banded together in 2019 to found Space-ISAC with the strong backing of the Trump administration's National Security Council. Other founding members

include: Northrop Grumman; L3Harris; Kratos; SES; Parsons; Booz Allen Hamilton; the Aerospace Corporation; MITRE and Microsoft; as well as the US government's National Cyber Center of Excellence and a handful of universities.

Using Microsoft's Azure cloud environment, the new center initially will be staffed by 10 analysts housed in a Colorado Springs facility, but also virtually link to other cyber security experts.

Source: https://breakingdefense.com/2023/03/new-watch-center-to-ring-alarms-on-space-related-cyber-threats/

Space Development Agency readies launch of first satellites for comms, missile tracking

SpaceX successfully launched the SDA payloads on April 2 following an abort on March 30. This will be the first substantiation of the Space Force's long-touted "pivot" towards on-orbit resilience via use of large, low-cost constellations in multiple orbits.

The 10 satellites are essentially test satellites, designed to demonstrate the feasibility of the cost, schedule and scalability of a proliferated architecture to perform beyond line of sight targeting and advanced missile detection and tracking.

SDA's mission is to rapidly, and relatively cheaply, field LEO networks and accompanying ground infrastructure for a number of key Space Force missions, using an incremental approach that will see improved capabilities on orbit every couple of years. This network of networks, newly dubbed the Proliferated Warfighter Space Architecture, includes hundreds of satellites, battle management software, new types of technologies and payloads (for missions such as augmenting GPS) and ground support.

Included in the launch are eight satellites for the SDA's Transport Layer, a high-speed, low-latency, tactical communications network using laser intersatellite links; and two for the Tracking Layer, designed for missile warning and tracking of both ballistic and hypersonic missiles. There will be 28 Tranche 0 satellites in total, with the second lot of 18 planned for launch in June. Each of the birds costs an average of $15 million to build.

The Transport Layer network eventually will comprise 300 to 500 satellites in LEO ranging from 750 kilometers to 1,200 kilometers in altitude. These satellites are designed to provide the communications backbone of the Defense Department's Joint All Domain Command and Control (JADC2) concept for managing operations across the ground, air, sea, space and cyber domains.

The Tracking Layer eventually will consist some 200 satellites called the Resilient Missile Warning Missile Tracking – Low Earth Orbit program by the Space Force. This effort is one of three separate Space Force programs for developing missile warning/tracking in different orbits, with the other two managed by the service's main acquisition unit, Space Systems Command.

Source: https://breakingdefense.com/2023/03/space-development-agency-readies-launch-of-first-satellites-for-comms-missile-tracking/

ELECTRONIC WARFARE

Aatmanirbhar Bharat: MoD inks two contracts with BEL, worth Rs 2,400 crore, for procurement of Automated Air Defence Control & Reporting System 'Project Akashteer' for Indian Army & Sarang Electronic Support Measure systems for Indian Navy

Rs 3,000 crore contract signed with NewSpace India Limited for an Advanced Communication Satellite for Indian Army

In yet another boost to 'Aatmanirbharta' in defence, Ministry of Defence, on March 29, 2023, signed three contracts – two with Bharat Electronics Limited (BEL), Ghaziabad and one with NewSpace India Limited (NSIL) – at a total cost nearly Rs 5,400 crore, to bolster the defence capabilities of the country. The first contract with BEL pertains to procurement of Automated Air Defence Control & Reporting System 'Project Akashteer' worth Rs 1,982 crore for the Indian Army. The second contract with BEL relates to acquisition of Sarang Electronic Support Measure (ESM) systems along with associated Engineering Support Package from BEL, Hyderabad at an overall cost of Rs 412 crore for the Indian Navy.

The contract with NSIL, a Central Public Sector Enterprise under Department of Space, Bengaluru pertains to procurement of an advanced Communication Satellite, GSAT 7B, which will provide High Throughput Services to the Indian Army at an overall cost of Rs 2,963 crore. All these projects are under Buy {Indian – IDMM (Indigenously Designed Developed and Manufactured)} category.

Project Akashteer

The Automated Air Defence Control & Reporting System 'Project Akashteer' will empower the Air Defence units of the Indian Army with an indigenous, state-of-the-art capability, to effectively operate in an integrated manner. Akashteer will enable monitoring of low level airspace over the battle areas of Indian Army and effectively control the Ground Based Air Defence Weapon Systems.

Sarang systems

Sarang is an advanced Electronic Support Measure system for helicopters of the Indian Navy, designed and developed indigenously by Defence Electronics Research Laboratory, Hyderabad under programme Samudrika. The scheme will generate an employment of approximately two lakh man-days over a period of three years.

Both the projects will encourage participation of Indian Electronics and associated industries, including MSMEs, who are sub vendors of BEL.

Advanced Communication Satellite

The satellite will considerably enhance the communication capability of the Indian Army by providing mission critical beyond line of sight communication to troops and formations as well as weapon and airborne platforms. The geostationary satellite, being a first-of-its-kind in the five-tonne category, will be developed indigenously by Indian Space Research Organisation (ISRO).

Many parts and sub-assemblies and systems will be sourced from indigenous manufacturers, including MSMEs and start-ups, thereby giving a fillip to the private Indian space industry, in line with the Prime Minister's vision of 'Aatmanirbhar Bharat'. The project will generate an employment of approximately three lakh man-days over a period of three and half years.

Source: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1911937

US must revive, dominate electronic warfare, Pentagon CIO Sherman says

John Sherman, the Pentagon's chief information officer, told the House Armed Services Cyber, Information Technology and Innovation subcommittee at a March 9 hearing on defense in the digital era that the U.S. must "regenerate" its electronic warfare capabilities after years of neglect to ensure dominance on battlefields of the future. He said, "As we get ready for China, we better be able to fight and dominate" the electromagnetic spectrum.

Sherman said, "This is something I'm going to bird-dog very carefully from my office here, particularly as we see the services starting to, kind of, regenerate electronic warfare and other capabilities, both to put the enemy back on their heels and ensure our non-commissioned officers and our trigger-pullers can stay in touch with one another. I think we need to keep a close eye on it here, and monitor, as we regenerate this capability that we had in the Cold War, that we had to maybe somewhat turn away from a bit during the war on terror."

He said, "As we've seen on the Ukrainian battlefield — all the dynamics with [electromagnetic spectrum operations], of how the Russians are trying to use it, and the Ukrainians are using it — we cannot be cut off on this, to be able to make sure we can conduct combat operations."

Source: https://www.c4isrnet.com/electronic-warfare/2023/03/09/us-must-revive-dominate-electronic-warfare-pentagon-cio-sherman-says/