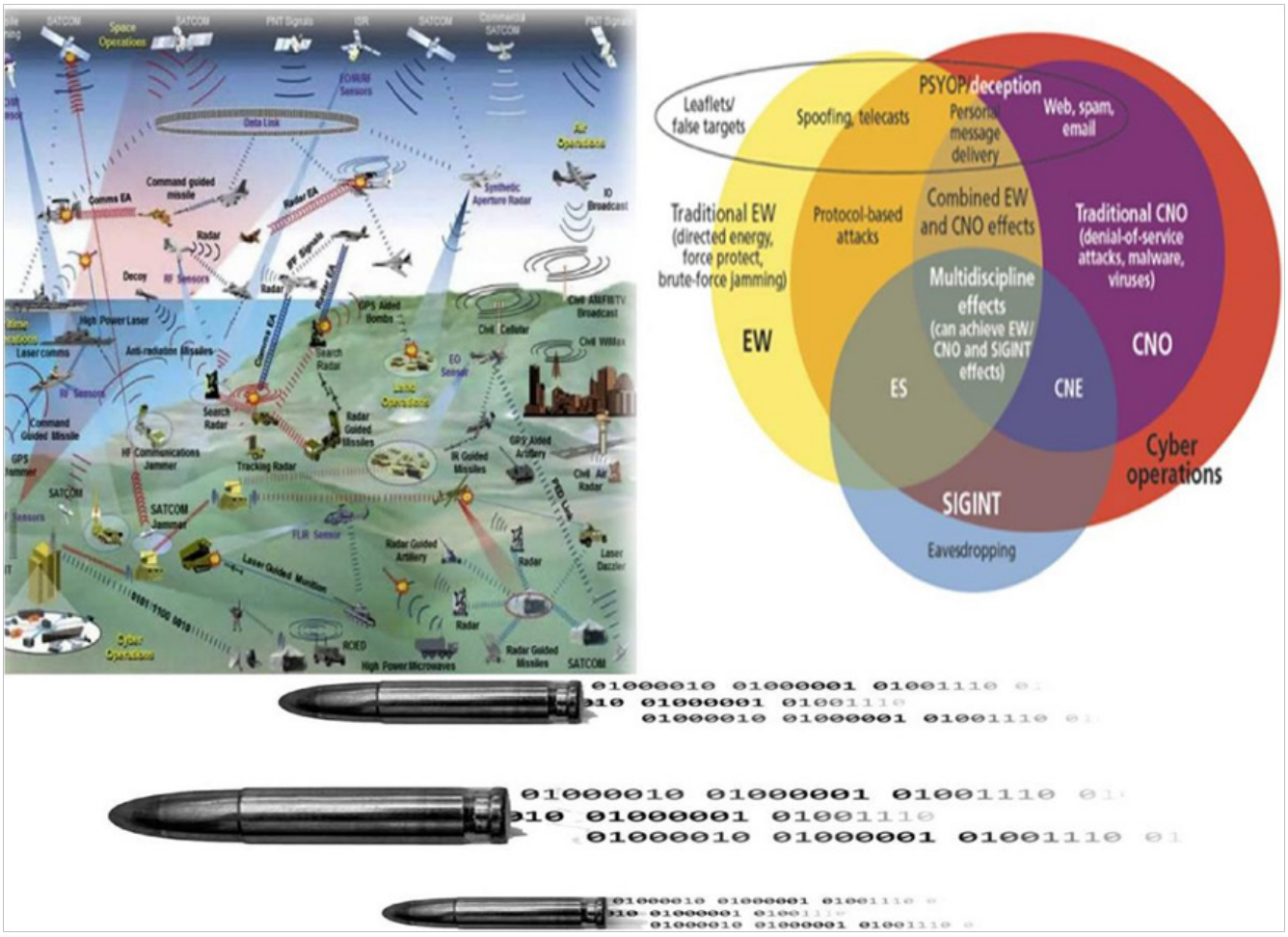
Cyber, Communications, EW & Technology (C2ET) Digest

By Maj Gen P K Mallick, VSM (Retd)



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

PUBLISHED BY STRATEGIC STUDY INDIA

Contents

CYBER

Ransomware trends: 2022.

Delinea has published its 2022 State of Ransomware Report, finding that there's been a sharp decrease in the volume of ransomware attacks, though the average ransom demand has gone up.

Despite the slowdown in attacks, the researchers found that the average ransom demand has gone up over the past year:

"It's important to note that while the volume of attacks appears to be decreasing, the average ransomware payment is increasing. The payments in cases worked by Unit 42 incident responders were nearly $1 million in the first five months of 2022, a 71% increase over the same period the previous year. On top of payments, companies are also paying for remediation expenses, downtime, and reputational harm."

Larger companies are much more likely to be victims of ransomware, as 56% of companies with 100 or more employees said they were victims of ransomware attacks.

Vigilance is on the decline. Organisations seem to be taking the ransomware threat less seriously than they did in 2022. The researchers found that most (76%) of organisations increase their security budgets only after they've suffered a ransomware attack.

Source: https://thecyberwire.com/stories/518a46a74c6e49e08f8b1f11eea7b30c/ransomware-trends-2022

Ukrainian hackers hacked the Russian Mail.ru service and made the database publicly available

The largest Russian hosting and registrar of domain names, Reg.ru, also suffered cyberattacks.

On the morning of January 13, Ukrainian hackers from NLB and DumpForums hacked the Russian Mail.ru service and Reg.ru hosting. The founder of the Hackyourmom group, Mykyta Knysh, announced this on Facebook. After successful cyberattacks, all the data of employees of Mail.ru and Reg.ru ended up in free access.

Source: https://odessa-journal.com/ukrainian-hackers-hacked-the-russian-mail-ru-service-and-made-the-database-publicly-available/

Cybercriminals Using ChatGPT to Build Hacking Tools, Write Code

Expert and novice cybercriminals have already started to use OpenAI's chatbot ChatGPT in a bid to build hacking tools.

The Israeli security company Check Point spotted(Opens in a new window) a thread on a popular underground hacking forum by a hacker who said he was experimenting with the popular AI chatbot to "recreate malware strains."

The hacker had gone on to compress and share Android malware that had been written by ChatGPT across the web. The malware could steal files of interest, Forbes reports.

The same hacker showed off an other tool that installed a backdoor on a computer and could infect a PC with more malware.

Check Point noted that some hackers were using ChatGPT to create their first scripts. Another user shared Python code he said could encrypt files and had been written using ChatGPT. The code, he said, was the first such one he had written.

Check Point said that it could "easily be modified to encrypt someone's machine completely without any user interaction." While ChatGPT-coded hacking tools appeared "pretty basic," it is "only a matter of time until more sophisticated threat actors enhance the way they use AI-based tools for bad."

ChatGPT's developer, OpenAI, has implemented some controls which prevent obvious requests for the AI to build spyware. However, the AI chatbox has come under yet more scrutiny after security analysts and journalists found it could write grammatically correct phishing emails without typos.

Source: https://www.pcmag.com/news/cybercriminals-using-chatgpt-to-build-hacking-tools-write-code

ChatGPT could be 'nuclear weapon' for cyber war

Artificial intelligence (AI) systems like ChatGPT could be devastating for the cyber security landscape with experts warning "it's only a matter of time" before AI-assisted attacks unleash cyber warfare on a previously unimaginable scale.

For the world of cyber security, in which a small team of underground hackers can send shivers down the collective spines of executives at

multi-billion dollar companies, the public availability of fast, accurate, and highly intelligent AI systems like ChatGPT threatens to make attacks even easier to pull off.

Making dynamic changes to malware as a way of bypassing antivirus detection is a scary prospect, especially when tools like ChatGPT enhance the skills of cyber criminals.

In the same way that guided code writing tools can help everyday developers do their jobs more efficiently, low code AI tools could lower the bar for would-be cyber criminals who want to eke out a living from extorting businesses or writing and selling ransomware.

"Today you can't get ChatGPT to give you a list of exploitable websites, but it's only a matter of time before something similar is connected to the internet, or to a search engine like Google – then you will have a nuclear weapon of cyber warfare."

"Imagine being able to say 'give me all the ecommerce websites in Australia vulnerable to an SQL injection' and it printing out a list of IP addresses."

For its part, OpenAI – creator of ChatGPT – is aware of potential misuse and said it is "eager to collect user feedback" to improve the AI.

Source: https://ia.acs.org.au/article/2023/chatgpt-could-be--nuclear-weapon--for-cyber-war.html

Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft

Millions of dollars-worth of cyber security help given by Microsoft and Amazon to Kyiv has dramatically reduced the number of cyberattacks by making it harder for Moscow to mount digital offensives.

Statistics published by Ukraine's government show that while the country suffered more than 2,100 separate cyberattacks last year, the frequency per month halved in the months following the outbreak of war.

It came as some of the world's biggest technology companies mobilised to support Kyiv, with Microsoft and Amazon donating around $400m of digital support between them. Big Tech's help was crucial in helping fend off the worst of the ongoing Russian cyber-assault.

Cyber attacks surged as Russian tanks rolled across its eastern borders in February 2022. Kyiv suffered nearly 290 separate assaults in that month alone, as Moscow deployed its digital weaponry alongside traditional firepower. However, by August, the number had dropped to around 140 attacks per month, according to figures from Ukraine's Computer Emergency Response Team.

Western governments and private companies have contributed hundreds of millions of dollars worth of digital support, with Amazon and Microsoft accounting for around £400m of backing.

Microsoft president Brad Smith said in November, "The continued defence of Ukraine depends in part on a critical digital alliance of countries, companies and nonprofits."

Amazon provided some of its Snowball devices for copying vital computer files out of Ukrainian data centres, allowing people to move crucial information online.

Jeff Bezos's company has also helped migrate Ukrainian government operations into its cloud, Amazon Web Services. Mikhailo Fedorov, Ukraine's deputy prime minister, said in December that this support had "made one of the biggest contributions to Ukraine's victory."

Google has organised charitable donation efforts during 2022 totalling $45m (£37.5m), it said, along with a further $5m raised by the advertising technology company's employees.

The company has also cracked down on Russian propaganda on Google Search as well as in YouTube videos.

US cyber security company Mandiant, which is a Google subsidiary, published research detailing how Russian hackers from a criminal gang nicknamed Turla had tried to compromise the computer servers of Ukrainian businesses. Booby-trapped USB sticks planted near the buildings of targeted Ukrainian companies were loaded with malware. Hackers hoped curious staff would plug them into computers and unintentionally unleash computer viruses saved on them.

Aside from major tech companies, Western governments have also provided crucial behind-the-scenes cyber security support to Ukraine.

Lindy Cameron, chief executive of GCHQ agency the National Cyber Security Centre (NCSC), said Whitehall has contributed around £6.5m in cyber support to Ukraine, including specialised antivirus software.

The US also proffered help. As well as defensive support, US Cyber Command has carried out offensive cyber operations against Russia. General Paul Nakasone told Sky News last summer: "We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations."

Source: https://www.telegraph.co.uk/business/2023/01/07/russian-cyberattacks-ukraine-halved-help-amazon-microsoft/

Pentagon Builds "Breakthrough" Cyber Security for Armed Combat Vehicles

Military vehicles, aircraft and ships in combat often have seconds, or even less, to identify and destroy an emerging enemy target, a technical ability now more possible due to the advent of Artificial Intelligence (AI)-enabled computing and multi-domain targeting systems. However, this paradigm-changing advantage can be complicated or offset by new risks. Extended multi-domain networks must be hardened against cyber threats across unprecedented distances and technical formats.

Instant, unanticipated cyberattacks can increasingly cripple military operations in a matter of seconds by jamming networks, intercepting and corrupting time-critical warfare data, intruding into and denying cyber network operations, derailing targeting sensors and weapons guidance systems, or simply disabling vital, interconnected operational networks.

This is the key reason why the Pentagon has massively revved up its cybersecurity emphasis in recent years by applying new technologies, seeking to "bake in" cyber resilience earlier in a system's development and prototyping process, and integrate a new generation of network protections and security protocols.

In October, several Pentagon and industry data-hardening or "information assurance" innovations were put to the test in the Army's Project Convergence "campaign of learning" in the desert at the U.S. Army Proving Ground in Yuma, Arizona. Multiple air, ground, manned and unmanned nodes, sensors and weapons were integrated with cutting-edge, AI-enabled systems to instantly process data and "pair" sensors to shooters. This process has become quite successful since the Project Convergence effort began in 2020, has massively expedited the decision-cycle necessary to find and destroy a critical target faster than an enemy can operate. This breakthrough networking technology, which has reduced the targeting process from 20-mins to 20-secs and introduced a new generation of multi-domain attack and high-speed Combined Arms Maneuver, is essential to high-speed warfare at what Pentagon leaders call "the speed of relevance."

The transport and analysis of previously unprecedented, massive amounts of data across multiple domains at breakthrough speeds naturally increases the need to "cyber-harden" networks and ensure cyber resilience. As cybersecurity continues to expand beyond historic perimeter-based security, the security of users, devices, networks, applications, services, and data continues to heavily rely upon a host of distributed and embedded cyber sensors and effectors designed to identify and thwart cyber attacks in near real-time. Preventing and stopping cyber attacks before they can negatively impact the operation of mission-critical systems and trying to stay ahead of continuously evolving cyber threats are the primary reasons why the Pentagon and its industry partners are making new efforts to pioneer breakthrough cybersecurity solutions.

"Applying Post Quantum Crypto to systems, networks, applications, and services will help address Quantum-enabled cyber attacks, but it will not automatically eliminate all cyber threats. One also needs to address other potential cyber attacks vectors, such as the underlying system hardware, operating system, storage, and networks. REDPro ZTX allows us to consistently and automatically enforce zero-trust policies and access controls across all aspects of a system, including users, devices, networks, applications, services, and data. For mission-critical systems, we typically start deploying zero trust security at the lowest possible level such as hardware and seamlessly extend monitoring and policy enforcement to the user space, including advanced user and entity-based analytics," said Dr. Torsten Staab, a Raytheon Intelligence & Space Principal Engineering Fellow and

Zero Trust Security R&D Lead.

Source: https://warriormaven.com/cyber/pentagon-breakthrough-cyber-security-armed-combat-vehicles-redpro-ztx-raytheon

Wiper Malware, Critical Infrastructure Threats Unleashed by War

Russia's invasion of Ukraine unleashed a concurrent cyberwar, with wiper malware and threats to critical infrastructure just two of the consequences that have spread to other nations. Wiper malware was considered an old and time-worn attack method until it made a comeback in 2022, as attackers introduced new variants. It's now back with a vengeance, and 2023 should see it begin to appear in more headlines.

There's even been growing evidence that data destruction could replace ransomware, as ransomware groups seek leverage to force victims to pay.

The new year will also likely bring an increase in catastrophic attacks on critical infrastructure, resulting in a major outage of some kind. There may also be digital civil disobedience cropping up in 2023, as people attack their own government sites or national infrastructure to protest against rising inflation or political turmoil. The U.S., for example, has recently seen a spate of attacks on power substations; capabilities unleashed by the war in Ukraine create the potential for much worse.

Source: https://www.esecurityplanet.com/trends/cybersecurity-predictions-2023/

RaaS and CaaS Continue to Grow

Beyond threat actors combining a computer worm with wiper malware and ransomware for maximum impact, there is growing concern about the possible commoditization of wiper malware for cyber criminals due to the maturation of Cybercrime as a Service (CaaS).

It becomes increasingly likely that malware developed by nation-state actors could be picked up and reused by criminal groups and spread through the CaaS model. Given its broader availability combined with the right exploit, wiper malware could cause massive destruction quickly, said Derek Manky, chief security strategist and VP of global threat intelligence at FortiGuard Labs.

2022 was notable for the spread of ransomware as a service (RaaS). Cyber gangs evolved their supply chains to the point where RaaS kits could allow those lacking technical skills to hold enterprises to ransom. The RaaS developers gain a cut of any successful heists.

That success has given rise to additional attack vectors being made available as a service through the Dark Web to fuel a significant expansion of cybercrime as a service. Seasoned cyber criminals can create and sell attack portfolios as a service to receive simple, quick, and repeatable paydays.

The LockBit threat group is the most significant source of ransomware and RaaS attacks, accounting for 44% of successful ransomware attacks in 2022, according to Trustwave SpiderLabs in a new report. Black Basta — with alleged connections to Conti, REvil and Fin7 — and Hive were the next most active ransomware groups. Whatever form they take, expect them to continue to make headlines in 2023.

Another new attack service, laundering as a service (LaaS), enables cyber criminals using machine learning (ML) to identify potential money mules to launder cash, reducing the time it takes to find recruits. This includes the deployment of automation to move money through layers of crypto exchanges, making the process faster and more challenging to trace.

Supply Chain Attacks, Dependencies Remain Issues

Software supply chain issues like the SolarWinds attack and the Log4j vulnerability have made supply chain security and software dependencies major issues in recent years. Expect the tangled combination of proprietary and open source software to remain a major threat in 2023 — with the hopeful note that we may see effective security solutions begin to emerge.

DigiCert predicts that 2023 will be "the Year of the SBOM," as the software bill of materials framework moves from a federal requirement to the commercial market. By listing every software component and library that went into building an application, as well as services, dependencies, compositions and extensions, SBOMs provide critical visibility that will speed their adoption, DigiCert predicted.

Security Products Face Greater Scrutiny

Software and applications won't be the only thing facing greater scrutiny this year. Economic headwinds and tighter IT budgets will mean that security products will get a much more rigorous evaluation by potential buyers.

Security buyers have long faced a lack of information on how well security products work, but 2023 will be the year buyers finally start doing something about it.

End Users Are Still the Trouble Spot

Despite the higher stakes and global threats, you can bet that the attack vectors will largely remain the same. The usual avenues, such as email phishing, credential compromise, and exploitation of vulnerabilities, will continue and even expand. Add social media scams and the growing use of convincing deepfakes and it becomes clear that users are under siege and constant vigilance is required.

The answer to attacks across so many channels lies in a shift in focus to creating a security culture within organisations across the globe, supported by security awareness training that covers these newer channels and the traditional avenues used by attackers.

Automation and Services Grow in Importance

"As the cyber risk for small and medium-size businesses keeps growing and more business owners see this as an actual threat to the existence of their business, the notion that every organisation needs a CISO — or a professional that is accountable for cybersecurity — becomes more popular. Organisations are realising that security tools are insufficient and that strategy to coordinate and govern the usage of these tools is critical." said David Primor, founder and CEO of Cynomi.

More Companies Ditching Cookies

Google has promised to eliminate third-party cookies in Chrome browsers by 2024, and others are following suit. If Google stops them, others have little choice but to go along with it or face a backlash from users.

From a user perspective, this is excellent news, as it results in more online privacy. Marketing personnel won't appreciate it so much since cookies have been used to gather a treasure trove of individual user data across sites, which typically ends up in advertisers' hands to create personalised and intrusive ads.

More Metaverse Means More Hacking

The proliferation of the metaverse means there are more opportunities for cyber criminals to perpetrate attacks. With developers creating virtual cities and vast online worlds, cyber criminals view these as a new set of attack surfaces to exploit.

The fully immersive experiences being made available online are growing so fast it is hard to keep up. Don't expect security best practices to be fully in place during the early rollouts. History repeats, and new technologies generally deploy security after attacks and breaches.

Avatars, as they are currently being implemented, could be used as a gateway to personally identifiable information (PII) by attackers. People can use their avatar to purchase goods and services in virtual cities. But that means they need fast access to digital wallets, crypto exchanges, NFTs, and various currencies and exchanges. Threat actors see this as yet another emerging attack surface.

"Biometric hacking could also become a real possibility because of the AR- and VR-driven components of virtual cities making it easier for a cyber criminal to steal fingerprint mapping, facial recognition data, or retina scans and then use them for malicious purposes. In addition, the applications, protocols, and transactions within these environments are all also possible targets for adversaries."

Source: https://www.esecurityplanet.com/trends/cybersecurity-predictions-2023/

Lt. Gen. Maria Gervais: Winning the Cyber Fight Requires Mastery of Sensing, C2, Data Processing

Electronic warfare — strategic, targeted attacks typified by cyber aggression and hacking of adversaries' technology systems — was first seen on the global battlefield at a large scale with Russia's instigating conflicts in Ukraine circa 2014. Destruction from EW was widespread then, with interceptions to communications networks causing fatalities and scrambling military organisation and planning. In one instance, a Ukrainian commander returned a call to his mother, which was tracked

through geolocation. The commander was slain by Russian artillery.

Russia's intervention in the Syrian Civil War saw intensified and more cunning EW strategies employed, a U.S. special operations commander attested that Syria was the world's most aggressive electronic warfare environment to date. U.S. Air Force pilots' communications were routinely jammed during their involvement.

The People's Liberation Army Strategic Support Force, has been established to handle EW, cyber and space operations, signalling the prevalence of these tactics. However, according to Lt. Gen. Maria Gervais, deputy commanding general and chief of staff of the U.S. Army Training and Doctrine Command, the most prominent display of EW right now conflicts with Russia and Ukraine.

Since February 2022, this ongoing war has shown "examples of how EW and cyber converge to [beget] sophisticated new kinds of fights—really a fight for speed and relevancy, which targets everything from tactical forces in the field to their command and control networks, all the way to national-level targets." Gervais shared these insights at the ExecutiveBiz Electronic Warfare Forum on Thursday.

Gervais asserted that EW attacks are predicated on exploiting vulnerabilities in the United States' sensing capabilities and its command and control architecture. This comes through incursions of soft power, which the Lt. Gen says can "provide an information advantage: a relative advantage, enabling a more complete operational picture."

Soft power aggression such as EW can additionally reap fear and panic in a government or populace, thereby bestowing power on the attacking nation. China and Russia want to use EW and other soft power tactics to "win without fighting," which would "separate the United States internally from its allies and partners and separate the elements of the joint force."

Modernisation in EW strategies does constitute innovation, but with that innovation comes a great deal of risk. Even though a unified communications network enables the U.S. military to thrive in "volatile, congested and contested environments.

Gervais remarked, "In the end, he or she who can sense the quickest, who can process and analyse information and data using artificial intelligence and machine learning to speed decision-making, and then distribute that the quickest to the multiple shooters…will win."

The test of fitness for dominance in the multi-domain environment will be measured by who is best trained in network, cyber and space tools. Leader development is crucial, and adopting an anticipatory rather than reactive approach to incoming cyber attacks.

Source: https://blog.executivebiz.com/2023/01/lt-gen-maria-gervais-winning-the-cyber-fight-requires-mastery-of-sensing-c2/

COMMUNICATION

Russia Versus Ukraine and the Role of Software-Defined Radios

Electronic warfare is now at the heart of modern warfare, a complementary component or even a replacement to traditional combat. Battles and wars can be won or lost based on defeating the opponent's technological advantage in the radio frequency spectrum and can also be used to infiltrate communications during times of peace. Radio frequency technologies—tactical radios, radar, positioning and navigation signals, weapons systems and various detectors to coordinate operations and find the enemy—are pivotal to military forces and have become increasingly important to disrupt, detect and deceive these adversarial capabilities.

Software-defined radios (SDRs) have proven critical to electronic warfare, signals intelligence countermeasures and counter-unmanned aerial vehicles. SDRs receive and transmit functionality over a wide tuning range, using multiple channels, high bandwidth and networking capabilities. The use of SDRs in various signals intelligence/electronic warfare receivers stems from their design flexibility, especially in terms of frequency configurability as well as interoperability with legacy equipment and waveforms.

As radio frequency communications are integral for civilian, military and overall general operations, radio-electronic warfare has been an inte-

gral part of breaking down or degrading enemy combat systems—or even regular systems. Take, for example, the R-330Zh Zhitel jammer, which can reportedly shut down all GPS, satellite communications and cellphone networks in the very high frequency and ultra-high frequency bands within a 25-kilometer radius. The command and control truck has signals intelligence equipment for detection, direction finding and analysis of radio signals using SDR-based technology.

According to a report by Thomas Withington on TheDrive.com, Russian forces in Ukraine have grounded Ukrainian unmanned aerial systems by jamming or spoofing GPS or other signals required for the SDRs in these systems.

On the battlefield, it's also become essential for SDR to be implemented into tactical radios for the ground soldiers and command and control communication. The SDR-based radio makes it possible to establish a tactical communications subsystem between commanding officers, ground forces and various other forces, all while ensuring a secure data exchange under many conditions, including in an electronic attack and countermeasures environment.

The radio also has a mode for frequency hopping—up to 20,000 hops per second—and thus severely hindering the possibility of communications countermeasures or signal intercept or direction finding by adversaries in this mode. On the Ukrainian side—nearly every Ukrainian ground unit was supplied with and trained on the NATO Single-Channel Ground and Airborne Radio System, which provides over 2,000 channels to choose from and replaces previous Russian-built radios that would be a liability due to espionage.

As with most military technology, the equipment deployed remains highly classified to ensure adversaries can't exploit weaknesses. Several electronic warfare and signals intelligence systems developed by Russia have been uncovered because Russian troops attempted to lighten their load as they advanced or retreated. Ukrainian troops discovered one of Russia's most sophisticated electronic warfare systems, the Krasukha-4 jammer developed by Russian state-owned company KRET.

NATO analysts report that Krasukha-4 is primarily designed to jam airborne or satellite-based fire control radars in the Ka and Ku bands, which is vital for intelligence, surveillance and reconnaissance programs, such as the U.S. E-8 Joint Surveillance Target Attack Radar System. Another system captured by Ukraine forces is the more advanced Borisoglebsk-2, which can jam drone guidance systems in the air and radio-controlled land mines on the ground.

While Russia was initially expected to have the upper hand in electronic warfare and military capabilities, Ukraine has been viciously fighting back with equipment supplied by allied forces, including SDR-based technologies. For example, Ukraine has been conducting electronic attack and countermeasures operations using counter-drone systems containing SDR transceivers provided by the United States. It has downed hundreds of Russian drones by jamming their GPS signals and, reportedly, even by damaging their electronics with high-power microwave beams.

Ukrainian forces have also exploited weaknesses of the large and powerful Russian electronic warfare systems, including their large size and the high-power transmission responsible for allowing jamming over a vast area. By using U.S. electronic support gear, Ukrainian troops have intercepted and detected transmissions from electronic warfare systems like the Leer-3 or Krasukha-4, reports Global Defence Technology. Ukraine also has directed rockets, artillery and drone counterattacks against the truck-borne Russian systems. It's often been the case that Russia's electronic warfare systems have interfered with their radio frequency technologies.

Elon Musk's Starlink proved to be an asset in combating jamming attacks on Ukrainian forces. Its constellation of low-orbiting satellites has provided broadband internet to more than 150,000 Ukrainian ground stations, including many of the Starlink ground station terminals, according to hackaday.com. At the heart of these terminals is an SDR of sorts for various means of steering the phased array antenna, tuning to near-microwave frequencies, and sending and receiving the data packets during use. As a further blow to Russia, it is very challenging to jam these connections. It is a far more difficult challenge to jam low-earth-orbiting satellites than geostationary ones.

Source: https://www.afcea.org/signal-media/cyber-edge/russia-versus-ukraine-and-role-software-defined-radios

TECHNOLOGY

AI Is Now Essential National Infrastructure

ARTIFICIAL INTELLIGENCE is evolving rapidly, with projects like OpenAI's DALL-E 2, Google's MINERVA, and DeepMind's Gato all pushing new technological boundaries. Until now, national governments have been slow to adopt this cutting-edge technology. In 2023, however, the opportunities to provide effective, targeted, and affordable services to citizens will prompt them to finally embrace AI, making government more transparent, accessible and effective.

In some countries, AI is already being used to improve people's interaction with the state. This year, the Estonian government launched a new AI-based virtual assistant called Bürokratt. Taking inspiration from Amazon's Alexa and Apple's Siri, Bürokratt provides Estonians with a voice-based way to navigate critical services provided by the state, such as renewing a passport or applying for benefits.

In Finland, a similar platform called AuroraAI was announced in 2018. It is part of a broader effort to provide Finns a personalised and autonomous service that helps them navigate various life stages, whether that be the birth of a child, marriage, or elderly care. This platform helps citizens interact with government departments and offers a proactive, concierge-like medical service that helps them renew prescriptions or even notifies them of new health risks.

In 2023, governments will also finally start using AI and big data to tackle some of society's biggest problems. In education, for instance, companies like the UK-based CENTURY Tech are helping governments deliver personalised learning. Its system essentially acts as a personal tutor, complementing the in-person teaching a child gets by tracking progress and analysing areas for improvement.

Done right—and with the proper privacy protections in place—such projects can generate a trove of data that is a competitive asset, helping research and innovation flourish. Consider the UK Biobank, one of the most essential government-led biomedical initiatives worldwide. This project has produced a public database with the genetic information of more than half a million people. To this date, it has been accessed by nearly 30,000 researchers from 86 countries, helping AI and biotech startups create new drugs and therapeutics.

For governments to fully deliver on the promise of AI, however, they will need to invest. Soon, a comprehensive digital infrastructure—which includes national computing power, a distributed cloud, and an interoperable set of applications and machine-readable legislation—will be as crucial to a country as roads, rail, and public water supply. In 2023, more and more countries will accelerate the building of such nationwide digital architectures, allowing them to deliver more AI-powered responsive services that cater to the individual and help the population at large. In 2023, bold governments will be making this move—and they will be examples to follow for the rest of the world.

Source: https://www.wired.com/story/digital-infrastructure-artificial-intelligence/?bxid=62c532e76c18539e1700c832&cndid=70226613&esrc=growl2-regGate-0321&mbid=mbid%3DCRMWIR012019%0A%0A&source=EDT_WIR_NEWSLETTER_0_DAILY_ZZ&utm_brand=wired&utm_campaign=aud-dev&utm_content=WIR_Daily_122622&utm_mailing=WIR_Daily_122622&utm_medium=email&utm_source=nl&utm_term=P2

The Army's Distributed Command Posts of the Future Will Need More than Videochats

A recent U.S Army exercise sought largely to test ways to distribute command and control—to, say, replace big command posts with small cloud-connected teams scattered around the Pacific region. But the I Corps' IT team discovered just how much of the service's vision of future warfare will depend on turning a morass of data into well-structured bundles.

The experiment was set up to use unstructured data, the kind that accounts for much of the information the Army moves around: PDFs, PowerPoint slides, emails, calendar invites, etc. It takes a lot of human brainpower to assemble this information into forms that can help commanders make decisions.

Col. Elizabeth Casely, who runs I Corps' communications, networks, and services said, "That's not good enough for the future battlefield. We're now

beginning to understand how much we were using, I would say, human-in-the-loop cognitive processing to achieve a result that could be easily achievable if we had exposed data that was structured in some way, [if] we had access to a data environment, or a tool if you will, to put it in. And then the big lift that has to occur inside the Corps is this data-engineering lift: this move from unstructured to structured. Because you can't begin to imagine what questions you might ask of the data until you begin to understand what sorts of things you have access to."

Toward "distributed mission command"

Headquartered at JBLM in Washington state, I Corps supports operations in the vast U.S. Indo-Pacific Command, whose area of responsibility stretches over more than half the Earth's surface. Like much of the U.S. military, the Corps has been re-thinking its methods as a potential fight with China looms. Key to these changes is a new concept called "distributed mission command," intended to allow small teams in various locations to perform all the functions of today's big command posts.

This requires better data networks, better cloud storage, and a lot more.

"We're responsible for making sure that we have the transport in place…make sure that transport is widely accessible, highly available, simple and intuitive to connect to and move data all over the place and in a way that the warfighter intends to use the network. The idea is to be able to have a tactically-enabled cloud environment, connect, and then have a predetermined architecture in mind about where we would need to have edge computing devices."

Bandwidth is a challenge. Latency is a challenge. There's the need to make sure the data can be understood as it passes between systems and organizations. That means developing standards for data, first within a given function, like intelligence or fires, and then across them. Not only does this help tie the systems together and turns the data into useful input for machine-learning or artificially intelligent tools.

A data-centric journey

I Corps' recent exercise, had the goal of duplicating a distributed architecture. One of the lessons was that they need a capability that converts unstructured data into structured information.

Data exists in varying forms all over the Corps. How do we start to pool all of that together, get it into an environment and then apply the appropriate talent to it. Then, ultimately, do what we're all trying to do—answer a question. All three of those steps are linked. You can't do one without the other.

Other challenges observed during the exercise include problems with authentication, latency, and the result of too much network chatter.

"The Corps will have to increase its software development investments significantly. But as a first step, we would like to use cloud-native industry best practices to deploy and configure workloads as code also called infrastructure as code. This will allow us to rapidly, securely and consistently deploy mission command capabilities in these automated DevOps pipelines, consisting of multiple stages and tasks. So you install it, connect to a database, provision the accounts, conduct the security scanning," Casely said. And if something breaks along the way, developers can go back and pinpoint the failure.

The Corps also plans to create an unclassified information-sharing system for its mission partners.

Source: https://www.defenseone.com/defense-systems/2022/11/elizabeth-casey-first-corps-communications/379333/

Why Military Leaders Need to Rethink Battlefield Intelligence in a Smartphone Era

Ukrainian forces recently leveraged Russian phone signals to strike a temporary base in the occupied city of Makiivka, killing dozens. The Russian Defense Ministry subsequently issued a rare statement attributing the unprecedented loss to the widespread, albeit unauthorised, use of personal phones. While powered on, the phones had been pinging Ukraine's cellular network, allowing Ukrainian forces to triangulate precise location information.

The universal adoption of smartphones and social media has revolutionised the dynamics of surveillance in a theater. Social media requires few intermediaries, meaning that members of the armed forces can—and do—use smartphones to participate in online dialogue without oversight. More

data—such as locations and information about habits, health, relationships, religious beliefs, and more—is being generated and shared than ever before. Although militaries often instruct soldiers in the field not to utilise personal phones, the rules are regularly ignored.

Net Politics

Military commanders historically exercised a high degree of control over the information flowing from and to the troops under their supervision. In the pre-digital days, soldiers who wrote letters to send by postal mail understood that their letters were subject to inspection by censors. Today, the sheer volume of digital information that can be conveyed by service members either intentionally (e.g. through social media posts) or inadvertently (e.g. through the use of apps that send data to the cloud) makes it impossible as a practical matter for military leaders to maintain full oversight over the flow of information. Military leaders in turn have little understanding of the information that their subordinates inadvertently make available to adversaries.

Analysing the sheer volume of available data is incredibly challenging. Securing smartphones against information leakage is difficult (due to the range of signalling protocols, each with its own exploits) and impossible when smartphone owners themselves post on social media or convey sensitive data to third parties. Attempts to curb personal phone use among troops—such as the threat of military jail for Russian soldiers that violate smartphone use and social media policies—have been unsuccessful in preventing their use.

Military leaders have occasionally banned phones altogether: In 2020, U.S. Army paratroopers deploying to the Middle East were prohibited from carrying personal devices, in part because of the cyber capabilities demonstrated by Russia, China and Iran in the region. However, South Korea, which had once outright banned personal phones (and strictly enforced the rules), eased its policy in 2018 due to dampened morale and widespread frustration.

Militaries need to adapt to the realities of an era in which smartphone and social media use by soldiers is inevitable. Part of the solution also requires rapidly detecting and localising unauthorised transmissions from within friendly ranks while abroad and creating technical frameworks to enforce security policies. Militaries are already monitoring their own troops—Israel has been eavesdropping on its soldiers for over a decade, and the United Kingdom claims to disable personal devices that breach protocol—but capabilities are neither comprehensive nor consistent.

More crucial, however, is educating soldiers that some forms of smartphone use, although seemingly innocuous and vital for morale, expose far more than expected. Military leaders should make digital hygiene a key component of programs like Advanced Individual Training, where soldiers should be taught the basics of signals intelligence and how they could avoid the most glaring collection opportunities. This program could be used to build a culture of awareness throughout the military by conveying sobering real-world examples that illustrate the potential consequences of unsafe smartphone use. The Israeli Defense Forces' approach of prioritising digital technologies and appreciating its dangers could serve as a potential model.

Despite their troubling vulnerabilities, smartphones on the battlefield do enable immense tactical opportunities. A key challenge for modern militaries lies in maximising the benefits of the extraordinary communications and computational capacity of current and next-generation smartphones while sufficiently mitigating the equally remarkable cyber and intelligence risks involved in their use.

Source: https://www.cfr.org/blog/why-military-leaders-need-rethink-battlefield-intelligence-smartphone-era

Ukraine Proves U.S. Troops Need Quick Access to Commercial Technology

Russia's invasion of Ukraine has all the traditional hallmarks of a conventional war, with troops and tanks on the ground and airstrikes from above. But even as today's battles resemble old wars, Ukraine has been successfully defending itself beyond expectations in part because of the courage and determination of its people, who have used new technology in ways that are changing how wars are fought.

Historically, the speed and accuracy of the information that reaches decision-makers have been an Achilles heel of armies. But Ukraine is showing the world how a smaller force can fend off a larger military foe using a readily available mix of military

and commercial technologies, especially for communications. The Russia-Ukraine war is a warning. In future conflicts, our nation needs far more public-private collaboration, and fast.

When Russian strikes in early 2022 hit Ukraine's infrastructure and knocked out the ability for Ukrainian military leaders to communicate with their troops, Ukraine moved fast to use commercially available, satellite-based internet access via Starlink and logistics services like FedEx to reopen lines of communication. Since then, hundreds of thousands of Ukrainian civilians have used technology to report critical battlefield information to the government, such as enemy troop movements and local intelligence.

On the battlefield, soldiers with limited weapons use handheld tablets and mobile devices to get real-time satellite data to target their efforts. Algorithms help Ukrainian troops rapidly determine the most urgent threats and opportunities, from the enemy's exact location to the weapons most likely to prove effective in a strike.

Traditionally, intelligence about the enemy would be communicated up the chain of command and then down through the military command structure. But Ukrainian troops are accessing this information immediately via an array of drone and satellite imagery, some of it from publicly available sources. Having that data can be the difference between an army's commanders deciding to advance or retreat from an attack.

Many of these practices are not new; armies using new technologies to win battles is as old as war. And certainly, we will continue to need clearly defined intelligence chains of command. But as Joint Chiefs Chairman Gen. Mark Milley recently said to the *Washington Post*, "We are witnessing the ways wars will be fought and won for years to come."

Military leaders should continue working to bridge the gap between the public and private sectors in ways that will help ensure the spirit of innovation is put to use, advancing a nation's defence and security. The leaders of most innovative companies must also see the MoD as a potential customer and feel obligated to assist in our country's defence regardless of profits. Patriotism requires more than waving a flag.

Red tape and bureaucracy often prevent the armed forces from capitalising quickly on technological advantages, which denies our service members capabilities.

The past year in Ukraine has underscored how wars will increasingly be won and lost based on which side proves more adept at developing, deploying, and scaling advanced technology.

Source: https://www.defenseone.com/ideas/2023/02/ukraine-proves-us-troops-need-quick-access-commercial-technology/382491/

ELECTRONIC WARFARE

Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones

The Russian military's failures in Russia's wider war on Ukraine are almost too numerous to list. Too many attacks along too many sectors thinned out Russia's best battalions. Too few infantry to screen the tanks. Inflexible air support. Artillery batteries bombarded too many empty grid squares. And perhaps most importantly: inadequate logistics for what would become a long, grinding war.

But it's important to note where the Russians succeeded. Consider the Kremlin's battlefield electronic-warfare troops for a rare picture of Russian military competence.

Amid the chaos of the Russian army's initial push into Ukraine starting in late February, it took a few weeks for the Russians to deploy their extensive jamming infrastructure. But once they did, they began deafening and confusing the Ukrainians' most sophisticated systems—particularly their drones—in numbers that surely startled Ukrainian commanders.

The electronic suppression of Ukraine's unmanned aerial vehicles blunted one of Kyiv's most significant advantages in the early months of the war. The Ukrainians counted on superior intelligence—provided mainly by UAVs—to make their smaller artillery arsenal more precise than Russia's larger arsenal of big guns and rocket launchers.

But the Russians' electronic warfare prevented those drones from navigating and communicat-

ing—and deprived the Ukrainians of the precision they were counting on. "The defeat of precision was critical to unit survival" for the Russians, analysts Mykhaylo Zabrodskyi, Jack Watling, Oleksandr Danylyuk and Nick Reynolds explained in a study for the Royal United Services Institute in London.

Analysts anticipated the Russians' jamming operations. The Organisation for Security and Co-operation in Europe, which monitored the Moscow's military buildup ahead of the February invasion, noted the deployment of a large number of electronic-warfare systems in Russian-occupied eastern Ukraine.

They included TORN and SB-636 Svet-KU signals-intelligence systems that can pinpoint Ukrainian units by tracing their radio signals, RB-341V Leer-3s that combine Orlan-10 drones carrying cellular-jamming payloads with a command post on a KamAZ-5350 truck, R-934B Sinitsa radio-jammers and R-330Zh Zhitels that block satellite links.

The Russian electronic-warfare force had become so potent that OSCE struggled to keep its drones in the air. The organization reported a sharp increase in jamming. OSCE's UAVs experienced signal-interference on 16 percent of flights in February that year, 28 percent in March and 58 percent in April.

Russia's E.W. systems work best when their operators have plenty of time to set up and coordinate different functions. This is why Russian E.W. was so fearsome in eastern Ukraine's Donbas region, where Russian and separatist forces held roughly the same positions for much of the seven years between 2015 and the current, wider war.

That also is why Russian jamming didn't work very well in the first few weeks after the Russians attacked in February. Russian battalions attacked and retreated too quickly for the E.W. troops to keep up. That finally began to change in March and April, as battered Russian forces finished pulling back from Kyiv Oblast in central Ukraine and repositioning in the east.

The Ukrainian air force's fighter pilots were the first to feel the effects of escalating Russian jamming. "As Russian E.W. complexes began to be deployed systematically, Ukrainian pilots found that they often had their air-to-ground and air-to-air communications jammed, their navigation equipment suppressed and their radar knocked out," Zabrodskyi, Watling, Danylyuk and Reynolds wrote.

Russian jammers soon were thick on the ground in the east. "With the concentration of effort on Donbas, Russia set up E.W. complexes with up to 10 complexes per [13 miles] of frontage," the RUSI analysts noted. "Collectively, these complexes effectively disrupted navigation along the front and conducted direction finding to direct artillery and electronic attack against Ukrainian aircraft and UAVs."

Ukrainian brigades and batteries depended on two broad drone types to find Russian forces and walk in artillery: small, hovering quadcopters and octocopters; and larger, fixed-wing UAVs such as the Turkish-made Bayraktar TB-2. As Russian jamming confused GPS and severed radio links, these drones started dropping like flies.

"The average life expectancy of a quadcopter remained around three flights," Zabrodskyi, Watling, Danylyuk and Reynolds wrote. "The average life expectancy of a fixed-wing UAV was around six flights" and, "in aggregate, only around a third of UAV missions can be said to have been successful."

Of the thousands of drones the Ukrainians possessed in February, 90 per cent were shot or crashed by summer, according to the RUSI analysts. This compelled authorities in Kyiv to plead with Ukraine's foreign allies for replacements.

The drone massacre complicated Ukrainian fire control, making Ukraine's artillery batteries less accurate—therefore buying time for Russian troops to reconsider in the east and prepare for the summer's fighting.

That the summer campaign ended badly for the Russian army doesn't change the fact that the E.W. troops did what the army asked of them: filled the air with electronic noise. "In the early phases of the fighting in Donbas when the [Ukrainian armed forces] had few precision systems, Russian E.W. reduced the effectiveness of these systems," Zabrodskyi, Watling, Danylyuk and Reynolds concluded.

If anything, the E.W. troops were too successful. They actually jammed more than a few Russian drones, too. "The Russians suffered extensively from these systems having an equally noticeable

effect on its own troops," the RUSI team noted.

Source: https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=e8c1c7a575cf

Outsmarting Agile Adversaries in the Electromagnetic Spectrum

- The U.S. Air Force's electronic warfare integrated reprogramming (EWIR) enterprise examines intelligence on adversary threats that emit in the electromagnetic spectrum (EMS) (in particular, radars and jammers) and configures electronic warfare software and hardware to enable aircraft or other resources to react to and/or respond to adverse changes in the EMS environment. With the growing advancements in U.S. adversaries' electronic warfare assets that enable complex and diverse EMS capabilities, identifying, tracking, and responding to these threats requires much faster updates than the existing EWIR enterprise was designed for. The research team conducted four interrelated technology case studies that together comprise the fundamental elements necessary for creating a near-real-time, autonomous, inflight software reprogramming capability and, more specifically, artificial intelligence–enabled cognitive electronic warfare capabilities—the use of machine learning algorithms that enable platforms to learn, reprogram, adapt, and effectively counter threats in flight. The research team also highlighted important continuing roles for the existing EWIR enterprise even as the U.S. Air Force moves toward a cognitive future.

Key Findings

- To remain competitive and adapt to changing threats, U.S. Air Force (USAF) systems that operate in the EMS must be capable of rapid reprogramming (including evaluating the environment, detecting adversary activity, and synthesizing an appropriate response), at least on the order of seconds to minutes, to effectively react to the most advanced threats.
- Agile software solutions, hardware upgrades, data engineering, and interoperability with other systems are all required to achieve the needed speed.
- Accompanying changes in policy, organizational mission alignment, personnel and computing availability, and personnel professional development are also needed.

Recommendations

- The USAF should start working today to accelerate and integrate technologies needed to realize cognitive electronic warfare. Steps include supporting a shift toward updated software architectures, such as containerized microservices, that would allow faster deployment of capabilities and needed updates to increase the reprogramming speed and provide support for the deployment of cognitive electronic warfare algorithms on platforms in the future; enhancing onboard high-performance computing; expanding experimentation and early technology adoption; prioritizing policies and technologies that will allow better data collection, standardization, classification, access, and integration processes; and ensuring coordinated investment and implementation of these activities given high interdependencies among key technologies.
- The USAF should also take immediate steps to adopt new software deployment architectures to enable faster fielding of capabilities and implement rapid and airborne mission data file updates in theater. This necessitates changes to existing policy; personnel professional development; review of requirements; and investments in software architecture standards, onboard processing, and computing and connectivity by the aircraft during the mission.

Source: https://www.rand.org/pubs/research_reports/RRA981-1.html