Cyber Center of Excellence

Unclassified Threat Read Book

01 - 15 May 2023

Prepared by: Threat Management Office
CCoE
Fort Gordon, GA 30905

POC: Threat Management Office, jeffrey.t.hardimon.civ@army.mil or kevin.m.bird.civ@army.mil 706-849-9259

Table of Content

Cyber

Electronic Warfare

Information Advantage

Signal

5. Zero Trust vs. Zero-Knowledge: What's the Difference? – 06 MAY
6. US Army revisiting how it develops, deploys advanced networking gear – 05 MAY
7. Air Force reaches out to industry to apply quantum computing and communications to C4ISR applications – 04 MAY
8. Zero trust would have helped prevent Pentagon leak, CIO Sherman says – 03 MAY
9. US Cyber leader loo to AI to augment network activities – 03 MAY
10. Connectivity will 'make or break' US military use of AI, official says – 28 APR

Items of Interest

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. Chinese general calls for military to prepare for 'hybrid' modern warfare – 15 MAY
4. Impoverished Communist Nation 50 Years Ago, China Now Challenges the Might of US & Japan – 15 MAY
5. Russia Attacked Patriot System In Ukraine With Hypersonic Missiles But Were instead Shot Down By the Same Patriot – CNN – 13 MAY
6. Foreign Reflections on U.S. Exercises and Operations, 12 May 2023 - 12 MAY
7. Ukraine Begins Phase-1 Of Counter Ofensive Ops Against Russia Begins Hitting Command Centre, Weapons Depot – CNN – 12 MAY
8. Putin tells WWII event West is waging a 'real war' on Russia – 09 MAY
9. Ukraine Isn't Buying Wagner Boss's Tirade About Pulling Out of Bakhmut – 05 MAY
10. Foreign Reflections on U.S. Exercises and Operations, 4 May 2023 – 04 MAY
11. RGF to Receive New Wearable Drone Detector System – 04 MAY
12. Drone Attack On The Kremlin In Moscow (Update) – 03 MAY
13. Airship Spotted Outside Giant Secretive Hanger In China – 01 MAY

Cyber

1. **North Korean hackers stole $721 million in cryptocurrency from Japan – Nikkei (Reuters, 15 MAY, Satoshi Sugiyama)**

   Hacker groups affiliated with North Korea have stolen $721 million worth of cryptocurrency assets from Japan since 2017, the Nikkei business daily reported on Monday, citing a study by U.K. blockchain analysis provider Elliptic

2. **US cyber team unearths malware during 'hunt-forward' mission in Latvia (C4ISRNet, 10 MAY, Colin Demarest)**

   A team of U.S. cyber specialists discovered malware during a three-month deployment to Latvia while scouring digital infrastructure for weaknesses.

   The so-called hunt-forward operation, conducted by the Cyber National Mission Force, was the second such endeavor in the former Soviet state. It wrapped up "recently," U.S. Cyber Command announced May 10.

3. **"Shared threats, shared understanding": U.S., Canada and Latvia conclude defensive Hunt Operations (U.S. Cyber Command, 10 MAY, Cyber National Mission Force Public Affairs)**

   A team of cyber experts from U.S. Cyber Command's Cyber National Mission Force (CNMF) recently returned from a hunt forward operation in Latvia.

   During the three-month long operation, the U.S. team worked with CERT.LV, the Information Security Incident Response Institution of the Republic of Latvia – on a defensive cyber threat hunting operation focused on the Latvian critical infrastructure. CERT.LV plays a critical role in safeguarding Latvia's cyber ecosystem and supporting the country's digital transformation.

   The U.S. team worked in tandem with Canadian Armed Forces and Latvian allies, to support their defensive operations, as well-- marking the first time American and Canadian forces have conducted hunts simultaneously.

4. **U.S. and Allies Identify and Expose Russian Intelligence-Gathering "Snake" Malware (U.S. Cyber Command, 09 MAY, Cyber National Mission Force Public Affairs)**

   U.S. Cyber Command's Cyber National Mission Force, along with interagency and foreign partners, have identified infrastructure for Russian Federal Security Service (FSB)'s "Snake" malware in over 50 countries across North and South America, Europe, Africa, Asia, and Australia, to include the U.S., and within Russia.

   The agencies, which include the National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Canadian Cyber Security Centre (CCCS), Australian Cyber Security Centre (ACSC), and the UK's National Cyber Security Centre (NCSC), publicly released the joint Cybersecurity Advisory, "Hunting Russian Intelligence "Snake" Malware", May 9, to assist network defenders in detecting the malware and any associated activity.

5. **US busts Russian cyber operation in dozens of countries (C4ISRNet, 09 MAY, Eric Tucker)**

   The Justice Department said Tuesday that it had disrupted a long-running Russian cyberespionage campaign that stole sensitive information from computer networks in dozens of countries, including the U.S. and other NATO members.

   Prosecutors linked the spying operation to a unit of Russia's Federal Security Service, or FSB, and accused the hackers of stealing documents from hundreds of computer systems belonging to governments of NATO members, an unidentified journalist for a U.S. news organization who reported on Russia, and other select targets of interest to the Kremlin.

6. **FBI disrupts sophisticated Russian cyberespionage operation (Cyber Scoop, 09 MAY, AJ Vicens)**

A law enforcement effort dubbed "Medusa" targeted malware deployed by Moscow's Federal Security Service, officials said Tuesday.

One of the Russian government's most sophisticated long-running cyberespionage operations was hacked and disrupted by the FBI as part of a sprawling international effort, officials with the U.S. government announced Tuesday.

7. **Updates to Cyber Command's challenge problems (U.S. Cyber Command Public Affairs, 09 MAY)**

U.S. Cyber Command released an unclassified update to the Command's Challenge Problem Set for 2023.

The update to these command challenge problems reflects CYBERCOM's continued commitment to innovation and transparency as the leader in the cyberspace domain.

8. **US disrupts Russian cyber espionage campaign targeting dozens of countries (The Charlotte Observer, 09 MAY, Ines Kagubare)**

The Department of Justice announced on Tuesday that it had disrupted a Russian cyber espionage group that allegedly released a sophisticated malware, known as Snake, on computer networks.

The agency attributed the malware to a unit within Russia's Federal Security Service (FSB) known as Turla. For nearly 20 years, the unit used the malware to steal sensitive information from hundreds of computers in at least 50 countries, including members of NATO.

9. **Top US cyber official warns AI may be the 'most powerful weapon of our time' (Cyberscoop, 05 MAY, Christian Vasquez)**

CISA Director Jen Easterly said the rapid advances in technologies such as ChatGPT could be used by adversaries to carry out cyberattacks.

Director of the Cybersecurity and Infrastructure Security Agency Jen Easterly warned that artificial intelligence may be both the most "powerful capability of our time" and the "most powerful weapon of our time."

"Imagine a world in the not to distant future where how-to guides, AI-generated imagery, auto-generated shopping lists are available for terrorist and for criminals, providing the capability to develop things like cyber weapons, chemical weapons, bio weapons," Easterly said Friday at a security summit at Vanderbilt University in Nashville, Tennessee. "And that's not even the worst case scenario."

10. **Dallas disrupted by hackers - courts closed, police and fire sites offline (Reuters, 04 MAY, Raphael Satter)**

Hacker sabotage has disrupted several public services in Dallas, closing courts and knocking emergency services websites offline, officials said on Thursday.

Courts were closed Wednesday and will remain closed Thursday, the City of Dallas said in a series of statements posted to the web. Although the statements said emergency services to residents were unaffected, the home pages of the police and fire service were unavailable as of Thursday and a police spokesperson said the city's computer-aided dispatch system was hit.

11. **Coming to DEF CON 31: Hacking AI models (Cyberscoop, 04 MAY, Elias Groll)**

A group of prominent AI companies committed to opening their models to attack at this year's DEF CON hacking conference in Las Vegas.

Agroup of leading artificial intelligence companies in the U.S. committed on Thursday to open their models to red-teaming at this year’s DEF CON hacking conference as part of a White House initiative to address the security risks posed by the rapidly advancing technology.

Attendees at the premier hacking conference held annually in Las Vegas in August will be able to attack models from Anthropic, Google, Hugging Face, Microsoft, NVIDIA, OpenAI and Stability AI in an attempt to find vulnerabilities. The event hosted at the AI Village is expected to draw thousands of security researchers.

12. **Hate passwords? You’re in luck - Google is sidelining them (AP News, 03 MAY, David Hamilton)**

Good news for all the password-haters out there: Google has taken a big step toward making them an afterthought by adding “passkeys” as a more straightforward and secure way to log into its services.

13. **Meta says ChatGPT-related malware is on the rise (Reuters, 03 MAY, Katie Paul)**

Facebook owner Meta (META.O) said on Wednesday it had uncovered malware purveyors leveraging public interest in ChatGPT to lure users into downloading malicious apps and browser extensions, likening the phenomenon to cryptocurrency scams.

Since March, the social media giant has found around 10 malware families and more than 1,000 malicious links that were promoted as tools featuring the popular artificial intelligence-powered chatbot, it said in a report.

14. **Generative AI providing fuel for hackers, DISA Director Skinner says (C4ISRNet, 02 MAY, Colin Demarest)**

Generative artificial intelligence, software capable of carrying a convincing, human-like conversation or crafting content like computer code with little prompting, will make hackers more sophisticated, ultimately raising the bar for U.S. safeguards, according to the leader of the Defense Information Systems Agency.

Director Lt. Gen. Robert Skinner said the technology is one of the most disruptive developments he’s seen in a long time, and has serious security implications. A similar warning was issued by the National Security Agency’s cybersecurity boss, Rob Joyce, earlier this year.

15. **Apple, Google partner to combat creepy tracking tactics (AP News, 02 MAY)**

Apple and Google are teaming up to thwart unwanted tracking through Bluetooth devices that were created to help people find lost keys, keep tabs on luggage or to locate other things that have a tendency to be misplaced or lost.

The two companies behind the iPhone and the software that powers Android phones on Tuesday submitted a proposal to set standards for combatting secret surveillance on Apple’s AirTag trackers and similar gadgets. The concept also has the backing of Samsung, which sells the most Android smartphones worldwide, as well as tracking products similar to the AirTag such as Tile, Chipolo, and Pebblebee.

16. **The Next Pandemic Could Be Digital: Open Source Hardware and New Vectors of National Cybersecurity Risk (Special Competitive Studies Project (SCSP), Feb, Rick Switzer)**

This paper was written by SCSP Senior Fellow Rick Switzer who is on a one-year sabbatical from the Department of State. Prior to joining SCSP, Rick was a State Department visiting professor at the National Intelligence University teaching graduate courses on China's economy and innovation system. Rick also served as a member of the Secretary of State's Policy Planning Council. From 2018 to 2019 he was a Senior State Department Advisor to the Department of Defense working with the Air Force and the Army. Preceding that he was the Environment, Science, Technology and Health Minister Counselor at Embassy Beijing, the largest science section in the world. Prior to joining government Rick co-founded a wireless technology start-up and also conducted innovation policy research at the University of California.

The views in this paper are the author's own and based on research he conducted prior to and during his sabbatical with SCSP. These views are not attributable to SCSP, the SCSP Board, or its staff.

Electronic Warfare

1. **China’s ‘Satellite Killer’ Spacecraft Threatens To Puncture US Military In Space By Crippling Its Recon, Navigation & EW Satellites (The EurAsian Times, 13 MAY, EurAsian Times Desk)**

   On May 8, a mysterious reusable Chinese spacecraft returned to Earth after staying in orbit for 276 days. On the face of it, it seems like a mere technological development. But, from a military perspective, it has far-reaching consequences.

   A highly maneuverable spacecraft like this could be used to “surveil, disrupt and outright attack an opponent’s space-based assets” or conversely can “retrieve or otherwise interact with friendly ones.”

   Private space services company LeoLabs revealed on its Twitter handle that the Chinese reusable space vehicle “docked with or captured a separate object on multiple occasions” during the orbit.

   The Chinese state-run China Aerospace Science and Technology Corporation has not provided many details about its time in orbit.

2. **Russia’s ‘On-Point Jamming’ Has Made Life Miserable For HIMARS, EW Attacks Cause It To Miss Its Target – US Report (The EurAsian Times, 06 MAY, Sakshi Tiwari)**

   In preparation for the much-anticipated counteroffensive against the Russian forces, Ukrainian troops have begun ‘shaping’ military operations, a top US military officer told CNN.

   The CNN report clarifies that ‘shaping’ means hitting targets like weapons depots, command & control centers, and artillery systems to prepare the battlefield for advancing Ukrainian soldiers.

   It’s a standard tactic made prior to major combined operations.

3. **Russia ups its drone game with “mosquito fleets” and electronic warfare (Euromaidan Press, 06 MAY)**

   Russians first were losing to Ukraine’s drone volunteers, but have now taken UAVs seriously

   Russians have become more serious about using drones and developing countermeasures against Ukrainian UAVs, including new weapons such as electromagnetic weapons. This information was shared by Viktor Taran, the head of the Center for Training UAV Operators “Kruk,” in an interview with Defense Express.

   According to Taran, Ukraine has made significant efforts to give its soldiers an advantage in drone technology. Simple civilian quadcopters have been actively supplied to the Ukrainian army since Russia’s first invasion in 2014, and these efforts have increased significantly since 24 February. Each drone in the hands of Ukrainian soldiers serves as an intelligence tool, a means of adjusting fire and unit actions, and a weapon.

4. **Protection Against Enemy Combat Drones Exists in Russia, and It Is Effective – 04 MAY**

   The news was posted online on 04 May 2023 at 15.02. The article discusses the latest Russian air defense systems “Repellant Patrol” and “Matrix” able to detect and counter enemy's unmanned aerial vehicles, and their utilization in Ukraine, and for protection of all large oil depots and other strategic facilities that are within reach of enemy drones. The article states that is quite possible that it was the "Matrix" system that protected the Kremlin from the drones that attacked it a day ago.

5. Is China's Korla laser ASAT site hacking Western satellites? (Airforce-Technology, 01 MAY, Andrew Salerno-Garthwaite)

Korla East Test Site in China shows a pattern of engaging foreign satellites with directed energy weapons in BlackSky's intra-day images.

New intra-day satellite imagery of the Korla East Test Site in Xinjiang, China, shows the operation of laser anti-satellite weapons (ASAT) to engage with Western satellites.

The satellite imagery from geospatial intelligence company BlackSky has uncovered a pattern of behaviour at the Korla East Test Site that is consistent with China's development of technology to disrupt, destroy or hijack foreign satellites, as mentioned in the recent US intelligence breach.

Army Technology has reviewed satellites images of Korla East Test Site featuring two laser gimbals with supporting infrastructure, housed within separate hangars with retractable roofs, to the north and south of the compound, confirming the view that this site holds ASAT weapons. The evidence suggests a pattern of opening the hangars to operate the ASAT lasers around solar noon, the time when foreign imaging satellites are most active.

Information Advantage

1. **Washington is determined to govern AI, but how? (Reuters, 15 MAY, Diane Bartz & Jeffrey Dastin)**

   U.S. lawmakers are grappling with what guardrails to put around burgeoning artificial intelligence, but months after ChatGPT got Washington's attention, consensus is far from certain.

   Interviews with a U.S. senator, congressional staffers, AI companies and interest groups show there are a number of options under discussion.

   Some proposals focus on AI that may put people's lives or livelihoods at risk, like in medicine and finance. Other possibilities include rules to ensure AI isn't used to discriminate or violate someone's civil rights.

2. **Central and Eastern Europe Are Playing Catchup on Russian Disinformation (World Politics Review, 10 MAY, Dominika Jajdu)**

   Russia's military invasion of Ukraine has become a geopolitical contest between Moscow and the West, with implications for the global economy, energy security and information technology. While tensions with Russia were not new, for many democracies on both sides of the Atlantic, Moscow's war in Ukraine dramatically changed their perception not just of Russian aggression, but also of their ability to respond to it.

   In areas of economics and energy, the policy solutions to disruptions caused by the war appeared to be relatively straightforward. They include measures like diversification of energy supply sources and government subsidies. But the realm of information security does not lend itself to similar quick fixes or short-term policy interventions.

   Central and Eastern Europe, or CEE, which comprises more than 10 countries at varying levels of resilience to Russian disinformation, provides several hard-learned lessons in how Russian disinformation is used and how it might be countered.

3. **AI may make scams and misinformation harder to spot, warns Apple co-founder (Metro, 09 MAY, Katherine Fidler)**

   Steve Wozniak, co-founder of Apple, has called for content generated by artificial intelligence to be clearly labelled, warning that AI could make scams and misinformation harder for everyday users to spot.

   Speaking to the BBC, the Silicon Valley pioneer said: 'AI is so intelligent it's open to the bad players, the ones that want to trick you about who they are.'

4. **UK reviews AI models as rapid growth fuels safety concerns (Reuters, 09 MAY, Paul Sandle)**

   Britain's competition regulator said on Thursday it would start examining the impact of artificial intelligence on consumers, businesses and the economy and whether new controls were needed on technologies such as OpenAI's ChatGPT.

   While research on AI has been going on for years, the sudden popularity of generative AI applications such as ChatGPT and Midjourney has highlighted a technology that could upend the way businesses and society operate.

5. **Timeline: China's steps to control its data and information (Reuters, 09 MAY, Josh Ye)**

A Chinese investigation of consulting firm Capvision Partners over national security concerns is the latest step in a years-long campaign by Beijing to tighten control of data generated within its borders.

State media accused overseas institutions of using domestic consulting firms to steal state secrets and intelligence in key areas key, state broadcaster CCTV said in a programme on the Capvision investigation.

6. **AI pioneer says its threat to world may be 'more urgent' than climate change (Reuters, 09 MAY, Martin Coulter)**

Artificial intelligence could pose a "more urgent" threat to humanity than climate change, AI pioneer Geoffrey Hinton told Reuters in an interview on Friday.

Geoffrey Hinton, widely known as one of the "godfathers of AI", recently announced he had quit Alphabet (GOOGL.O) after a decade at the firm, saying he wanted to speak out on the risks of the technology without it affecting his former employer.

7. **Russia’s ‘Art Of War’ Includes ‘Act Of Deception’; Ukraine Fears A Trap In Wagner’s Withdrawal From Bakhmut (The EurAsian Times, 06 MAY, Parth Satam)**

Russia’s Private Military Company (PMC) Wagner will give up its positions in Bakhmut (Artemovsk) on May 10 and has asked to be replaced by regular units of the Russian army, its chief Yevgeny Prigozhin has announced.

In an open letter to President Vladimir Putin, Prigozhin has reiterated his complaint about not being given ammunition and artillery shells and, in preceding videos, openly abused Defense Minister Sergei Shoigu and Chief of General Staff Valery Gerasimov, in a shocking expletive-ridden outburst.

Prigozhin, whose fighters made tremendous advances in Soledar and Bakhmut — the latter where only a 2.5-kilometer stretch remains out of 45 kilometers, according to his letter – has long been at odds with the Russian Ministry of Defense (MoD).

Interestingly Ukrainian military officials are taking Prigozhin’s claim with a pinch of salt and are far from buying into it. They believe President Vladimir Putin will eventually have a say on Wagner’s withdrawal and that the group’s losses were owing to the successful actions of the Ukrainian army and not the lack of ammunition.

8. **China-based networks sowing disinformation in West: Meta (The Hindu, 05 MAY)**

Meta said it had removed more than 100 Facebook pages, profiles and Instagram accounts linked to the network.

A China-based online network tried to recruit protesters in Europe and set up a media firm in Britain as part of a disinformation campaign, Facebook owner Meta said.

The network's social media accounts — which ranged from Facebook to YouTube, Telegram and Twitter — pushed content focusing on incendiary political issues in Europe and the United States, according to Meta.

9. **Russian Military Debates AI Development and Use (CNAS, 04 MAY, Samuel Bendett)**

Over the past decade, artificial intelligence (AI) moved front and center in the Russian military's thinking about new concepts and technologies for current and future wars. Following the Ukraine invasion, and the imposition of IT and high-tech sanctions on the Russian Federation, the Russian government and the Russian Ministry of Defense (MOD) are seeking ways to adapt to the resulting environment. The MOD considers AI as a decision-making tool and a key element in managing uncrewed technologies with a human-in-the-loop as a guiding approach to research and development.

10. China's AI industry barely slowed by US chip export rules (Reuters, 03 MAY, Stephen Nellis, Josh Ye & Jane Lee)

U.S. microchip export controls imposed last year to freeze China's development of supercomputers used to develop nuclear weapons and artificial-intelligence systems like ChatGPT are having only minimal effects on China's tech sector.

The rules restricted shipments of Nvidia Corp (NVDA.O) and Advanced Micro Devices Inc (AMD.O) chips that have become the global technology industry's standard for developing chatbots and other AI systems.

11. Cross-pollination on AI may be a way forward for US, China (C4ISRNet, 02 MAY, MAJ, Nicholas Dockery)

Conflict is not war, but it has become more challenging to separate the ideas when it comes to the Chinese Communist Party and the U.S.

Under the Biden administration, the U.S. has taken a stricter stance on the CCP's economic and political activities. From executive orders limiting trade on semiconductors to sanctions on foreign companies with military ties to the CCP's Military-Civil Fusion initiatives to strengthening regional alliances within the Association of Southeast Asian Nations.

12. Military cyber directors: Help us better leverage AI to gain the 'high ground' (Breaking Defense, 02 MAY, Jaspreet Gill)

In a sign of how ubiquitous AI has become recently, DISA Director Lt. Gen. Robert Skinner began his keynote not speaking himself, but with a generative AI that cloned his voice and delivered the start of his remarks.

The military services need to figure out how to better integrate and leverage disruptive technologies like artificial intelligence into data-driven decision making, and senior cyber officials said today they need industry's help to do it.

Using current technology right now, Lt. Gen. Maria Barrett, commanding general of US Army Cyber Command, said that work is "tremendously complex."

"Anything we can do to buy down that complexity by leveraging AI and [machine learning] would be absolutely fantastic and essential for, I think, the challenges that we face in the future," she told the audience at the AFCEA's TechNet Cyber conference in Baltimore. "I think we have the underpinnings of starting to be able to take advantage of it from an Army cyber mission standpoint."

13. Rinse and repeat: Iran accelerates its cyber influence operations world wide (Microsoft, 02 MAY, Clint Watts)

Iran continues to be a significant threat actor, and it is now supplementing its traditional cyberattacks with a new playbook, leveraging cyber-enabled influence operations (IO) to achieve its geopolitical aims.

Microsoft has detected these efforts rapidly accelerating since June 2022. We attributed 24 unique cyber-enabled influence operations to the Iranian government last year – including 17 from June to December – compared to just seven in 2021. We assess that most of Iran's cyber-enabled influence operations are being run by Emennet Pasargad – which we track as Cotton Sandstorm (formerly NEPTUNIUM) – an Iranian state actor sanctioned by the US Treasury Department for their attempts to undermine the integrity of the 2020 US Presidential Elections.

14. How the US government can combat Russian disinformation on Ukraine (C4ISRNet, 02 MAY, Noam Schwartz)

Last week, the US Department of Justice unsealed a significant criminal complaint. Police officers from China's Ministry of Public Security (MPS) were charged with creating 'thousands of fake online personas on social media sites, including Twitter, to target Chinese dissidents through online harassment and threats' and for spreading 'propaganda whose sole purpose is to sow divisions within the United States'.

This announcement marked the first definitive public attribution to a specific Chinese government agency of covert malign activities on social media. However, the MPS is one of many party-controlled organisations that analysts have long suspected of conducting covert and coercive operations to influence users on social media.

Signal

1. **Pentagon CIO taking over 5G activities with eye on expanded testing (C4ISRNet, 12 MAY, Colin Demarest)**

   The U.S. Department of Defense's chief information officer will take direct oversight of the department's 5G endeavors, as officials seek to box out Chinese influence in the communications market.

   The fifth generation of wireless technology is seen as critical to connectivity at home and abroad, with millions of dollars of government money already invested. U.S. military adoption has been slow, and global competition is fierce, with suspect players such as Huawei and ZTE jostling for space.

2. **EU weighs more stringent rules for cloud data storage (Verdict, 12 MAY)**

   The new cybersecurity rules aim to restrict foreign governments' access to EU data.

   Authorities in the European Union (EU) are considering a proposal that would require cloud service providers to store all their data within the block, reported Bloomberg.

   The European Union Agency for Cybersecurity (ENISA) is drafting a new, more stringent measure to prevent foreign governments from meddling with EU data, the publication said, citing a draft proposal.

   The new cybersecurity rules could require US cloud providers such as Amazon, Microsoft, and Alphabet to prevent the US government from accessing European cloud data.

3. **Japanese Media Report on Vulnerable Undersea Cables Near Okinawa (U.S. Army Asian Studies Detachment, 09 MAY)**

   According to a Japanese magazine, if the submarine cables around Okinawa were cut, the U.S. forces in Japan would be severely compromised. A Japan Maritime Self-Defense Force official said that in recent years, China may be using ships to determine the location of submarine cables. China has been developing undersea drones to destroy submarine cables since 2017 and has already manufactured 100 of them. China recently cut submarine cables connecting Taiwan's Matsu Islands on 2 and 8 February 2023.

4. **Pentagon's AI office rebooting global experiments for JADC2 (C4ISRNet, 08 MAY, Colin Demarest)**

   The Pentagon's artificial intelligence office is reviving a series of worldwide trials meant to advance its vision of seamless connectivity and coordination, known as Joint All-Domain Command and Control.

   The return of the Global Information Dominance Experiments, or GIDE, under the direction of the Chief Digital and Artificial Intelligence Office, or CDAO, comes after a months-long hiatus and amid an explosion of public interest in AI and its potential to augment humans, military or otherwise.

5. **Zero Trust vs. Zero-Knowledge: What's the Difference? (Make Use Of, 06 MAY, Sead Fadilpašić)**

   These two security concepts may sound similar but they're completely different.

While both zero trust and zero-knowledge concepts are critical components of today's cybersecurity trends, they aren't the same.

They sound somewhat similar and share a purpose, but zero knowledge goes one step further than zero trust in creating a security system that can counter ever-evolving cyber threats.

In fact, zero-knowledge proof can be used to turn the ideas of the zero-trust security model into reality. However, before we continue, let's clear up what these two concepts are.

6. **US Army revising how it develops, deploys advanced networking gear (C4ISRNet, 05 MAY, Colin Demarest)**

The U.S. Army is leaving behind what it formally recognizes as "capability sets" for an approach to upgrading networking gear multiple generals said is more fluid and applicable to the service's 2030 and 2040 goals.

As the Army prepares for potential widespread conflict in the Indo-Pacific, against China, or in Europe, against Russia, it is placing increasing emphasis on the division, a formation of some 15,000 soldiers and firepower capable of sustained fighting and maintenance.

7. **Air Force reaches out to industry to apply quantum computing and communications to C4ISR applications (Military & Aerospace Electronics, 04 MAY, John Keller)**

Project seeks to develop quantum computing algorithms and investigate entanglement distribution across a heterogeneous quantum network for C4ISR.

U.S. Air Force researchers are asking industry to develop quantum computing technology for next-generation command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications.

Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., issued a broad agency announcement (FA8750-23-S-7001) last week for the Quantum Information Sciences project to apply quantum information and communications technologies to C4ISR systems.

8. **Zero trust would have helped prevent Pentagon leak, CIO Sherman says (C4ISRNet, 03 MAY, Colin Demarest)**

The recent leak of national security documents would have been easier to discover and prevent had the U.S. Department of Defense already instituted the latest cybersecurity practices known as zero trust, according to Pentagon Chief Information Officer John Sherman.

The disclosure of the classified reports, allegedly spearheaded by a 21-year-old member of the Massachusetts Air National Guard, has prompted a hard look at the department's information-security practices. The breach included insights about the ongoing Russia-Ukraine war.

9. **US cyber leaders look to AI to augment network activities (C4ISRNet, 03 MAY, Colin Demarest)**

The increasing intricacy of military networks and the digital savvy of other world powers is making artificial intelligence and related programs more desirable for U.S. cyber leaders.

With an explosion of high-tech devices and vehicles and the vast amount of data they pass back and forth come additional security and responsiveness demands. And “anything we can do to buy down that complexity,” by employing AI and machine learning, “would be absolutely fantastic,” according to Lt. Gen. Maria Barrett, the leader of Army Cyber Command.

10. Connectivity will ‘make or break’ US military use of AI, official says (C4ISRNet, 28 APR, Colin Demarest)

Leaps in military artificial intelligence and other advanced computing capabilities will be for naught if troops and battlefield systems can’t ultimately connect to one another, and do so securely, an official with U.S. Central Command said.

While the Department of Defense hails AI as a game-changer and the defense industry likewise invests and advertises its wares, it is network infrastructure, basic connectivity, that is “at the core of anything related to” the technology’s real-world adoption, according to Schuyler Moore, CENTCOM’s chief technology officer.

Items of Interest

1. Russia-Ukraine Situation Report, (U.S. Army Asian Studies Detachment)

These reports are a compilation of articles from Russia, Ukraine, and other nations regarding the current tensions between Russia and Ukraine. Topics covered in this report include the following:

- Foreign Observations and Reactions
- Social Media Highlights
- Russian Eastern Military District Movements
- Other Topics

Russia-Ukraine Situation Report, 15 May 2023
Russia-Ukraine Situation Report, 12 May 2023
Russia-Ukraine Situation Report, 11 May 2023
Russia-Ukraine Situation Report, 10 May 2023
Russia-Ukraine Situation Report, 09 May 2023
Russia-Ukraine Situation Report, 08 May 2023
Russia-Ukraine Situation Report, 05 May 2023
Russia-Ukraine Situation Report, 04 May 2023
Russia-Ukraine Situation Report, 03 May 2023
Russia-Ukraine Situation Report, 02 May 2023
Russia-Ukraine Situation Report, 01 May 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Ukraine Situation Report: M1 Abrams Training Tanks Arrive In Germany – 15 MAY

Ukraine Situation Report: Kyiv Retakes Ground On Bakhmut's Flanks – 13 MAY

Ukraine Situation Report: Kinzhal Missile Targeted Patriot Battery, Report Claims – 12 MAY

Ukraine Situation Report: Kyiv Claims Russian Brigade "Seriously Damaged" In Bakhmut – 10 MAY

Ukraine Situation Report: RQ-4 Global Hawk Flies Off Sochi – 09 MAY

Ukraine Situation Report: 35 Shahed-136s Attacked Kyiv Overnight – 08 MAY

Ukraine Situation Report: Kyiv Claims Patriot Intercepted Kinzhal Air-Launched Ballistic Missile – 06 MAY

Ukraine Situation Report: HIMARS Shown Being Stashed In 'Soviet Bunker' – 03 MAY

Ukraine Situation Report: Russian Guided Bombs A Growing Threat, Kyiv Claims – 02 MAY

Ukraine Situation Report: 100k Russian Casualties Since December, White House Says (Updated) – 01 MAY

3. Chinese general calls for military to prepare for 'hybrid' modern warfare (SCAMP, 15 MAY, Amber Wang)

Writing in official newspaper, General Wang Haijiang gives glimpse of how PLA's top brass sees the war in Ukraine

He says China faces suppression and containment from Western countries that may 'escalate at any time'

4. **Impoverished Communist Nation 50 Years Ago, China Now Challenges The Might Of US & Japan (The EurAsian Times, 15 MAY, GP CPT TP Srivastava)**

   With China set to match/overtake the US economy by 2035, the geo-strategic scenario, specifically the 'world power center,' will likely change. Most ardent supporters of Karl Marx's propagated communism never dared to predict that to happen by the middle of the 21st century.
   The capitalist domination of world affairs would have to face a serious challenge, and that too from China which was an impoverished communist country barely 50 years ago.

5. **Russia Attacked Patriot System In Ukraine With Hypersonic Missiles But Were Instead Shot Down By The Same Patriot – CNN (The EurAsian Times, 13 MAY, Ashish Dangwal)**

   Russian military tried to strike the Patriot system in Ukraine last week with a Kinzhhal hypersonic missile, CNN reported citing officials.

   As per the reports, the attack failed, and the Ukrainian military instead intercepted the hypersonic missile using the 'under attack' Patriot system.

   The Ukrainian air defenders fired multiple missiles from the Patriot at different angles to intercept the Russian missile, demonstrating how quickly they have become adept at using the powerful system, one official said.

   US officials believe the Russians picked up on signals emitted from the Patriot, allowing them to detect, identify and target the US-origin system.

   Ukraine's MoD had confirmed the downing of the Kinzhal missile and tweeted: @KpsZSU (Ukraine Air Force) confirms that Ukraine's air defenders shot down Kinzhal, a hypersonic aeroballistic Russian missile, for the first time since the attacks began. This was done by operators of the Patriot air defense system.

6. **Foreign Reflections on U.S. Exercises and Operations, 12 May 2023 (U.S. Army Asian Studies Detachment, 12 MAY)**

   This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 4 to 11 May 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, Philippines, South Korea, and Taiwan.

7. **Ukraine Begins Phase-1 Of Counter-Offensive Ops Against Russia; Begins Hitting Command Centre, Weapons Depot – CNN (EurAsian Times Desk, 12 May)**

   In preparation for the much-anticipated counteroffensive against the Russian forces, Ukrainian troops have begun 'shaping' military operations, a top US military officer told CNN.

   The CNN report clarifies that 'shaping' means hitting targets like weapons depots, command & control centers, and artillery systems to prepare the battlefield for advancing Ukrainian soldiers.

   It's a standard tactic made prior to major combined operations.

8. **Putin tells WWII event West is waging a 'real war' on Russia (AP**

NEWS, 09 MAY)

President Vladimir Putin declared Tuesday that the West has unleashed “a real war” against Russia, reprising a familiar refrain at scaled-down Victory Day celebrations that may reflect the toll the Ukraine conflict is taking on his forces.

Putin’s remarks came just hours after Moscow fired its latest barrage of cruise missiles at targets in Ukraine, which Russia invaded more than 14 months ago. Ukrainian authorities said air defenses destroyed 23 of 25 missiles launched.

9. **Ukraine Isn’t Buying Wagner Boss’s Tirade About Pulling Out Of Bakhmut (The Drive, 05 MAY, Howard Altman)**

Wagner boss Vevgeny Prigozhin said his troops will leave Bakhmut on May 10 over a lack of ammo, but Ukraine isn’t buying that threat.

Ukraine’s Armed Forces are not buying into the head of the Wagner mercenary group’s emotional screed threatening to pull out of Bakhmut next week due to a lack of ammunition. In an impassioned address apparently delivered near the battlefield, Yevgeny Prigozhin said his troops were thrown into the "Bakhmut Meat Grinder" and then abandoned by "near-military bureaucrats" who cut off the ammunition flow and "sit and shake their fat bellies and think that they will go down in history as winners.”

10. **Foreign Reflections on U.S. Exercises and Operations, 4 May 2023 (U.S. Army Asian Studies Detachment, 04 MAY)**

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 27 April to 3 May 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, the Philippines, South Korea, and Taiwan.

11. **RGF to Receive New Wearable Drone Detector Systems (Army Europe Open Source Intelligence Center, 04 MAY)**

On 29 April 2023, multiple RUS outlets claimed RUS RGF will receive new wearable drone detector dystems dubbed "Sinitsa." It can detect UAVs at a distance of up to 2000 m in a sector of 120 degrees. When placed at a temporary deployment point, it is possible to combine several tactical complexes into a single network, according to a RUS source in the defense industry.The device runs on a single battery for at least 120 minutes and can be powered from a fixed network. At the same time, the device allows to install two additional types of UAV suppression modules operating in the frequency bands 433 - 1,600 MHz and 2,400 - 5,800 MHz and blocking the control and navigation channels of drones.

12. **Drone Attack On The Kremlin In Moscow (Updated) (The Drive, 03 MAY, Howard Altman & Joseph Trevithick)**

An attack on arguably the most symbolic target in Russia would be a victory for Ukraine, but it could be used by Putin to rally support too.

Video has emerged showing what appears to be a drone striking at the dome of the Senatsky Dvorets in the Kremlin in Moscow. Russian officials claim that the building came under attack by Ukraine and have vowed to retaliate, while Ukraine's president denied Kyiv's involvement in the incident.

The video shows what appears to be a drone approaching the dome and then exploding in a ball of fire that lit up the sky. It seems that this drone did not impact the dome itself, but detonated very close to it, sending flaming debris falling. Two drones are suspected to have attacked the dome in succession.

13. **Airship Spotted Outside Giant Secretive Hangar In China (The**

Drive, 01 May, Joseph Trevithick)

China’s extensive airship and balloon programs have seen new scrutiny after multiple shoot-downs over U.S. and Canadian airspace this year.

Private satellite imagery and geospatial intelligence firm BlackSky has released a photo showing what appears to be a teardrop-shaped airship or aerostat in front of a huge hangar in northwestern China. In 2021, The War Zone published an in-depth feature regarding this facility and ties to Chinese work on high-altitude airships able to act as intelligence-gathering platforms, early warning systems for missile defense, and more.