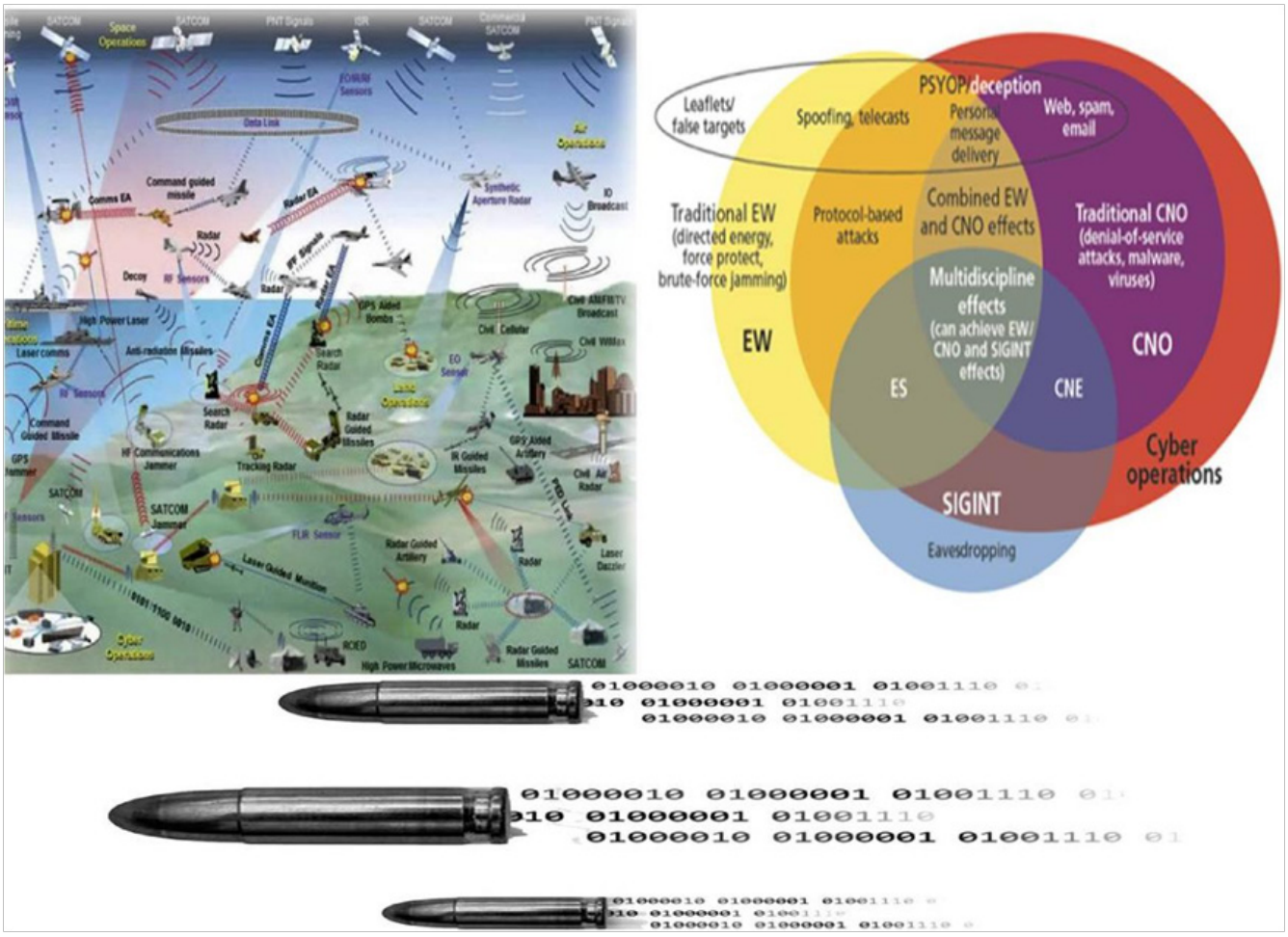
Cyber, Communications, EW & Technology (C2ET) Digest

By Maj Gen P K Mallick, VSM (Retd)



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

PUBLISHED BY STRATEGIC STUDY INDIA

Contents

CYBER

With dreams of JADC2, Pentagon relaunches AI-driven command & control experiments

The Pentagon kicked off a new Global Information Dominance Experiment in high-speed data sharing. The US military HQs aren't nearly as high-tech as people think they are, and that's a problem the Pentagon is eager to solve. Military and civilian leaders from across all service branches, all eleven combatant commands, technology vendors and international allies participated in the exercise.

Military command posts are not high-tech temples. Staff officers must retype reams of numbers into spreadsheets or scrawl them on sticky notes, because different networks can't share data directly. A lot of potentially useful information is ignored for sheer lack of time to look at it. About 98 percent of the data and information from early-warning radars was not being actually analyzed or assessed.

Joint All Domain Command & Control (JADC2) is to pool all the data, automate the data sharing and even use artificial intelligence for the first-pass analysis. This will spare the human beings hours of poring over satellite images, radar returns, and social media posts and you actually give them time to think.

This time around, using both commercial and military-specific technologies to pool data across the armed forces, host it on cloud servers, pick out telltale patterns with machine learning, and provide rapid-fire analysis to commanders and decision-makers across the Department of Defense.

"We want to rapidly improve access to data across the joint force — from the strategic level to our tactical warfighters." That's a crucial combat task in an era where big data is a big advantage everywhere from boardrooms to battlefields.

Source: https://breakingdefense.com/2023/02/with-dreams-of-jadc2-pentagon-relaunches-ai-driven-command-control-experiments-gide/?utm_campaign=Northrop%20Grumman&utm_medium=email&_hsmi=245252367&_hsenc=p2ANqtz---C5j31YOZ9RienY20q-qemDt9Pk5Bam3idg5HXoEjaLoKWoYmzgH-I3bvTF3KGSCJOewoNzoQqswxukIgvHW-G9KYwQ&utm_content=245252367&utm_source=hs_email

US Cyber Command developing own intelligence hub

U.S. Cyber Command, tasked with defending Department of Defense IT networks and coordinating cyberspace operations, is developing its own intelligence hub, after years of relying on other information-gathering sources.

"We know everything about a T-72 tank, all the way to every nut and bolt in there, for the Army. But we don't have that for networks, with respect to an all-source capability."

Cyber Intelligence Center would complement the slate of well-established centers and intel-collecting practices with products that are sought-after but still not available.

"We've got great partners with the National Security Agency, and they're very focused on signals intelligence. That's a huge part of what we look at. But across the spectrum, a combatant command really needs all-source intelligence. We have found, unfortunately, that the foundational layer in cybersecurity just wasn't there."

The Cyber Intelligence Center would be primarily staffed through the Defense Intelligence Agency, which produces, analyzes and disseminates military intelligence for combat and noncombat missions. Exactly when such a center will come to fruition isn't clear.

Source: https://www.strategicstudyindia.com/2023/03/us-cyber-command-developing-own.html#more

The government cannot win cyber warfare without the private sector

The Biden administration has made cyber attacks a major diplomatic front, but the executive and legislative branches have done little to stop these attacks. The government agencies charged with deterring and defeating this threat are not properly equipped for the task, and there is a lack of consensus about which methods will be most effective for countering digital dictatorship. The Council on Foreign Relations (CFR) recommends "a program of deepening public-private collaboration between the Defense Department (DOD) and the defense industry" to stop these hacks. It suggests this because it recognizes that the private sector is who owns and operates the networks and systems that the problem countries

target, while the public sector "lacks the same picture of the threat environment."

Private-sector actors regularly face hackings and understand that their survival in the marketplace hinges upon addressing them swiftly and efficiently. The government doesn't recognize many of these threats until they occur. The government has the ability to contract with anyone, so why wouldn't it choose to work more closely with private companies?

As the old cliché goes, the government that governs best is the one that governs least. As such, federal procurement officers should consider quickly outsourcing more of the public sector's current responsibilities to private-sector companies.

However, even if the government relies heavily on the private sector's shoulders, hacking of its infrastructure will still occur. Disaster preparedness and response is one thing that it will never be able to outsource. That's why it's critical that the government dramatically increase the number of cyber security experts it employs and begin to treat hacking as a national security priority.

We may not be able to stop China and Russia from working to steal our sensitive information and damage our critical infrastructures, but we can stop them from being effective. We will be able to do so only if the government stops trying to manage everything and instead begins focusing singularly on its hacking detection and response effort. Only then will it find the right private and public sector balance needed to respond to these threats of terrorism and keep the American people safe and secure for generations to come.

Source: https://www.strategicstudyindia.com/2023/03/the-government-cannot-win-at-cyber.html

Ukraine one year on: When tech companies go to war

Russia's war in Ukraine is the first conflict in which global technology companies have played a direct and central role. Many domains that are critical in securing a state's territorial integrity are now controlled by these companies – including cybersecurity, satellite imagery, access to the internet and the surveillance of information.

Microsoft and Amazon have proven fundamental in helping Ukrainian public and private actors secure their critical software services. They have done so by moving their on-site premises to cloud servers to guarantee the continuity of their activities and aid in the detection of and response to cyber-attacks. Google has assisted Ukraine on more than one front: it created an air raid alerts app to protect Ukraine's citizens against Russian bombardment, while also expanding its free anti-distributed denial-of-service (DDoS) software – Project Shield – which is used to protect Ukraine's networks against cyber-attacks.

Another game changer has been the accessibility of open-source intelligence through commercial satellite services. As the attack unfolded, Ukrainian forces tracked Russian troop movements using Google Maps. Later, when this became a double-edged sword for Ukraine because it revealed Ukrainian troop positions to Russia's forces, Google disabled traffic updates and concentration features to prevent the exposure of Ukrainian operations. Private satellite companies, such as Maxar Technologies and Capella Space, have also made their imagery publicly available through media outlets and social media platforms.

Tech companies hold the keys to an effective fight against disinformation. Meta established a special operations centre to monitor and curb disinformation spread by Russia-controlled media outlets. Digital platforms such as Twitter, YouTube, and Google have curbed the access of state-owned Russia Today (RT) and Sputnik news in Europe and in some cases globally.

Elon Musk's Starlink supplies the Ukrainian government and armed forces with internet connection through its low-orbit satellite service and some 5,000 terminals. This has enabled Ukrainian troops and institutions to continue operating despite Russia's destruction of telecommunications infrastructure. The Tesla CEO has since requested that the Pentagon assume all the financial responsibility. Musk has also moved to restrict the use of Starlink's internet services with drones This demonstrates the risks of allowing effective public-private cooperation to break down – particularly when companies' priorities may diverge from states' geopolitical interests.

Tech corporations have become owners and rulers of the critical assets that a sovereign state requires

to function. A lack of access to technology can be a matter of life or death

Source: https://www.strategicstudyindia.com/2023/03/ukraine-one-year-on-when-tech-companies.html#more

What is the United States-India Initiative on Critical and Emerging Technologies (iCET)?

At the end of January 2023, India's National Security Advisor (NSA) Ajit Doval and the U.S. NSA Jake Sullivan officially launched the United States-India initiative on Critical and Emerging Technologies (iCET). The two NSAs took part in an unofficial discussion hosted on January 30, 2023, where they were joined by the U.S. Secretary of Commerce Gina Raimondo and a whole host of Indian and American officials.

The room was filled with industry mavericks, thought leaders, representatives from India's impressive startup ecosystem, and others who have been long invested in the bilateral partnership. That the governments, the private sector, research laboratories, and the academia in India and the United States were entering into a distinctive chapter for partnerships was clear.

Those in the room highlighted the possibilities of deepening ties between the two countries in strengthening quantum communications, building a semiconductor ecosystem in India, accelerating defense collaborations, exploring commercial space opportunities, and catalyzing existing and forging new research opportunities and partnerships.

A day later, the two NSAs took part in G2G meetings alongside an impressive group of government representatives. On the evening of January 31, the White House published a fact sheet on the iCET. The fact sheet made clear that the iCET was a process that started in May 2022, following a meeting between Prime Minister Narendra Modi and President Joe Biden in QUAD leaders' summit in Tokyo. The fact sheet features details on a range of areas covered by the iCET—from creating quantum coordination mechanisms and collaborating on high-performance computers to creating a defense industrial cooperation roadmap and setting up a task force to "identify near-term opportunities and facilitate longer-term strategic development of a complementary semiconductor ecosystem."

This is an initiative that is led by the NSAs of the two countries and their respective bureaucracies: the National Security Council (NSC) in the United States and the National Security Council Secretariat (NSCS) in India.There is much to be done between defense-focused startups and MSMEs in India and the United States. The iCET could catalyze a defense innovation bridge between the Bay Area and several institutions dotted across India, especially the IITs.

The momentum led by the NSC and the NSCS has immense potential to electrify opportunities that lay dormant, create green-shoot prospects in emerging and critical technologies and deepen the strategic arc of technology cooperation between the two countries across several sectors of promise. The iCET will require the private sector, knowledge partners in the industry, and the academia in both countries to give functional meaning to these very outcomes.

Source: https://www.strategicstudyindia.com/2023/03/what-is-united-states-india-initiative.html

A Private Company Is Using Social Media to Track Down Russian Soldiers

On Oct. 12, 2022, Russian soldier Aleksey Lebedev logged onto VKontakte, Russia's most popular social network, and uploaded a photo of himself in military fatigues crouching in a large white tent. He had obscured his face with a balaclava, but did not obscure the exact location from which he had posted: Svobodne village in southern Donetsk.

Lebedev's post was picked up by a Ukrainian military investigations company called Molfar. This lead was transferred to an analyst in its open-source intelligence (OSINT) branch, and investigators spent the next few hours constructing a target location profile for Lebedev and his military unit. The unit's location was believed to be a training base for Russian and pro-Russian separatist troops. After discovering two other photos posted from the same location by pro-Russian servicemen—as well as other corroborating evidence, Molfar passed its findings onto Ukrainian intelligence.

Two days later, explosions and "fireworks" were observed at the site of Lebedev's selfie, approximately 40 miles behind Russian lines. On its Telegram channel, the Security Service of Ukraine

(SBU) reported the attack.

But what is new in Ukraine is how these techniques are being reverse-engineered: not to retrospectively expose atrocities and malfeasance but to proactively kill enemy forces and destroy enemy hardware on the battlefield itself.

Since the beginning of the war, Molfar has received funding from the Civilian Research and Development Foundation—a nongovernmental organization that includes the U.S. State Department, U.S. Defense Department, and the U.K. government among its backers—to give additional OSINT trainings to officials from the SBU, as well as to the Defense Intelligence of Ukraine and other government bodies.

The private-sector OSINT market is booming. The big five U.S. intelligence conglomerates (Booz Allen Hamilton, CSRA, Leidos, SAIC, and CACI International) are also making significant commitments to open-source intelligence. As a result, the OSINT industry, valued at $5.1 billion in 2021, is projected to reach $34.9 billion by 2030.

Like Russia, Ukraine has learned this the hard way and has suffered through its own OPSEC blunders, such as when Russian OSINT researchers successfully identified the location of a tank repair facility in Kyiv from a report on April 7 by Ukrainian TV channel 1+1. Local media reported that the facility was targeted shortly after, on April 15, by a Russian missile, reportedly resulting in "destruction and casualties."

Molfar said its targeting operations continue. It claims to provide an average of 15 actionable intelligence reports to Ukrainian intelligence per month.

Fully aware of the lethal potential of OSINT, the Ukrainian government has heavily restricted journalists reporting from the front line and other sensitive locations. A law in force since March 2022 has made filming the movements of Ukrainian military personnel, sites of shelling, street names, transport stops, shops, factories, and other civilian and military facilities punishable by up to 12 years in jail.

Now, digital technology, real-time connectivity, and artificial intelligence have made the smallest details—from a tree line to a mountain range to a minor architectural feature—liable to identification and geolocation, particularly when the approximate location of the target is already known.

Source: https://www.strategicstudyindia.com/2023/03/a-private-company-is-using-social-media.html

China Is Relentlessly Hacking Its Neighbors

IN MAY 2022, Joe Biden invited the leaders of 10 Southeast Asian nations to the White House for talks about the region, which is home to more than 600 million people. High on the agenda was China—a key trading partner for all the countries, but also a potential threat to their stability. However, in the weeks leading up to the meeting, hackers working on behalf of China were stealing thousands of emails and sensitive details from the Southeast Asian nations. The Chinese-linked hackers have quietly compromised neighboring countries, looking to gain political and economic information.Chinese-linked hackers were able to break into mail servers operated by the Association of Southeast Asian Nations (ASEAN) in February 2022 and steal a trove of data.

The hackers stole more than 10,000 emails, making up more than 30 GB of data.

For all countries across Southeast Asia, China is a crucial partner. The nation is the biggest power in the region, and trade between the countries is crucial to many of their economies. "Chinese president Xi Jinping has talked of building a "community of common destiny" with ASEAN countries. China has spent billions on infrastructure and manufacturing across Southeast Asia—particularly through the Belt and Road Initiative, an infrastructure investment project that helps give China political and economical power. As a result, there are many tensions between the neighbors, including around the South China Sea.

China's state-sponsored hackers are incredibly active in the area. In recent years government and military units in Southeast Asian countries have been a common target for China's hackers. Security firm Recorded Future has tracked 10 Chinese-linked groups attacking Southeast Asian countries in the past two years—primarily government and military organizations.

The identified intrusion campaigns almost certainly support key strategic aims of the Chinese government, such as gathering intelligence on

countries engaged in South China Sea territorial disputes or related to projects and countries strategically important to the Belt and Road Initiative.

Across Southeast Asia, Che says, it is likely that China's increase in attacks could be a response to the US focusing more on its relationships within Asia—he highlights economic and security operations as possible causes.

Source: https://www.strategicstudyindia.com/2023/03/china-is-relentlessly-hacking-its.html

China to establish National Data Administration

China will establish a National Data Administration as part of the reorganization of the country's State Council, according to a proposal submitted Tuesday to the National People's Congress. The new agency will be under the management of the National Development and Reform Commission, which broadly oversees China's macroeconomic planning, and will be responsible for the "coordination and advancement of building the data factor system; overall planning of the integrated sharing and development and use of data resources; [and] overall planning of the advancement of Digital China, digital economy, and digital society plans and construction." The formation of the new agency follows last week's release of the "Digital China Construction Plan," which calls for the construction of a "national data management system and mechanism" as part of the "opening up of the main arteries of China's digital infrastructure."

Source: https://www.cfr.org/blog/cyber-week-review-march-10-2023

Chinese cybersecurity company alleges cyberattacks originating from Europe, North America

According to the *Global Times*, Beijing-based cybersecurity company Qi An Pangu Lab has identified six members of a hacker group called Against The West (ATW) accused of carrying out large-scale scanning detection and supply chain attacks on Chinese networks since 2021. Pangu Lab attributed ATW to individuals from Switzerland, France, Poland, and Canada, among other countries. The group has stolen and leaked information from institutions such as the People's Bank of China and China's Ministry of Public Security, along with targets in Russia, Belarus, Iran, and North Korea. Pangu Lab and other Chinese cybersecurity companies have published several reports on advanced persistent threat (APT) groups in the last two years, including one on the Equation Group, an APT linked to the NSA, although researchers have questioned the timing and content of some reports.

Source: https://www.cfr.org/blog/cyber-week-review-february-24-2023

EU agencies warn of Chinese APT attacks

The European Union Agency for Cybersecurity (ENISA) and the EU Computer Emergency Response Team (CERT-EU) warned this week that several Chinese state-sponsored hacking groups are targeting businesses and government organizations in the EU. The joint advisory said [PDF] the threat actors were observed "conducting malicious cyber activities against business and governments in the Union." The groups identified in the advisory include: Emissary Panda, APT 30, Zirconium, Mirage, Gallium, and Mustang Panda. The agencies said that the groups frequently used the invasion of Ukraine and its effect on EU businesses as a hook in phishing attempts. The joint statement called for European organizations to focus on increasing access controls, hardening software products and highly-privileged accounts, and using highly secure passwords and multi-factor authentication on all accounts. The advisory comes a week after the FBI warned U.S. secretaries of state about the growing threat of Chinese hacking operations against state government networks.

Source: https://www.cfr.org/blog/cyber-week-review-february-24-2023

UK military intelligence team wins Western Europe's 'largest cyber warfare exercise' held in Estonia

A team from British military intelligence placed first at a cyber warfare exercise described as "Western Europe's largest" hosted at the CR14 cyber range in Estonia.The exercise, titled Defence Cyber Marvel 2 (DCM2), was organized by the British Army and featured 34 teams from 11 countries, including the United Kingdom, India, Italy, Ghana, Japan, the U.S., Ukraine, Kenya, and Oman. It concluded on February 17th.

The specific tasks the teams had to take on were

not disclosed, however the MoD described a seven-day competition in which participants responded to "common and complex simulated cyber threats including attacks to networks, industry control systems and unmanned robotic systems."

The challenges were "simulating some of the tactics Russia used to disrupt Ukrainian cyberspace in the early days of the invasion one year ago," It took place at the CR14 in Tallinn — the digital equivalent of a traditional military shooting range. The Estonian Ministry of Defence described the range when it opened in 2019 as "a system capable of imitating the functioning of a complex computer network and providing the opportunity to practice various cyber operations without endangering regular computer networks."Since then, C14 has become the regular host of the annual Locked Shields exercises, organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn. The CCDCOE exercise is not limited to NATO members, and participants have historically included Japan and Ukraine.

Each team that took part in DCM2 was judged on "the effectiveness and speed of their response and how quickly they identify and adapt to new threats – vital for developing war fighters for the digital age," The winning team came from Britain's 7 Military Intelligence who competed remotely from Italy, while Tallinn-based 5 Military Intelligence "came a close second" MoD added.

Military personnel taking part in the challenge "get to exercise and learn with folk from a vast array of different nations, backgrounds and specialisations – all united by a common purpose – to hone their skills to a fine edge, in order to protect our people, our prosperity and our principles," Copinger-Symes added.

Comments. One would like to know who participated from India in this Exercise and what was their position overall.

Source: https://www.strategicstudyindia.com/2023/03/uk-military-intelligence-team-wins.html

Ukraine Suffered More Data-Wiping Malware Last Year Than Anywhere, Ever

After a year of war, it's becoming clear that the cyberwar Ukraine has endured the most active digital conflict in history.

in 2022, Ukraine saw far more specimens of "wiper" malware than in any previous year of Russia's long-running cyberwar targeting Ukraine or any other year anywhere. The growing volume of destructive code hints at a new kind of cyberwar that has accompanied Russia's physical invasion of Ukraine, with a pace and diversity of cyberattacks that's unprecedented.

In total, 16 different "families" of wiper malware in Ukraine over the past 12 months, compared to just one or two in previous years, even at the height of Russia's cyberwar prior to its full-scale invasion. "We're not talking about, like, doubling or tripling It's an explosion, another order of magnitude."

The growing volume of wiper malware specimens hitting Ukraine may be creating a more global proliferation problem. As those malware samples have shown up on the malware repository VirusTotal or even the open-source code repository Github, other hackers were detected reusing those wipers against targets in 25 countries around the world. Once that payload is developed, anyone can pick it up and use it. Since early 2022, Russia's cyberattacks against Ukraine have shifted into a different gear. Instead of masterpieces of malevolent code that required months to create and deploy, as in Russia's earlier attack campaigns, the Kremlin's cyberattacks have accelerated into quick, dirty, relentless, repeated, and relatively simple acts of sabotage.

Despite that sheer volume of wiper malware, Russia's cyberattacks against Ukraine in 2022 have in some respects seemed relatively ineffective compared to previous years of its conflict there.

Russia appears to have swapped quality for quantity in its wiper code. Most of the dozen-plus wipers launched in Ukraine in 2022 have been relatively crude and straightforward in their data destruction, with none of the complex self-spreading mechanisms seen in older GRU wiper tools like NotPetya, BadRabbit, or Olympic Destroyer.

Source: https://www.strategicstudyindia.com/2023/02/ukraine-suffered-more-data-wiping.html

Russian phishing attacks flooded Ukraine, tripled against NATO nations in 2022: Report

As Russian ground troops started massing along the border with Ukraine in 2021, Russian hackers

began laying the foundation for their own unprecedented cyber onslaught.

According to a new report by Mandiant, a cybersecurity firm now part of Google Cloud, the spring and fall of 2021 saw dramatic spikes in phishing attempts. When Russia invaded Ukraine, Russian phishing attempts against Ukraine rose 250 percent, while Russian phishing against NATO countries increased over 300 percent, compared to a 2020 baseline.

Since the invasion kicked off, some observers have been confounded by the apparent lack of success Russia's once-feared cyber squads have had in taking Ukraine offline. More recently officials noted that the attacks were happening, but Ukraine, with a lot of Western help, had managed to mainly fend them off.

Overall, the pace of attacks slowed and appeared less coordinated than the initial wave in February 2022. Mandiant's analysis suggests Russia may have expended a lot of stockpiled cyber ammunition early in the war. Hackers can lurk undetected in a network for months or years, quietly stealing data, but once they unleash destructive malware, visibly disrupting operations, it becomes obvious that someone has unauthorized access to the system, and cybersecurity specialists can often lock them out.

Yet Russia has also showed a certain restraint in its recent cyber attacks. In 2017, the Russian Notpetya attack spread far beyond Ukraine, most likely by mistake, paralyzing global shipping company Maersk and doing billions of damage worldwide. In February 2022, Russian hackers disrupted the Viasat broadband network, crippling communications not only in Ukraine — that is, until Elon Musk's Starlink stepped in — but also across Europe. Since then, however, Mandiant reports, "we've seen little evidence of a spillover effect outside Ukraine."

Russia hasn't even used malware to attack the Ukrainian power grid, as it did in 2017 with the Industroyer/Crashoverride virus that briefly blacked out part of Kyiv. This isn't because Russia lacks the expertise. Russia definitely has the capability and intent to create [physically] destructive attacks — as evidenced with INDUSTROYER.v2 — should they choose to, but they have not done so.

Instead, Russia resorted to real-world attacks, expending much of its missile arsenal against Ukrainian infrastructure, seeking to destroy it permanently rather than disrupt it temporarily with a hack. That shows, some limits of cyber warfare. "Cyber tools are often best used for espionage because in the kinetic war, conventional means are going to have most of the destructive impacts."

Source: https://www.strategicstudyindia.com/2023/02/russian-phishing-attacks-flooded.html

The US has announced its National Cybersecurity Strategy: Here's what you need to know

On March 2, President Joe Biden released a new National Cybersecurity Strategy, which outlines steps the government is taking to secure cyberspace and build a resilient digital ecosystem that is easier to defend than attack — and that is open and safe for all.

Biden wrote in the framework's preface,"When we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable and secure,"

The strategy included efforts to increase accountability for tech companies, boost privacy protections and ensure fair competition online. The scope of the document is limited to cybersecurity, as its title is "National Cybersecurity Strategy" rather than "National Cyber Strategy." They are not identical in scope.

Although the strategy builds on cybersecurity efforts from the previous three administrations, its most important characteristic is its departure from past perspectives and practices. Information or influence operations and the use of offensive operations in cyberspace to advance any national goals would naturally be included in a National Cyber Strategy, but that is not what this document is. The strategy document is also silent on cybersecurity for national security systems, such as those operated by the Department of Defense and the intelligence community.

In arguing for a rebalancing of the responsibility for cybersecurity, the strategy does not absolve end users of all security responsibilities. It does, however, indicate that we as a nation must "ask

more of the most capable and best-positioned actors" in society. The strategy states that cybersecurity "must be the responsibility of the owners and operators of the systems that hold our data and make our society function, as well as of the technology providers that build and service these systems."

The strength of cybersecurity cannot be left simply to individual private-sector actors to decide based solely on their business needs. For public safety and national security needs, the nation needs a more robust cybersecurity posture than that which would result if left up to these individual actors.

Disrupting and Dismantling Threat Actors. The strategy also endorses a highly assertive approach to disrupting threat actors in cyberspace. The strategy does not shy away from the use of military power for such disruption where appropriate.

A notable omission from the strategy document is the word "deterrence." Nowhere in the document do the words "deter" or "deterrence" appear. This can't be by accident, and it points to the failure of deterrence as a policy for promoting cybersecurity.

Many cybersecurity analysts have, for years, advocated liability as a way of incentivizing vendors to pay more attention to cybersecurity. But for the first time, a document with the full endorsement of the executive branch has done the same.

The new strategy is a significant departure from past practices and precedent, and I applaud it. But its public calls for regulation, the imposition of liability for insecure software products and services, and the increased involvement of the U.S. military in support of private-sector cybersecurity will be controversial.

The strategy promises that the Department of Defense and the intelligence community will work within their legally established roles to disrupt the activities of malicious cyber actors. The need for effective attack assessment across a broad range of civilian assets will require technical, legal, and policy coordination between the private sector and the U.S. government. It may entail a significant Defense Department presence on privately owned networks. How the American people will react to such coordination remains to be seen.

Source: https://www.lawfareblog.com/where-new-national-cybersecurity-strategy-differs-past-practice

What are the 5 pillars of the National Security Strategy?

Each of the five pillars it sets out are broken down into strategic objectives, but here's a quick overview of what they entail:

1. Defend critical infrastructure

2. Disrupt and dismantle threat actors

3. Shape market forces to drive security and resilience

4. Invest in a resilient future

5. Forge international partnerships to pursue shared goals

Source: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

My Strange Day With Bing's New AI Chatbot

Bing search engine showcased new search features powered by the technology behind startup OpenAI's ChatGPT. Microsoft executives hyping their bot's ability to synthesize information from across the web instead focused on examples. But they had, implicitly, put into high gear a race to use chatbots to upend the way people look up information online. Google also announced search upgrades this week and its own chatbot, named Bard. These battling bots' ability to handle unexpected, silly, or manipulative questions from the public will surely play a big part in how the products work out for their creators and web users.

As I looked at the citations for this search—gearjunkie.com and cnn.com—the response started to bum me out. The Bing bot was drawing from the written work of humans who had spent time on these reviews. But it had obfuscated and, in some cases, straight-up plagiarized their sentences. A Microsoft executive told reporters this week, "We care a bunch about driving content back to content creators. That's why we put annotations and citations. We make it easy for people to click through to get to those sites." But the chatbot's responses are designed to remove the need to visit those sites, and I'm not sure many people will click through.

So far, I'm enjoying Bing's search chatbot. It's fun

and diverting. I am mostly entertained by Bing's obsession with emoji, particularly 🙂, which it includes at the end of many responses. But in my years online I have already built up an arsenal of ways to fact-check and screen the information that I find through search engines. I'm not sure I want to have to develop more to handle the quirks of searches with a chatbot—or perhaps soon, multiple chatbots, as Google and others enter the fray.

Source: https://www.strategicstudyindia.com/2023/02/my-strange-day-with-bings-new-ai-chatbot.html

Why does the US need a National Cybersecurity Strategy?

The world is increasingly complex and cyberthreats are growing more sophisticated, with ransomware attacks running into millions of dollars in economic losses in the US. In 2022, the average cost of a ransomware attack was more than $4.5 million, according to IBM.

Attacks on critical information infrastructure could have disastrous consequences for public infrastructure and health. Cybercrime and cyber insecurity were seen by risk experts surveyed for the World Economic Forum's *Global Risks Report* as the 8th biggest risk in terms of severity of impact, across both the short term (next two years) and over the coming decade.

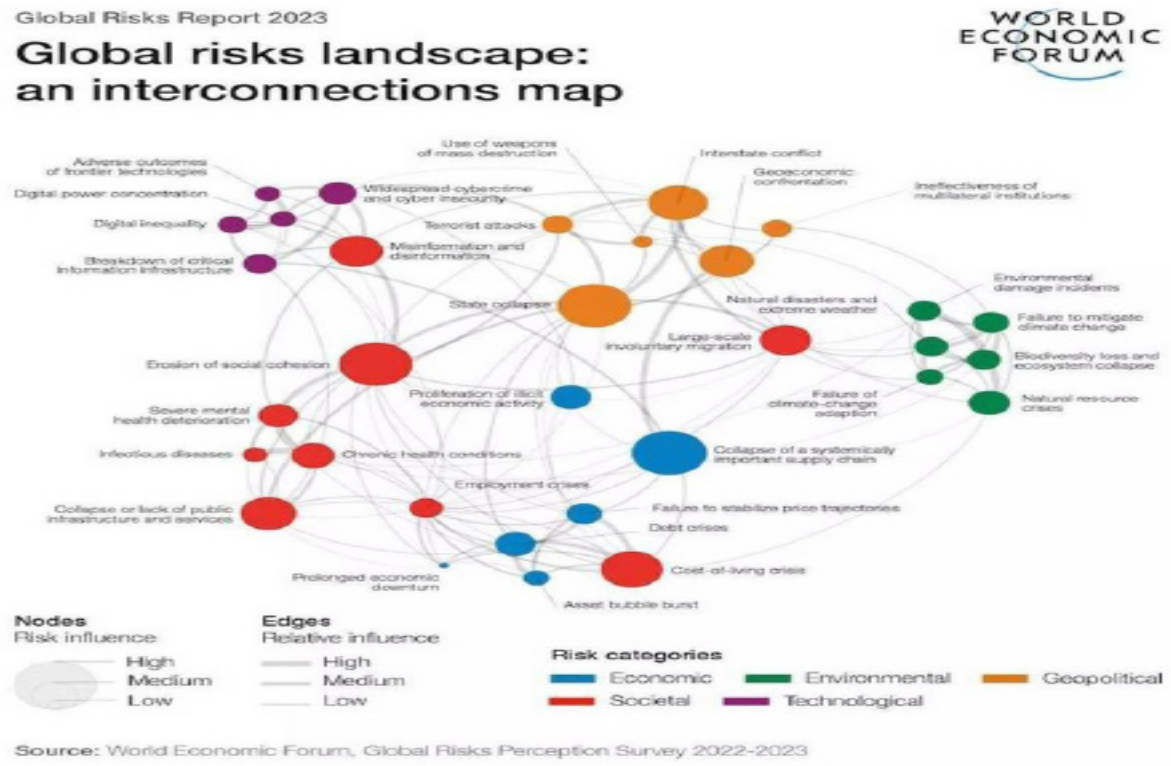
In 2022, state-sponsored cyberattacks targeting users in NATO countries increased by 300% compared to 2020, according to Google data.

With cyberattacks on the rise, experts at the World Economic Forum's Annual Meeting at Davos predicted that 2023 would be a "busy year" for cyberspace with a "gathering cyber storm".

"This is a global threat, and it calls for a global response and enhanced and coordinated action," Jürgen Stock, Secretary-General of the International Criminal Police Organization (INTERPOL), said at Davos.

The Forum's *Global Cybersecurity Outlook 2023* also found that 93% of cybersecurity experts and 86% of business leaders believe that global instability will have a negative impact on their ability to ensure cybersecurity over the next two years.

Source: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/



Source: World Economic Forum, Global Risks Perception Survey 2022-2023

COMMUNICATIONS

Space Force to launch 'marketplace' for satellite-to-cellular communications services

The U.S Space Force is planning to request bids from providers of wireless phones enabled to connect with satellite networks. This will enable the Defense Department to equip warfighters with smaller and lighter, more capable, less expensive communication devices. Some of these architectures will enable existing smartphones to seamlessly communicate with satellites using the cellular spectrum that's been allocated to that to that [cell phone] provider.

The plan is to set up a contracting vehicle that allows military users to buy satellite-direct-to-cellular communications capability as a service, along the lines of CSCO's ongoing initiative to provide DoD customers with satellite communications (SATCOM) and internet access via large constellations in low Earth orbit.

T-Mobile and SpaceX announced their plan to connect vast majority of smartphones already on TMobile's network to Starlink satellites. The two firms intend to create a new network, broadcast from Starlink's satellites using T-Mobile's mid-band spectrum nationwide, at first providing text services, adding voice and data coverage at a later stage.

Qualcomm and Iridium announced that they are collaborating to bring satellite connectivity for 5G communications to Android phones.

Hughes Network Systems, working with DISH Network, OneWeb and EchoStar satellite operators, scored an experimental contract to develop a military-only SATCOM empowered 5G network. The Federal Communications Commission (FCC), which licenses US telecommunications firms to access radio frequency spectrum, is eyeing changes to processes that would ease such partnerships between satellite and terrestrial providers. The proposed changes would allow satellite-to-cellular communications by letting sats use spectrum already licensed to wireless cell phone providers.

This would enable expanded coverage to a terrestrial licensee's subscribers, especially in remote, unserved, and underserved areas, and would increase the availability of emergency communications."

Source: https://breakingdefense.com/2023/03/space-force-to-launch-marketplace-for-satellite-to-cellular-communications-services/?utm_campaign=Newsletters&utm_medium=email&_hsmi=248967597&_hsenc=p2ANqtz--vOKuKOr-BCedkyYH9lng49jzrGpmPpzsBe3P8lbQOCwnX-pfl-w43YmnCTtC40diG-sI_dWsVqFF1QPLuT6H-JB6inweSA&utm_content=248967597&utm_source=hs_email

STRATCOM wrapping spectrum ops center plan, as military faces bandwidth grab by 5G firms

US Strategic Command expects approval soon of the action plan for its Joint Electromagnetic Spectrum Operations Center (JEC), designed to identify gaps in and improve capabilities across the US military to fight through attacks on spectrum access, STRATCOM head Gen. Anthony Cotton said today. The electromagnetic spectrum (EMS) superiority is critically important for not just STRATCOM, but all of the combatant commands, underpinning communication through all domains, and assured PNT, position, navigation and timing.

SPACECOM is responsible for providing to the joint force, from PNT to SATCOM to missile warning, are dependent upon access to EMS. Spectrum availability it foundational to what US Space Command does.

DoD's EMS Superiority Strategy and the JEC are focused on threats primarily from Russia and China, which have been building up their electronic warfare capabilities. But there are concerns about another threat to DoD spectrum access closer to home —commercial communications firms hungry for spectrum to launch 5G wireless phone and internet services.

DoD for several years has been fighting a battle against major telecommunications firms, their congressional backers on the House and Senate commerce committees, and the Federal Communications Commission (FCC, which regulates commercial spectrum usage) to keep access to the 3.1-3.45GHz S-band, which currently is walled off for military use alone.

The House in July 2022 passed a bill, called the Spectrum Innovation Act, that would mandate the

FCC to auction off the 3.1-3.45GHz band to interested 5G players, such as telecomm behemoths AT&T and Verizon. That band is primarily used by DoD ground-, air- and sea-based radars for detecting airborne and missile threats in particular, by the Navy's Aegis Combat System that is the heart of its ballistic defense capabilities.

DoD officials and military commanders assert that keeping some level of access to the band is critical, and that there isn't another spectrum band suitable for those systems. In addition, they argue, replacing current radar systems relying on the band would cost billions and take some two decades. Replacing just the Aegis radar with one capable of using different frequencies would likely cost $120 billion.

Source: https://www.strategicstudyindia.com/2023/03/stratcom-wrapping-spectrum-ops-center.html

What are the differences between SD-WAN and MPLS?

Multiprotocol label switching (MPLS) is a common method for constructing the connections between local area networks (LANs) that make up wide area networks (WANs). Using specialized routers, MPLS sends packets along predetermined network paths, improving upon the typical way the Internet works. These predetermined network paths can be used as the connective tissue that comprises a WAN and allow multiple virtual WANs to coexist over a shared network backbone. However, they take quite a bit of time to set up, can be expensive, and require a contracted service from a carrier or telecommunications company.

A software-defined WAN (SD-WAN) is a large network that connects LANs using software, not hardware. SD-WANs do not require any specialized equipment for routing. They run over the regular Internet, making them cheaper to implement than other networking methods.

The SD-WAN model does not exclude the usage of MPLS — MPLS can be one of the networking methods used in an SD-WAN — but overall SD-WANs are often more flexible and cost-effective by comparison.

MPLS connections are dedicated only to the users of those connections. They are more direct and more reliable than the public Internet. However, they require the purchasing of expensive hardware and their routes cannot change very easily. Meanwhile, SD-WANs are built on existing paths like the public Internet and can easily increase their routes and the number of users served, like the bus line.

What are some SD-WAN benefits compared to MPLS?

- SD-WANs do not rely on specialized hardware.
- SD-WANs have no inherent bandwidth limits.
- SD-WANs are service provider-agnostic.
- SD-WAN routing is more flexible.
- SD-WANs integrate more easily with the cloud.

What are some SD-WAN drawbacks compared to MPLS?

- MPLS offers more granular control over where packets go.
- MPLS is sometimes more reliable.
- MPLS is better for real-time applications.

How does SD-WAN compare to the network-as-a-service (NaaS) model?

Network-as-a-service (NaaS) is a cloud service model in which organizations rent networking services from a cloud provider instead of setting up their own networks. Users connect to their applications directly through a virtual network, and they do so via any Internet connection. SD-WANs still require hardware setup; NaaS only requires Internet connectivity.

Source: https://www.cloudflare.com/learning/network-layer/sd-wan-vs-mpls/

The Army's unified network concept is gaining momentum in 2023 capability builds

The U.S Army is expecting to see progress in linking its enterprise network to tactical formations in upcoming tactical network capability sets.

The Army has adopted a multiyear strategy involving the incremental development and delivery of new capabilities to its integrated tactical network, involving a combination of program-of-record sys-

tems and commercial off-the-shelf tools.

Currently, there are too many tools on the network that aren't integrated, interoperable or sustainable between the enterprise strategic network and the tactical network at the very edge. Leaders want to better connect these disparate systems to get to a truly singular unified network across the globe that will be centered around data and allow forces to have greater insights and visibility from theater to theater.

The Army is moving away from the brigade combat team-centric fight during the war on terror years that saw the brigade as the primary unit of action. Top nation-state powers that are more technologically sophisticated and transnational are forcing the Army to shift to higher echelons with the division as the unit of action.

"It will be a division and corps fight. Brigades will be maneuver elements. How do you maneuver a division network? How do you maneuver a corps network? How is it linked back to the enterprise so you can get to a strategic and operational effect at the point in time that a maneuver commander needs it anywhere on the battlefield."

"If you buy into data centricity, and we all should, where do you place that complexity? You don't place it at the lowest possible level. That's not how industry does it; it's not how the United States Army should do it. We've got to work our way through how do we raise that complexity up to the appropriate echelon where people can deal with it, hence, this division and corps centric approach. We do need to be able to plug into whatever infrastructure is available, whether it's commercial or military, do so securely and then reach back into that broader enterprise so that we can apply those strategic and operational effects to the point of need."

Those effects could be long-range precision fires, cyber effects, some electronic warfare effects or deep sensing. The Army of the future must be able to see something, feed it into the network and act on it in a timely manner. These efforts are also about reducing complexity and allowing greater visibility into the network, both from a tactical level all the way up to the strategic perspective.

Maj. Todd Donaldson, the communications officer at 2nd Armored Brigade Combat Team, 3rd Infantry Division, said "I want to be able to see what's on the network, what's not on the network, if something starts to drift be able to pull it back in, see how much data we're using and how congested that network might be at that time and how many users we have up on it." He added that as more capabilities are added to the network, such as radios and expanded mesh networking capabilities, he needs to be able to see everything to facilitate those capabilities and maneuver the network for the commander.

The Army has begun moving personnel and resources to regional cyber centers, division headquarters and corps headquarters to enable a DoDIN operations framework from the enterprise to the tactical level. This includes empowering newly created Expeditionary Signal Battalions-Enhanced, which support units that don't have organic communications capabilities.

Networking at the tactical edge. In the tactical sphere, the Army wants to reduce the network complexity and training burden for personnel.

Capabilities in the lower and upper tactical tier aren't well integrated like they are in the enterprise. Notions such as identity management and zero trust don't exist in the tactical space, which is something the Army is beginning to address.

Source: https://fedscoop.com/the-armys-unified-network-concept-is-gaining-momentum-in-2023-capability-builds/?__hstc=152211110.04cd1e11d6a7813d%E2%80%A6%201/

The Army Is Putting All Its Network Efforts Under One Roof

The U.S Army's shop in charge of battlefield communications will soon handle all of the service's network development and purchasing.

The move aims to streamline how the Army manages network integration, materiel development and acquisition since enterprise and tactical networks are no longer separate. The shift is also part of the implementation plan for the Army's 2021 unified network strategy.

The Army has been working to solve data, communications, and network challenges, particularly in the Indo-Pacific region. In addition to the satellite pilot, the Army is testing out a logistics dashboard this week as part of its cloud-based Command Post

Computing Environment.

They'll be able to see where everything is moving that's got their cargo on it, and they'll be able to click on it and tell you exactly what's in that ship or on that plane. The display will also use artificial intelligence for predictive analysis.

The goal is to move beyond sending messages and searching for information that could be buried in calendar entries or email attachments, what's often referred to as unstructured data.

Source: https://www.defenseone.com/defense-systems/2023/03/army-putting-all-its-network-efforts-under-one-roof/384119/

TECHNOLOGY

The military should turn its network innovation upside down

When it comes to network restrictions, the military may finally be catching up to the times.

The U.S Army's recent announcement that it's adopting Gmail, could be a sign that the service's outdated and stovepiped network restrictions may be loosening. We should remember that the bureaucracy is working hard to claw back the old way of doing business.

In 2018, the Pentagon banned mobile devices from secure areas. However, in reality, the ban was a last ditch attempt to stop the inevitable rise of mobile computing. This had the effect of driving the entire leadership structure of the department back to the 1990s desktop computing environment.

In Iraq, Afghanistan, and Syria, military commanders took on bureaucracies and built unprecedented jury-rigged networks to conduct combat operations with allies across commercial networks and systems. The operational flexibility, along with the innovative use of non-program of record commercial systems, far outweighed the risk of compromised information.

Once these wars ended and the innovators redeployed from combat operations, the older network security protocols took hold again, making it nearly impossible for units to tinker with commercial software and hardware to experiment and change how they fight. In the war in Ukraine, we're seeing firsthand that communications driven from the bottom-up work just as well as top-down communications on the battlefield.

It's time for the services to take a hard look at themselves and realise that if they can't keep top talents then something is wrong. In the world of information technology, everyone is not created equal. One superstar is worth a dozen marginal performers since returns are exponential. This is why the truly best make millions of dollars in the private sector. In the information space at the department, change should be measured in weeks and months, not years.

The Defense Department should abandon the top-down philosophy that currently permeates Joint All-Domain Command and Control, or JADC2. Instead, it should turn the requirements process upside down and let the operational warfighting commanders make the risk versus reward trade. They can see the benefits of technology on the ground and know better than anyone else at headquarters how it can be used. The Pentagon can assist in this effort by providing encryption capabilities, such as instant messaging system Signal, which reside on commercial phones.

The Pentagon should adopt a philosophy of protecting the data rather than protecting the network. For 50 years, the Pentagon manned the perimeter of its network with ever more sophisticated software, most of which is easily overcome by determined adversaries. Once inside the network, as we saw with the hack at the Office of Personnel Management a few years ago, the information is theirs for the taking. Implementing a 180-degree change in security would focus on protecting the information rather than the network. Encrypting the data where it sits and along the route it travels makes it irrelevant to then protect the pipes.

The actual network should be viewed as a space to preserve freedom of maneuver rather than as something to protect. Pentagon has to take charge and stop depriving our warfighters of the capabilities being exploited in Ukraine through its top-down approach to network innovation. Instead, it should turn its network innovation upside down and let our warfighters decide what risks to take.

Source: https://www.strategicstudyindia.com/2023/02/the-military-should-turn-its-network.html

To prepare for digital warfare, the military must run more digital exercises

Pentagon leaders have been clear that they view the digital battlefield as the battlefield of the future. And yet, much of the exercising the military does is still focused on traditional capabilities. It's time for the military to more regularly integrate digital tools as it trains for the next conflict.

Last month, the "Dragon Joint Operations Center" (DJOC) at Fort Bragg was packed with more than 400 people and humming with energy. Military operators, policy makers, technical experts, and industry representatives all milled around a wall of screens displaying an array of maps, live feeds, and software tools. CENTCOM and XVIII Airborne Corps had gathered the group for a large-scale exercise called "Scarlet Dragon Oasis," which included multiple organizations from across the Department of Defense, with dozens of assets dropping live munitions.

But the traditional assets and munitions were a sideshow to the real capability being showcased and stress-tested: the software tools and algorithms on the screens that are increasingly shaping the future of warfare.

From computer vision and synthetic aperture radar algorithms identifying rocket launchers for intelligence analysts, to digital workflow tools improving speed and precision of targeting teams, the exercise marked a critical step toward digital warfighting. Just as CENTCOM and XVIII Airborne Corp use events like this one to practice traditional warfighting, they are also using them to drive forward software capability at a speed previously unimaginable.

In 21st century conflict, digital warfighting is king. Automation software, statistical modeling tools, and AI algorithms provide an opportunity to orient ourselves faster, respond more precisely, and predict outcomes further out than our adversaries. If software is a key to success in future conflict, the military's exercises and preparations must adjust to reflect this reality.

The military exercises should increasingly reflect the pace and tempo of a rapid software lifecycle and should focus on solving digital friction points like data access, data preparation, software tool testing, and AI model refinement.

The US military transition to digital warfare will not happen without practice. Military operators need to train with software tools in the context of operations, give feedback to software developers, train with the tools again, and continue that loop to drive tool functionality and adoption across the military.

As the exercise drew to a close, discussion focused not on the flight paths of aircraft, or the dispersal of troops on the ground, but on the data requirements for software tools, the cloud networks available to operators, and the data sharing agreements required for future events. One conclusion was clear to everyone present: it was not the munitions and ordnance that provided explosive capability, it was the software behind them.

Source: https://breakingdefense.com/2023/02/to-prepare-for-digital-warfare-the-military-must-run-more-digital-exercises/?utm_campaign=Northrop%20Grumman&utm_medium=email&_hsmi=245252367&_hsenc=p2ANqtz-_usv8w1pnb4d72tRAelWMNzkPUt-68pLPYOI7c8TNoebE7oddv_ts2Zcha_BzAd5yyMzHmKCWecf2YOKCI7_fxYf9ol0w&utm_content=245252367&utm_source=hs_email

The Rise of Web 3.0: How the next generation of the internet could change everything

Web 3.0: The future of the internet, where security and decentralization take center stage, but will it overtake the current Web 2.0? Let's first compare the two other versions of the Web to see how things are about to change again.

Version I. The first web version was called Web 1.0. This was the earliest version of the internet. Web 1.0 offered a potential for digital communication and info-sharing. During the early days, there were only a few consumers of content. Personal web pages were everywhere, commonly static and read-only functions. Mainly run ISP web servers or other alternatives. Slowly over time static Web 1.0 pages were getting boring, only being one-sided.

Version: II. The version we are currently in now. Web 2. The second stage of the World Wide Web, changing static web pages to dynamic or user-generated content. This version of the web allows us to interact or communicate with each other through social media. Web 2.0, computers use HTTP with unique addresses to find the info which is stored in specific locations. Some examples are Twitter

and Facebook. Then came a problem of people that caused a new or better version of the web. Web 3.0.

Final Version: III. The future web. Web 3.0 is supposed to be the next generation of the web, in which users a connected through a decentralized internet run on a blockchain network. This will keep your information private and secure. The goal of Web 3.0 was to cut out the middlemen, allowing individuals to give services to each other without someone else controlling everything they use or utilize.

Will it overtake Web 2.0?. Companies like Google and Facebook have made some big bucks with Web 2.0. While Web 3 is still in its early stages, many experts believe that Web 3 has the potential to overtake Web 2 in terms of functionality and user experience. This is because it offers a more secure and transparent way of storing and sharing data. However, the adoption of Web 3 will likely take time, as it requires a significant shift in how we use and think about the internet.

Source: https://www.strategicstudyindia.com/2023/03/the-rise-of-web-30-how-next-generation.html

Russia's information war against Ukraine went stealth after Meta crackdown

Initially one of the most prolific purveyors of information operations on Facebook, Russian operatives have during the course of the war in Ukraine found themselves taking a "smash-and-grab" approach to gain influence online, substituting quality with quantity.

The new assessment of Russian influence operations comes from data that Meta, Facebook's parent company, released just as the war in Ukraine nears its one-year anniversary. Similarly, data out from other social media researchers concludes that Russian state-sponsored media influence operations aren't as potent as they once were. Instead of slowly building up an audience, influence operatives are now flooding the platform with low-quality accounts hoping some evaded Meta's detection.

Meta highlighted this behavior in two previously announced takedowns. In August, Meta took action against accounts tied to the pro-Russia troll army "Cyber Front Z," remarking that the operation's unsophisticated accounts "represented no distinct personas and were essentially fungible" and that the accounts were easily detected by automated systems. Meta followed with another report in September about the takedown of accounts belonging to a slightly more sophisticated and expansive Russia-originated network of more than 60 websites impersonating news organizations across social media platforms. Meta researchers described that campaign as "an unusual combination of sophistication and brute force."

Meta researchers speculate that the high-volume, low-quality nature of the campaigns may be influenced by the wartime nature of operations, which resulted in a hasty response from operators. According to a new Atlantic Council report on Russia's information operations to undermine Ukraine, Russian state media appeared to be caught off-guard by its de-platforming during the war and quickly sought other channels of influence, such as Telegram, a messaging app popular in both Russia and Ukraine.

While detecting the impact of Meta's enforcement against covert behavior can be harder to analyze, its shift toward demoting Russian state-sponsored content has been clearer.

The decline in influence operations on social media doesn't mean Russia will step away from these tactics. He expects that as war rages on in Ukraine, Russia will continue to adjust its approach.

Source: https://www.strategicstudyindia.com/2023/03/russias-information-war-against-ukraine.html

How Telegram became the battlefront of the Russia-Ukraine cyberwar

When Russia invaded Ukraine on February 24th, 2022, many warned that the conflict could escalate into a global cyberwar. A self-styled IT Army allied with Ukraine declared a counter-offensive. Yet, for all their bluster, these groups failed to impact the ground campaign significantly.

Instead, the war's digital presence manifested in other ways. A year after the war began, Cybersixgill investigated how the war echoed on the deep and dark web, the context of hybrid conflict, and how cybercriminals kept business humming.

Telegram has been the central deep web venue for the war. Many conversations about the war occurred on large, existing cybercrime channels, and

the invasion spawned many new channels.

Chatter on Telegram tended to follow events in the war. Many Telegram channels assumed a fiercely nationalistic tone. While groups aligned with Ukraine and Russia have carried out many successful attacks against many governmental and civilian targets, they are similar to traditional hacktivist methods, such as data compromise, defacement, and denial of service. It does not appear that any attack has provided even a minor tactical advantage, though they perform a valuable symbolic service in energising the base of supporters to the cause.

Telegram provided a valuable service to Ukrainian and Russian civilians alike. Many turned to channels to consume critical information, follow battlefield events, find humanitarian assistance and determine how to escape the fighting or mobilization.

Pro-Ukrainian forces have joined the fight. One prominent pro-Ukraine hacker collective on Telegram, boasting nearly 13,000 members, has called on Western hackers and groups to join in the fight against Russia. In the early days of the war, a Ukrainian cybersecurity official alleged that their ranks numbered over 400,000 Ukrainians and sympathizers from abroad. In the last year, they have claimed attacks against hundreds of Russian websites and military targets such as the Wagner group and even caused a traffic jam in Moscow by ordering dozens of drivers to the same site. Pro-Ukranian hackers also stole $25,000 in Bitcoin from a Russian dark web drug market and gave it to a Kyiv charity.

None of these attacks stands out as unique in scale and scope, and they have had little effect on the situation. Still, these attacks provide symbolic victories essential for morale and resilience. The nature of discourse on Telegram contrasts with discussions of the war on established dark web forums, which were generally more balanced.

Russians have also resorted to the deep and dark web to circumvent sanctions, enabling them to transfer funds and purchase goods from beyond Russia's borders. And even though Russian cardholders cannot purchase items outside of Russia, actors on underground forums can procure cryptocurrency or virtual and prepaid credit cards to make purchases abroad.

While many predicted that the war would herald a new era of cyber warfare, this has yet to materialize; there were many nationalistically-motivated attacks, but they were limited in scale and largely symbolic. Instead, the real impact of the deep and dark web on the war has been the ability to share news and humanitarian developments.

Source: https://www.strategicstudyindia.com/2023/03/how-telegram-became-battle-front-of.html

Software-defined Defence: Algorithms at War

Software and artificial intelligence (AI) are critical enablers of modern military operations, lead the evolution towards multi-domain operations, enhance interoperability among allied forces, and support the achievement of information superiority and decision-advantage against adversaries. Much of the functionality and performance offered by military equipment is already software-defined. As software now drives most of many military platforms' functionality, it is increasingly clear that it is not merely layered on to military hardware. Software is part and parcel of a weapons system.

The paper considers software-defined defence to be a fundamental architectural, organisational and operational principle of modern military operations. Software-defined defence entails a new logic for capability development which disaggregates sensors from effectors, software from hardware, and data from specific applications, while connecting them in data-centric, multi-modal, multi-domain, adaptative battle networks; to assess ongoing practices and processes in the development of defence software and AI/ML, and identify recurring challenges; to explore and assess the ongoing efforts towards software-defined defence in five country case studies – China, France, Germany, the United Kingdom and the United States – and how Sino-American strategic competition is shaping them.

Software-defined defence is based on four foundations:

- A changing relationship between military software and hardware, in which technological progress is faster in software than in hardware, and software-defined functionality of systems increasingly determines operational advantage in information superiority.,

- Software-defined defence requires a data-centric approach to developing new capabilities and systems-of-systems.
- It takes a human-centric approach to designing API-enabled end-to-end electronic workflows that enhance human capacity and safety.
- Software-defined defence regards advanced defence software and AI/ML as a core weapon capability and therefore places emphasis on the software component in early system design, as well as in subsequent upgrades.

As Sino-American strategic competition intensifies, with the integration of advanced technologies like AI/ML at its core, China's investment in software-defined defence will narrow the West's military-power advantage. The US is racing to meet this threat and is consistently attempting to accelerate the safe and responsible integration of defence software and AI/ML into its defence capabilities.

Source: https://www.strategicstudyindia.com/2023/02/software-defined-defence-algorithms-at.html

How AI can actually be helpful in disaster response

An open-source project that was sponsored and developed by the Pentagon's Defense Innovation Unit and Carnegie Mellon University›s Software Engineering Institute in 2019, xView2 has collaborated with many research partners, including Microsoft and the University of California, Berkeley. It uses machine-learning algorithms in conjunction with satellite imagery from other providers to identify building and infrastructure damage in the disaster area and categorize its severity much faster than is possible with current methods.

The program can directly help first responders and recovery experts on the ground quickly get an assessment that can aid in finding survivors and help coordinate reconstruction efforts over time.

Over the past five years, xView2 has been deployed by the California National Guard and the Australian Geospatial-Intelligence Organisation in response to wildfires, and more recently during recovery efforts after flooding in Nepal, where it helped identify damage created by subsequent landslides.

In Turkey, xView2 has been used by at least two different ground teams of search and rescue personnel from the UN's International Search and Rescue Advisory Group in Adiyaman, Turkey, which has been devastated by the earthquake and where residents have been frustrated by the delayed arrival of search and rescue. xView2 has also been utilized elsewhere in the disaster zone, and was able to successfully help workers on the ground be "able to find areas that were damaged that they were unaware of." Turkey's Disaster and Emergency Management Presidency, the World Bank, the International Federation of the Red Cross, and the United Nations World Food Programme have all used the platform in response to the earthquake.

This is an improvement over more traditional disaster assessment systems, in which rescue and emergency responders rely on eyewitness reports and calls to identify where help is needed quickly. In some more recent cases, fixed-wing aircrafts like drones have flown over disaster areas with cameras and sensors to provide data reviewed by humans, but this can still take days, if not longer. The typical response is further slowed by the fact that different responding organizations often have their own siloed data catalogues, making it challenging to create a standardized, shared picture of which areas need help. xView2 can create a shared map of the affected area in minutes, which helps organizations coordinate and prioritize responses—saving time and lives.

Since the code is open source and the program is free, anyone could use it. Rather than writing off or over-hyping the role that emerging technologies can play in big problems, researchers should focus on the types of AI that can make the biggest humanitarian impact.

Source: https://www.strategicstudyindia.com/2023/02/how-ai-can-actually-be-helpful-in.html

Clandestine U.K. Program Developed 3D-Printed 'Suicide' Drone For Ukraine

The United Kingdom has rapidly developed and flight-tested a number of "complex" drones that would be suitable for use by Ukraine in its conflict with Russia. A range of different capabilities was explored in the process, including surveillance drones and, most intriguingly, what is described as a "3D-printed delta-wing 'suicide' drone."

Some details of the rapid development program were recently revealed by QinetiQ, the U.K.-based defense technology company that works closely with the U.K. Ministry of Defense, especially on experimental projects and novel technologies.

Within just three weeks, the QinetiQ-led team was to demonstrate a series of new drones and related technology to senior U.K. Ministry of Defense officials, during a two-day event. This would include "flying experimental UAS and EW [electronic warfare] testing."

According to QinetiQ, the test projects "included C2 [command and control] and sensor payload[s] as well as VTOL [vertical takeoff and landing] UAS and a unique 3D-printed delta-wing 'suicide' drone."

The trials also included experiments on the ground, and use was also made of Boscombe Down's anechoic test facility, which can be used to assess how test specimens respond to radio-frequency energy, as well as providing a controlled environment to see how electronic systems and emissions interact with one another. The anechoic chamber was also used to expose the test specimens to command link jamming, an important consideration in Ukraine considering Russia's widespread use of offensive electronic warfare.

Ukrainian efforts to field a 'suicide' drone in broadly the same class as the Iranian-designed Shahed-136 used by Russia may well be gaining momentum.

Depending on the performance of the 3D-printed delta-wing drone tested at Boscombe Down, it's even possible that it could be the weapon they plan to offer Ukraine "longer-range capabilities."

The cost factor could also be important for any kind of drone rapidly developed for Ukraine, especially one that makes use of 3D printing. A UAS of this kind could potentially offer a much cheaper way of striking Russian targets at distance, or even overwhelming Russian air defenses if launched in considerable numbers. At the same time, the 3D printing method should allow the drone to be designed and developed in the United Kingdom, before production is launched in Ukraine, with only minimal preparation required.

Source: https://www.strategicstudyindia.com/2023/02/clandestine-uk-program-developed-3d.html

5G and EVs Crucial Technologies for 2023

The five most important areas of technology this yearwill be cloud computing, 5G, the metaverse, electric vehicles, and the Industrial Internet of Things.

In "The Impact of Technology in 2023 and Beyond: An IEEE Global Study," the global senior executives also weighed in on what areas could benefit from 5G implementation, what tasks would be automated by artificial intelligence, and how they plan to adopt the metaverse.

Almost 95 percent of the leaders said incorporating technologies that would help their organization become more sustainable and energy efficient was a top priority. The executives said they thought telecommunications, transportation, energy, and financial services would be the areas most affected by technology this year.

The impact of 5G. Theareas that will benefit from 5G include remote learning and education; telemedicine; live streaming of sports and other entertainment programs; day-to-day communications; and transportation and traffic control. About 95 percent said satellites that are used to provide connectivity in rural areas will enable devices with 5G to connect from anywhere at any time. The space satellites will be game-changers because they "enable leapfrogging off the need to build very expensive terrestrial infrastructure. They're also the ultimate virtual private network—VPN—for extrajurisdictional content access."

Automation through AI and digital twins. Nearly98 percent of tech leaders said routine tasks and processes such as data analysis will be automated thanks to AI-powered autonomous collaborative software and mobile robots, allowing workers to be more efficient and effective. They agreed that digital twin technology and virtual simulations that more efficiently design, develop, and test prototypes and manufacturing processes will become more important.

Meetings in the metaverse. Ninety-one percent said they plan to use the technology for corporate training sessions, conferences, and hybrid meetings. 5G and ubiquitous connectivity, virtual reality headsets and augmented reality glasses will be important for advancing the development of the

metaverse.

But for the technology to really take off, more innovations are needed in 5G and ubiquitous connectivity, virtual-reality headsets, augmented-reality glasses and haptic devices.

Source: https://www.strategicstudyindia.com/2023/02/5g-and-evs-crucial-technologies-for-2023.html

Smartphones Are Changing the War in Ukraine

Smartphones are making the war in Ukraine the most intensively documented in history, changing the shape of the conflict and transforming the world's understanding of it.

Each of the millions of devices in and around Ukraine are sensors that can provide data located to place and time. Their microphones and cameras can record and transmit sounds and images that depict the facts of war or provide tools for propaganda.

They have been deployed to identify military targets with the witting or unwitting involvement of users and to assess damage. They allow ordinary people the means to provide the military with targeting information, blurring the division between civilians and combatants. They are used by the Russian and Ukrainian public to raise funds for uniforms, drones or other military equipment, and by the Ukrainian military to guide drones and one device becomes the means by which you produce, publish and consume media, but also target the enemy.

The devices have a significant military utility. "Smartphones are a dream come true for the intelligence people and a nightmare for the counter-intelligence people,"the former because they can help to identify enemy movements, the latter because they can equally expose one's own side.

Chechen fighters known for their use of TikTok and Instagram to advertise their exploits, have on several occasions exposed their locations by using cellphones, drawing at least three strikes after Ukraine's military intelligence was able to locate them through their social-media posts.

One incident was at a school building in a rural part of Ukraine's Kherson region during Ukraine's fall offensive there. "The author of a video filmed his colleagues from different angles as well as the premises and territory of the school where they were located," the official said. Hours later, the building was hit with precision artillery. The strike killed around 30 fighters, Chechens said on social media.

The use of phones on the battlefield is a test of fundamental discipline. A really well-disciplined military will probably never be perfect in preventing people from using mobile phones and things like that. But they'll do a lot better than the Russians. Smartphones also give the home front a window into the battlefield and open up opportunities for information warfare.

Platforms such as Facebook, which is blocked in Russia, and VKontakte carry significant war content, but the service where much of the war is playing out on both sides is Telegram, an encrypted app that allows widespread distribution of content with almost no curation.

Another organization documenting the conflict from smartphone footage and other materials is Bellingcat. "People started following the conflict when average Russians began filming tanks being transported to the border in the lead-up to the invasion," said Bellingcat founder Eliot Higgins. Since the start of the war Bellingcat has begun operations consulting Ukrainian and international prosecutors on how to process and archive materials online to meet the standards necessary for them to be used in court. "It's the first open-source war."

Source: https://www.strategicstudyindia.com/2023/02/smartphones-are-changing-war-in-ukraine.html

AI agents take control of modified F-16 fighter jet

Artificial intelligence agents have demonstrated their ability to control a modified F-16 fighter jet during an initial round of test flights in California as the Defense Advanced Research Projects Agency moves forward with its Air Combat Evolution program.

"In early December 2022, ACE algorithm developers uploaded their AI software into a specially modified F-16 test aircraft known as the X-62A or VISTA (Variable In-flight Simulator Test Aircraft), at the Air Force Test Pilot School (TPS) at Edwards Air Force Base, California, and flew multiple flights over several days. The flights demonstrated that AI

agents can control a full-scale fighter jet and provided invaluable live-flight data," DARPA said in a press release.

The agency noted that a human pilot was onboard the two-seat aircraft to take over if anything went awry while the AI agents were in control during the test flights.The platform was recently upgraded with what officials are calling a System for Autonomous Control of Simulation (SACS).

"What we've done with investments from DARPA, with investments from the [Air Force] Research Lab is put it an autonomy core kind of brain on there. That's going to allow us to actually go fly autonomy [technology] and have a person still in the aircraft to intervene if we need to," Maj. Gen. Evan Dertien, commander of the Air Force Test Center, told reporters during a media roundtable in September at AFA's Air, Space and Cyber conference.

"We're heading down the path to have much more capability for uncrewed aircraft," Air Force Chief of Staff Gen. Charles "CQ" Brown said. "When you look at one of our operational imperatives — next-generation air dominance family of systems — we're going down the path of collaborative combat aircraft."

"As we look into our future budgets there's three aspects of this. There's the platform itself, there's the autonomy that goes with it, and then there's how we organize, train and equip to build the organizations to go [use that technology]. And we're trying to do all those in parallel. So we are thinking through aspects" of that,

Source: https://www.strategicstudyindia.com/2023/02/ai-agents-take-control-of-modified-f-16.html

How the Army is battle-testing cloud computing

The Army is in the midst of a significant shift in how it buys, builds and delivers technological capabilities to warfighters. At the crux of those plans is a cloud infrastructure called cArmy that can deliver communications, tools and sensor data so commanders can have a clear digital picture of the battlespace and make crucial decisions more quickly.

Paul Puckett, director of the Enterprise Cloud Management Agency, told that priorities this year focus on determining "the opportunity truly in the tactical domain to leverage cloud computing and then start to deliver really persistent mission command as a service for the Army…. That mission is going to drive us to invest heavily in understanding and then leveraging" cloud computing capabilities outside the continental U.S. while tying the enterprise and tactical domains together under a unified network.

Creating a global digital infrastructure. ECMA's efforts also build on the Army's digital transformation plan, which outlines how the service will use technology to change the way it conducts business operations and warfighting. Cloud really then becomes the global digital infrastructure that that mission is essentially executed on. Cloud infrastructure is a major element of several other recent DOD strategies related to data, software modernization and the vision for Joint All-Domain Command and Control.

Part of ECMA's mission is to design and deploy that digital infrastructure and determine the computing and storage footprint and the common services that will come with it, while also understanding its limitations and opportunities.

Experimenting with cloud in theatre. Those efforts are part of a broader strategy for cloud-enabled mission command. The Army has been testing its Command Post Computing Environment (CPCE), which provides a common operating picture so that commanders or their staffs can "look at one screen and be able to see all of the operational data that is important for his or her mission." The goal is to create greater structure and repeatability while enhancing training, operational readiness, and tactics, techniques and procedures.

Although continued experimentation this year seeks to answer technical questions, officials also want to address challenges related to doctrine and how the units use the capability. "There are certainly technical challenges to overcome, which we will," Paul said. "But we're experimenting so we're still trying to figure out what the unknown unknowns are as we leap into the cloud."

Making a foundational change. It's important to note that the Army isn't completely moving to tactical cloud, and the trick has been harmonizing cloud and non-cloud infrastructure.

"We're not advocating a wholesale move to cloud

with capabilities and not having anything at the physical location with the units. I think paramount to understanding across the Army when we talk about these things is they have to work in concert with the soldier on the edge. That is, part of the bigger technical challenges that we're having."

Source: https://fcw.com/defense/2022/05/armys-plan-tactical-cloud-computing/366931/

ELECTRONIC WARFARE

Aussie Space Command looks to electronic warfare, other tech to deter attacks on satellites

The head of Australia's Defense Space Command says her country seeks technologies to deter countries that might try to laze, jam, bump or move Aussie satellites. "We are working on making sure that we've got a level of capability so that we can deter attacks on our satellites, essentially through non-kinetic means so that we can have some impact. EW is a key tool."

One of the most interesting bureaucratic battles over time is sure to be between the Space Command and the Australian Space Agency, which controls policy and budgets for all launch in the country, and the Australia intelligence community, which controls the budget for its birds and ground stations.

"It's going to be really complicated as we go into the future, because it's fine when they're just an intelligence asset. But satellites are becoming more and more multi-mission," Bottom line for today: she is not responsible for the entire space budget and she doesn't control launch.

Source: https://www.strategicstudyindia.com/2023/03/aussie-space-command-looks-to.html

Armenia, Ukraine Lessons Shape New US Cyber/EW Unit

The U.S Army's year-old Cyber Warfare Support Battalion has "fully fielded" the first of 12 Expeditionary Cyber Teams, the head of Army Cyber Command said.

But Fogarty disagrees with the widespread wisdom that Azerbaijan defeated Armenia primarily through the power of drones. After all, before Azerbaijan's Unmanned Aerial Systems (UAS) could attack Armenian targets, they first needed to find them. They needed to electronically blind or disable their defenses. And above all, they needed commanders to pull together a wide range of information and quickly make the decision to strike – before the target moved on and was lost.

UAS certainly were important. However, the information aspects of this were critically important; the impact of spectrum was critically important, but it truly was the ability to converge all the capabilities across all five domains."

Lessons For All-Domain Ops. Rapid decisions, abundant information, using the electromagnetic spectrum, and converging forces across all five domains – land, sea, air, space, and cyberspace are crucial characteristics of the US military's evolving concept for Operations.

Part of the problem is habits developed over 20 years of counterinsurgency. In future conflicts, adversaries will jam our sensors, hack our networks, shoot down our drones, and frequently relocate key targets, so that when we spot something, we won't have the luxury of time. We need to learn to go after targets quickly.

When it comes to high-value targets, the likelihood is we will detect them for very short periods of time, so we're going to have to take our shots. To keep up this pace, we need to accelerate our processes, especially for how staff collate information and present it to commanders.

So what are the best-run command posts doing? They're pulling the different disciplines together into a single "information warfare" organization that can thrash out their different perspectives, put together their different puzzle pieces, and present a single, coherent picture with clear options for the commander. As information comes in from any of the different disciplines, they're able to do that coordination and integration to provide the boss a course of action that's actually viable.

Not all HQs have the expertise on hand to do this. For one thing, the Army's still standing up Cyber/Electromagnetic Activity (CEMA) cells across the force, which combine cyber, electronic warfare, and spectrum management expertise. Even when

the CEMA cells are in place, cyber/electronic warfare assets remain rare and specialized, which is the reason the Army is creating the 915th Cyber Warfare Support Battalion (CWSB), a central pool of expertise which will send out Expeditionary Cyber Teams to support local commanders as needed.

The first Expeditionary Cyber Team is now "fully fielded," Rather than a dozen identical ECTs, it is envisioned a high degree of custom-tailoring as each team matches up with a particular HQ it will support, with a different mix of assets for cyber attack, cyber defense, network and information operations.

Source : https://breakingdefense.com/2021/05/armenia-ukraine-lessons-shape-new-us-cyber-ew-unit/

Army EW Targets Foes For Infantry

As the Army rebuilds its long-neglected electronic warfare arm, it's finding simple tools can have a big impact – at the right place and time.

While EW is best known for *disrupting radio and radar*, recent wargames at Fort Benning showed tremendous tactical value to simply *detecting* hostile transmissions. EW troops following behind the frontline infantry used portable sensors to detect "enemy" units' transmissions a kilometer or more away, long before regular soldiers could see them.

"It provides that ground force commander early warning. It gives him more time to make those tactical decisions … than 'I'm walking thru the woods and I just received contact 300 meters away'" after the enemy opened fire.

That early warning lets the infantry fly a drone to confirm the report, get into prime position for any infantry attack, or artillery, call up a fire mission and destroy the enemy entirely… before the mission has even started."

The Cyber Center's eight-soldier detachment brought two types of radio-frequency sensors. One is mounted on a small drone (what the military calls a Group II UAS). While the Army wouldn't reveal the exact model, it's capable of launching from a few hundred feet of dirt runway. The drone has longer endurance than the smaller, hand-launched Ravens and Pumas in widespread Army service today. Once it gets aloft, it can see above ground clutter and detect transmissions much more easily than ground level sensors.

But you can't always count on drones being available, especially in bad weather or against an enemy with extensive anti-aircraft defenses. So the Cyber Center also brought ground-based sensors. This system can be carried by a pair of soldiers on foot and run off portable batteries, or it can be hooked up to a vehicle – in this exercise, ordinary pickup trucks – and operated off the vehicle's battery.

The Cyber Center gave some gadgets to the Fort Benning soldiers playing the enemy, aka the Opposing Force (OPFOR). They got multiple radio decoys, designed to give off misleading signals and to draw attention away from the real OPFOR. They also got a pair of advanced tactical radios capable of LPD/LPI transmissions, Low Probability of Detection/Low Probability of Intercept, to allow them to communicate without being so easily spotted.

Cyber/electronic warfare adds a new dimension to the battlefield beyond the traditional physical cues troops are trained on. That's another domain that platoon leaders, platoon sergeants, squad leaders, company commanders in the maneuver force are learning to utilize.

Source: https://breakingdefense.com/2021/02/army-ew-targets-foes-for-infantry/

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

John Sherman, the Pentagon's chief information officer, told a congressional panel "As we get ready for China, we better be able to fight and dominate the electromagnetic spectrum.

As we see the services starting to 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."

A conflict with either China or Russia would likely involve significant amounts of digital-first tactics, including jamming, spoofing, hacking and influence campaigns.

The U.S. Army and Air Force are trying to inject

new life into their respective EW arsenals after years of allowing them to atrophy. The Army in 2022 awarded multimillion-dollar contracts to Lockheed Martin and General Dynamics Missions Systems for what is known as the Terrestrial Layer System, which will provide soldiers a collection of electronic warfare, cyber and signals intelligence capabilities.

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

Top 10 radar and electronic warfare stories of 2020

The most popular radar and electronic warfare (EW) stories throughout 2020 covered subjects such as 6G stealth fighter planes, radar defense against hypersonics, dominating the electromagnetic spectrum, heterogeneous architecture and more. Check them out below.

6G stealth fighter planes: The quarterback of the kill web

Advancing radars for defense against missiles and hypersonic weapons

Raytheon, UTC merger closer to final with spinoff of subsidiaries

RF and microwave suppliers for military use face demands for innovation

Dominating the electromagnetic spectrum requires processing and AI innovation

Military AI innovation, SOSA hot topics at Embedded Tech Trends

Failure is not an option: the trends behind military test systems

Standard network interfaces, heterogeneous architecture, and COTS solutions: Recent trends in signal processing

Unmanned fighter planes (UCAVs) and the kill web

CMOSS is rolling forward