Cyber Center of Excellence

Unclassified Threat Read Book

01 - 15 Jun 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

1. North Korean hackers create fake web portal, South's spy agency says - 15 JUN
2. Hackers create fake GitHub profiles to deliver malware through repositories - 14 JUN
3. Ongoing Russian cyberattacks targeting Ukraine - 14 JUN
4. CISA: LockBit behind 1 in 6 ransomware attacks on US gov't in 2022 - 14 JUN
5. Microsoft identifies new hacking unit within Russian military intelligence - 14 JUN
6. Chinese Cyberspies Caught Exploiting VMware ESXi Zero-Day - 13 JUN
7. Americans 'Need to Be Prepared' for Chinese Cyberattacks - 12 JUN
8. US cyber experts sent to Latin America on ‘hunt-forward’ mission - 09 JUN
9. Detecting and mitigating a multi-stage AiTM phishing and BEC campaign - 08 JUN
10. Chinese ‘Volt Typhoon’ hack underlines shift in Beijing’s targets, skills - 07 JUN

Electronic Warfare

1. Dumb and cheap: When facing electronic warfare in Ukraine, small drones’ quantity is quality - 13 JUN
2. Ukrainian forces destroy RP-377LA Lorandit crucial player in Russian Army's electronic warfare - 12 JUN
3. First Time! China’s ‘Cutting Edge’ Y-9DZ Electronic Warfare Aircraft Spotted, Intercepted By Japanese Fighters - 10 JUN
4. Russian EW ‘Ambushes’ Mohajer-6 Drone Over Crimea; Officials Celebrate, Mourn The Downing Of Iranian UAV - 09 JUN
5. IDF’s electronic warfare role jumps forward in current major IDF drill - 06 JUN
6. Army ‘on the cusp of greatness’ with its critical EW programs - 05 JUN

Information Advantage

1. Google, one of AI’s biggest backers, warns own staff about chatbots - 15 JUN
2. France accuses Russia of faking websites to sow confusion and disinformation about Ukraine war - 13 JUN
3. US decides to rejoin UNESCO and pay back dues, to counter Chinese influence - 12 JUN
4. The viral AI-generated image showing an explosion near the Pentagon is 'truly the tip of the iceberg of what's to come,' tech CEO says - 09 JUN
5. Unlock new insights with Azure OpenAI Service for government - 07 JUN
6. Senators plan briefings on AI to learn more about risks - 07 JUN
7. Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data - 07 JUN
8. US Wages ‘Undeclared War’ Against Russia; Ukraine Tries Psychological Warfare Against Russian Military - 07 JUN
9. Japan, Australia, US to fund undersea cable connection in Micronesia to counter China’s influence - 07 JUN
10. From Provocations And Deterrence To Preparing For Unification: Why An Information Campaign Is Vital To Political Warfare In Korea - 05 JUN
11. Russia says Ukraine is launching major attacks; Kyiv accuses Moscow of misinformation - 05 JUN
12. ‘Testing Ground’ For Artificial Intelligence, Ex-US Navy Admiral Says Ukraine War Hotbed For Cutting-Edge Technology - 4 JUN
13. BRI - Belt and Road Initiative - Highlights, 31 May 2023, - 01 JUN
14. Air Force Colonel Now Says Drone That Turned On Its Operator Was A “Thought Experiment” - 01 JUN

Signal

1. How a Shady Chinese Firm's Encryption Chips Got Inside the US Navy, NATO, and NASA - 15 JUN
2. Device level quantum-computing-hardened encryption keys - 14 JUN
3. China's quantum leap — Made in Germany - 13 JUN
4. DoD finding it 'hard to orchestrate' services on zero trust, holding monthly discussions: Resnick - 08 JUN
5. DoD official envisions faster 'secure pipeline' to help small business tech contractors protect information - 07 JUN
6. Expand National Quantum Initiative to keep up with China, say officials, experts, - 07 JUN
7. Army Assesses Cyber Posture of Its Weapons, Control Systems Ahead of Zero Trust - 05 JUN
8. GDIT drastically upping investments in DoD emerging tech areas like AI, zero trust - 02 JUN

Items of Interest

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. Deutsche Welle (DW) Ukraine updates
4. Russian Capture Of Ukrainian Leopard Tank, Bradleys Seen In Video - 13 JUN
5. Ukraine Accuses Russia Of Blowing Up Another Dam - 12 JUN
6. Russia's improved weaponry and tactics pose challenges to Ukraine's counteroffensive - 12 JUN
7. AP Exclusive: Drone footage of collapsed dam shows devastation, no evidence to back Russian claims - 08 JUN
8. Chinese 'Tiger' Roars In Ukraine War; Pro-Russia Troops Flaunt Chinese Military Vehicles For SMO - 08 JUN
9. Ukraine's Big Offensive Kicks Off To Tough Resistance - 08 JUN
10. Xi Jinping Calls for "Speeding up the Modernization of National Security" - 06 JUN
11. Who are the Freedom of Russia Legion and Russian Volunteer Corps? - 05 JUN
12. Crippled Russia Is 'Re-Importing' Military Hardware From India Amid Shortage Of Components – Reports - 05 JUN
13. Foreign Reflections on U.S. Exercises and Operations, 5 June 2023 - 05 JUN
14. The Taliban Is Using U.S. And Russian Weapons To Fight Iran - 04 JUN
15. Attacks in Russia 'destroy myth of Putin's invincible army' - 02 JUN
16. Russia Claims It Foiled Tank-Backed Incursion Across Its Border - 01 JUN

Cyber

1. **North Korean hackers create fake web portal, South's spy agency says (Reuters, 15 JUN, Hyunsu Yim)**

   North Korean hackers have set up a fake website that looks almost identical to the popular South Korean web portal Naver, marking a more sophisticated attempt to target users in the South, Seoul's spy agency said.

   The National Intelligence Service (NIS) issued a warning this week, urging people to refrain from accessing the website called "Naver Portal" and said it was working with overseas organisations to track down the activity of the group it believed was behind the fake portal.

2. **Hackers create fake GitHub profiles to deliver malware through repositories (The Record, 14 JUN, Daryna Antoniuk)**

   Hackers launched an elaborate but likely unsuccessful campaign to deceive cybersecurity professionals on the code-hosting platform GitHub and trick them into downloading malware, according to research published on Wednesday.

   The group created fake profiles of real security researchers to promote code repositories that appear to house exploits for popular products like Chrome, Exchange, and Discord.

3. **Ongoing Russian cyberattacks targeting Ukraine (Microsoft, 14 JUN, Tom Burt)**

   Microsoft threat intelligence teams have been tracking a wave of cyberattacks from an actor we call Cadet Blizzard that is associated with the Russian GRU. These attacks, which began in February 2023, targeted government agencies and IT service providers in Ukraine. We can also now attribute to Cadet Blizzard the destructive WhisperGate wiper attacks against Ukraine detected by Microsoft in January 2022 prior to Russia's invasion.

4. **CISA: LockBit behind 1 in 6 ransomware attacks on US gov't in 2022 (The Record, 14 JUN, Jonathan Greig)**

   About one in every six ransomware attacks targeting U.S. government offices in 2022 can be traced back to a single group: LockBit.

   Cybersecurity agencies around the world said Wednesday that the LockBit gang, which has links to Russia, is one of the biggest cybersecurity threats that governments and other organizations face.

   The U.S. Cybersecurity and Infrastructure Security Agency (CISA), FBI and Multi-State Information Sharing and Analysis Center (MS-ISAC) joined the cybersecurity authorities of Australia, Canada, United Kingdom, Germany, France, and New Zealand in publishing a lengthy examination of the group behind the "most deployed ransomware variant across the world" in 2022.

5. **Microsoft identifies new hacking unit within Russian military intelligence (Cyberscoop, 14 JUN, Aj Vicens)**

   Dubbed "Cadet Blizzard," the hacking group carried out operations targeting Ukrainian infrastructure in the run-up to the Russian invasion.

   On Jan. 13, 2022, about five weeks before Russia's full-scale invasion of Ukraine, Russian hackers carried out one of the first cyberattacks in the run-up to the conflict.

Posing as ransomware, the malware worked in two stages: First, it would overwrite the master boot record with a ransom note, pointing victims to a bitcoin wallet and demanding a relatively paltry $10,000 to recover corrupted files. Then it would download and deploy file corrupter malware, targeting files in particular directories to be overwritten. But the operation was a ruse: There was no way to recover the files.

6. Chinese Cyberspies Caught Exploiting VMware ESXi Zero-Day (Security Week, 13 JUN, Ionut Arghire)

Mandiant has observed a Chinese cyberespionage group exploiting a VMware ESXi zero-day vulnerability for privilege escalation.

A Chinese cyberespionage group tracked as UNC3886 has been observed exploiting a VMware ESXi zero-day vulnerability to escalate privileges on guest virtual machines, Mandiant warns.

Initially detailed in September 2022, UNC3886 has been using malicious vSphere Installation Bundles (VIBs) – packages that are typically used to maintain systems and deploy updates – to install backdoors on ESXi hypervisors and gain command execution, file manipulation, and reverse shell capabilities.

7. Americans 'Need to Be Prepared' for Chinese Cyberattacks (VOA News, 12 JUN, Jeff Seldin)

The United States may not be resilient enough to fend off and survive Chinese attacks on its critical infrastructure should the present great power competition between Washington and Beijing evolve into an actual conflict, according to a top U.S. cyber official.

U.S. officials have ramped up efforts to bolster cybersecurity for the country's electric grid and water systems — much of them run by private companies — since Russia's invasion of Ukraine last year, but the head of the Cybersecurity and Infrastructure Security Agency (CISA) warned Monday that more precautions need to be taken in case China decides to strike.

8. US cyber experts sent to Latin America on 'hunt-forward' mission (C4ISR Net, 09 JUN, Colin Demarest)

U.S. cyber specialists were sent south to identify digital weaknesses on foreign networks and expose tools hackers employ, according to an official with Cyber Command.

The so-called hunt-forward mission, handled by experts on the Cyber National Mission Force, was conducted inside Southern Command's area of responsibility, which comprises more than two-dozen countries such as Argentina, Brazil, Jamaica and Nicaragua.

9. Detecting and mitigating a multi-stage AiTM phishing and BEC campaign (Microsoft, 08 JUN)

Microsoft Defender Experts uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations. This attack shows the complexity of AiTM and BEC threats, which abuse trusted relationships between vendors, suppliers, and other partner organizations with the intent of financial fraud.

10. Chinese 'Volt Typhoon' hack underlines shift in Beijing's targets, skills (Breaking Defense, 07 JUN, Sydney J. Freedberg Jr.)

"The PRC's goal is developing capabilities to disrupt critical infrastructure in the event of a future conflict," NSA Cybersecurity Director Rob Joyce told Breaking Defense in a statement.

For decades, Chinese hackers focused on wholesale and often ham-handed theft of Western trade secrets, what then-NSA director Gen. Keith Alexander called in 2012 "the greatest transfer of wealth in history." But in recent years, the NSA and independent experts agree, the Chinese have gotten a lot subtler — and some of their best hackers have changed tactics, moving from using cyberspace for theft to using it to prepare the battlefield of a future conflict.

This shift, years in the making, became unmistakable last month, when news broke of a widespread security breach of US critical infrastructure, particularly around the strategically crucial island of Guam. While it's not not a harbinger of impending apocalypse or a major breakdown in an increasingly fraught relationship, experts told Breaking Defense that the activity serves as a scary sign of a kind of new normal, where both superpowers are using cyber capabilities to prepare for a potential open war.

Electronic Warfare

1. **Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality (Breaking Defense, 13 JUN, Sydney J. Freedberg)**

   With Ukraine losing up to 10,000 drones a month, mostly to Russian electronic warfare, it's tempting to invest in anti-EW protection – but, experts agreed, it's probably more cost-effective to accept high losses and just buy more bare-bones drones.

   Ukraine is on the march with a motley mix of weapons, from 70-ton Leopard II tanks to two-pound mini-drones. And while the war has been a brutal proving ground for a wide range of technology and tactics, arguably nothing has defined the Ukrainian conflict more than the ubiquity of drones.

2. **Ukrainian forces destroy RP-377LA Lorandit crucial player in Russian Army's electronic warfare (Army Recognition, 12 JUN)**

   According to a video published on the "Ukraine Defence" Facebook account on June 11, 2023, during a joint mission conducted by the 31st separate reconnaissance battalion, 73rd Maritime Operations Center of the SSO of Ukraine, 406th Artillery Brigade, an RP-377LA «Lorandit» electronic warfare vehicle deployed in the occupied Oleshki, Kherson region was destroyed by artillery fire. The RP-377LA is a very sophisticated VHF radio jammer, spectrum analyzer, monitor, and direction finder mounted on Buhanka UAZ-452 4x4 tactical vehicle.

3. **First Time! China's 'Cutting Edge' Y-9DZ Electronic Warfare Aircraft Spotted, Intercepted By Japanese Fighters (The EurAsian Times, 10 JUN, Ashish Dangwal)**

   On June 8, Japan's Air Self-Defense Force (JASDF) intercepted PLA's Y-9DZ electronic-warfare aircraft over the Pacific Ocean, marking this aircraft type's first-ever sighting and photographic documentation.

   The map provided by Japan's Ministry of Defense indicated that the surveillance aircraft was detected approximately 225 kilometers (140 miles) south of the Yaeyama Islands, an archipelago in the southwest of Okinawa Prefecture, Japan.

   In a media release on June 8, it was reported that upon detecting the aircraft, the JASDF promptly deployed fighter jets to visually identify and escort the Chinese military aircraft into international airspace.

4. **Russian EW 'Ambushes' Mohajer-6 Drone Over Crimea; Officials Celebrate, Mourn The Downing Of Iranian UAV (The EurAsian Times, 09 JUN, Sakshi Tiwari)**

   In an unexpected turn of events, Russian troops reportedly shot down an Iranian Mohajer-6 drone deployed over Crimea after mistaking it for one of the many Ukrainian combat drones that make frequent trips to the Crimean peninsula.

   The Russian state media reported on June 6 that the drone intercepted over Crimea was a Ukrainian combat UAV. However, after the photographs of the drone went viral, the authorities acknowledged that it was an Iranian 'Mohajer-6' drone that remains in service with the Russian military.

   Pro-Ukraine social media accounts and local Ukrainian media were quick to mock the incident, labeling it as an error by Russia's "demoralized forces." The drone was

downed in the eastern part of Crimea, and the kill has been attributed to Moscow's formidable Electronic Warfare (EW) system.

5. IDF's electronic warfare role jumps forward in current major IDF drill (The Jerusalem Post, 06 JUN, Yonah Jeremy Bob)

They were about to aim and fire a precise form of weaponry at IDF forces in the field when suddenly the IDF could hear the enemy forces asking themselves, "Why aren't we shooting? Why aren't we shooting?"

The Jerusalem Post has learned that in this still mostly classified instance in which the IDF's electromagnetic spectrum warfare center was used to disable the enemy forces ability to function, neither the enemy forces nor the IDF forces who were saved had a clue what had transpired.

6. Army 'on the cusp of greatness' with its critical EW programs (Defense News, 05 JUN, Jaspreet Gill)

The Army is progressing in its EW portfolio "after a few solid years of investment, lots of support from the Army and from [the Defense Department]," Kenneth Strayer said.

The Army is making progress on two of its most critical electronic warfare (EW) programs as the service seeks to "reestablish its dominance to the spectrum for the next fight," according to a service official.

Information Advantage

1. **Google, one of AI's biggest backers, warns own staff about chatbots (Reuters, 15 JUN, Jeffrey Dastin & Anna Tong)**

   Alphabet Inc (GOOGL.O) is cautioning employees about how they use chatbots, including its own Bard, at the same time as it markets the program around the world, four people familiar with the matter told Reuters.

   The Google parent has advised employees not to enter its confidential materials into AI chatbots, the people said and the company confirmed, citing long-standing policy on safeguarding information.

2. **France accuses Russia of faking websites to sow confusion and disinformation about Ukraine war (AP News, 13 JUN)**

   France's government accused Russia on Tuesday of operating a long-running online manipulation campaign, including impersonating the websites of leading French media and the French Foreign Ministry, aimed at spreading confusion and false information about the war in Ukraine.

   The French agency responsible for fighting foreign digital interference, VIGINUM, said it has monitored the alleged operation since soon after Russia invaded its neighbor and that France was one of several European countries targeted. It said it traced the campaign to Russian individuals, companies and "state entities or entities affiliated to the Russian state."

3. **US decides to rejoin UNESCO and pay back dues, to counter Chinese influence (AP News, 12 JUN, Angela Charlton & Matthew Lee)**

   UNESCO announced Monday that the United States plans to rejoin the U.N. cultural and scientific agency — and pay more than $600 million in back dues — after a decade-long dispute sparked by the organization's move to include Palestine as a member.

   U.S. officials say the decision to return was motivated by concern that China is filling the gap left by the U.S. in UNESCO policymaking, notably in setting standards for artificial intelligence and technology education around the world.

   The move will face a vote by UNESCO's member states in the coming weeks. But approval seems a formality after the resounding applause that greeted the announcement in UNESCO's Paris headquarters Monday. Not a single country raised an objection to the return of a country that was once the agency's single biggest funder.

4. **The viral AI-generated image showing an explosion near the Pentagon is 'truly the tip of the iceberg of what's to come,' tech CEO says (Insider, 09 JUN, Grace Dean)**

   The viral AI-generated image showing an explosion near the Pentagon is "truly the tip of the iceberg of what's to come," a CEO who works in image authenticity detection has warned.

   The image, which was largely thought to have been created using AI, quickly spread on social media last month and even caused the stock market to briefly dip.

5. **Unlock new insights with Azure OpenAI Service for government (Microsoft, 07 JUN)**

Microsoft continues to develop and advance cloud services to meet the full spectrum of government needs while complying with United States regulatory standards for classification and security. The latest of these tools, generative AI capabilities through Microsoft Azure OpenAI Service, can help government agencies improve efficiency, enhance productivity, and unlock new insights from their data.

6. **Senators plan briefings on AI to learn more about risks (C4ISR Net, 07 JUN, Colin Demarest)**

Democrats and Republicans can agree on at least one thing: There is insufficient understanding of artificial intelligence and machine learning in Congress.

So senators are organizing educational briefings. Majority Leader Chuck Schumer, a New York Democrat, on June 6 announced three such planned get-togethers this summer, including a classified session dedicated to AI employment by the U.S. Department of Defense and the intelligence community, as well as AI developments among "our adversaries" such as China and Russia.

7. **Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data (AP News, 07 JUN, Zen Soo)**

A former executive at ByteDance, the Chinese company which owns the popular short-video app TikTok, says in a legal filing that some members of the ruling Communist Party used data held by the company to identify and locate protesters in Hong Kong.

Yintao Yu, formerly head of engineering for ByteDance in the U.S., says those same people had access to U.S. user data, an accusation that the company denies.

Yu, who worked for the company in 2018, made the allegations in a recent filing for a wrongful dismissal case filed in May in the San Francisco Superior Court. In the documents submitted to the court he said ByteDance had a "superuser" credential — also known as a god credential — that enabled a special committee of Chinese Communist Party members stationed at the company to view all data collected by ByteDance including those of U.S. users.

The credential acted as a "backdoor to any barrier ByteDance had supposedly installed to protect data from the C.C.P's surveillance," the filing says.

8. **US Wages 'Undeclared War' Against Russia; Ukraine Tries Psychological Warfare Against Russian Military (The EurAsian Times, 07 JUN, Ashish Dangwal)**

The US is waging an undeclared war against Russia and Belarus, Russian Security Council Secretary Nikolay Patrushev said, Tass reported.

"The US is waging an undeclared war against Russia and Belarus, aiming to destroy the national identity and the people of our countries. Today, Western politicians state this openly and point this out in their documents," Patrushev said.

US and UK governments are using NATO, EU, Ukrainian neo-Nazis, and NGOs, as well as Ukraine's puppet government, to weaken Russia, the official believes.

10. **Japan, Australia, US to fund undersea cable connection in Micronesia to counter China's influence (AP News, 07 JUN, Mari Yamaguchi)**

Japan announced Tuesday that it joined the United States and Australia in signing an agreement on a $95 million undersea cable project that will connect East Micronesia island nations to improve networks in the Indo-Pacific region where China is increasingly expanding its influence.

The approximately 2,250-kilometer (1,400-mile) undersea cable will connect the state of Kosrae in the Federated States of Micronesia, Tarawa in Kiribati and Nauru to the existing cable landing point located in Pohnpei in Micronesia, according to the Japanese Foreign Ministry.

11. **From Provocations And Deterrence To Preparing For Unification: Why An Information Campaign Is Vital To Political Warfare In Korea (19 Forty Five, 05 JUN, David Maxwell & Matthew Ha)**

North Korea has conducted sustained psychological warfare or information operations against its own people, the Republic of Korea, the U.S., and the international community. The ROK-U.S. alliance has not reciprocated to any appreciable extent.

Psychological warfare and propaganda are critical to supporting the three major lines of effort of the Kim family regime. First is political warfare to subvert the ROK and drive a wedge in the ROK-U.S. alliance. Second is blackmail diplomacy — the use of increased tensions, threats, and provocations to gain political and economic concessions. Third is the development of advanced warfighting capabilities to support its political warfare and blackmail diplomacy strategies and ultimately to conduct its campaign to unify the Korean peninsula by force.

12. **Russia says Ukraine is launching major attacks; Kyiv accuses Moscow of misinformation (AP News, 05 JUN, Susie Blann)**

Ukrainian forces were making a major effort to end months of a battlefield stalemate and punch through Russian defensive lines in southeast Ukraine for a second day, with Russian officials saying on Monday that Moscow's forces have foiled at least one assault.

Kyiv authorities said their forces were indeed increasing offensive operations and making gains, but suggested some of the Russian announcements were misinformation as speculation grows about a widely anticipated counteroffensive after more than 15 months of war.

Vladimir Rogov, an official in the Russia-backed administration of Ukraine's partly occupied Zaporizhzhia province, said fighting resumed on its border with the eastern Donetsk province on Monday after Russian defenses beat back a Ukrainian advance the previous day.

13. **'Testing Ground' For Artificial Intelligence, Ex-US Navy Admiral Says Ukraine War Hotbed For Cutting-Edge Technology (The EurAsian Time, 04 JUN)**

Amidst the grueling warfare in Ukraine, marked by mud, trenches, and intense infantry attacks akin to those witnessed during World War I, a retired US Navy admiral has pointed out how the war in Ukraine could serve as a testing ground for artificial intelligence (AI).

In an opinion piece published in Bloomberg, James Stavridis, a retired US Navy

admiral and former supreme allied commander of NATO, has made a compelling prediction regarding the future of AI in military operations.

Stavridis believes that fast advances in artificial intelligence (AI) will soon play a critical role in supporting decision-makers on the battlefield at all levels of the military hierarchy.

14. BRI - Belt and Road Initiative - Highlights, 31 May 2023, (U.S. Army Asian Studies Detachment, 01 JUN)

The Belt and Road Initiative (BRI) is an expansive economic and infrastructure program initiated by the People's Republic of China aimed at increasing its influence throughout the world. Targeted primarily at poorer nations, or nations the PRC has a strategic interest in, it aims to increase the infrastructure usable by the PRC as well as making those nations economically dependent upon the PRC.
The following is a compilation of reports covering projects the PRC will initiate or have already started, as well as covering the evaluation or criticism of BRI in local countries and diplomatic efforts by China to promote BRI.

15. Air Force Colonel Now Says Drone That Turned On Its Operator Was A "Thought Experiment" (The Drive, 01 JUN, Joseph Trevithick)

A U.S. Air Force officer says he misspoke when describing a simulation involving a drone going rogue and attacking its controllers.

AU.S. Air Force officer helping to spearhead the service's work on artificial intelligence and machine learning says that a simulated test saw a drone attack its human controllers after deciding on its own that they were getting in the way of its mission. The anecdote, which sounds like it was pulled straight from the Terminator franchise, was shared as an example of the critical need to build trust when it comes to advanced autonomous weapon systems, something the Air Force has highlighted in the past. This also comes amid a broader surge in concerns about the potentially dangerous impacts of artificial intelligence and related technologies.

Update: The Royal Aerospace Society says that Col. Tucker Hamilton has since reached out to them directly about this and "admits he 'mis-spoke' in his presentation at the Royal Aeronautical Society FCAS Summit and the 'rogue AI drone simulation' was a hypothetical 'thought experiment' from outside the military, based on plausible scenarios and likely outcomes rather than an actual USAF real-world simulation." An update to their initial report adds that Hamilton told them "the USAF has not tested any weaponized AI in this way (real or simulated)."

Signal

1. **How a Shady Chinese Firm's Encryption Chips Got Inside the US Navy, NATO, and NASA (Wired, 15 JUN, Andy Greenberg)**

   The US government warns encryption chipmaker Hualan has suspicious ties to China's military. Yet US agencies still use one of its subsidiary's chips, raising fears of a backdoor.

   FROM TIKTOK TO Huawei routers to DJI drones, rising tensions between China and the US have made Americans—and the US government—increasingly wary of Chinese-owned technologies. But thanks to the complexity of the hardware supply chain, encryption chips sold by the subsidiary of a company specifically flagged in warnings from the US Department of Commerce for its ties to the Chinese military have found their way into the storage hardware of military and intelligence networks across the West.

2. **Device level quantum-computing-hardened encryption keys (EE News, 14 JUN, Jean-Pierre Joosting)**

   Quantinuum has announced the launch of Quantum Origin Onboard, an innovation in cryptographic key generation that provides quantum computing hardened cyber protection for a wide range of connected devices by maximizing the strength of keys generated within the devices themselves.

   The risk of cyberattacks compromising organizations continues to grow. As cybercriminals uncover new techniques to exploit connected systems and their data, even the cryptographic foundations of cybersecurity measures remain vulnerable to advanced threats. Cryptographic keys created using current typical methods deployed by organizations around the world are not provably unpredictable, leaving encrypted data and systems potentially at risk of devastating attacks. Quantinuum's quantum-computing-hardened cryptographic key enhancement provably minimizes the risk that businesses generate and use vulnerable encryption keys to protect encrypted data.

3. **China's quantum leap — Made in Germany (DW, 13 JUN, Sandra Petersmann)**

   Germany's oldest university hosts many scientists conducting groundbreaking work. Little did they know how they would become entangled in China's quantum military strategy. A DW investigation with CORRECTIV.

   The podium is decorated with pink and white plastic flowers. The Chinese man behind it speaks at length about a laser radar system for detecting stealth aircraft. Amid the COVID-19 lockdown in 2020, his audience joins him virtually for the talk.

   A young participant is curious — why is quantum research so important for Xinjiang? The Xinjiang Association of Science and Technology has organized the online session to showcase groundbreaking achievements in Chinese quantum research.

   It's a "battlefield against terrorism," the lecturer replies, referring to the northwest province. As the technical director of Chinese start-up Quantum CTek's Xinjiang branch, his words are deliberate, even telling.

4. **DoD finding it 'hard to orchestrate' services on zero trust, holding monthly discussions: Resnick (Breaking Defense, 08 JUN, Jaspreet Gill)**

The Pentagon has started doing weekly “huddles” and larger monthly meetings with the services and “communities of interest” in an effort to educate them on how to execute the department’s vision outlined in its zero trust strategy.

The Pentagon is keeping a close eye on the military services as they develop their own plans for implementing the department’s zero trust vision, a key official spearheading the effort said today.

The Defense Department’s zero trust strategy, released last November, tasked each service to develop its action plan to achieve a baseline level of zero trust by fiscal 2027. But Randy Resnick, the director of the Defense Department’s zero trust portfolio management office, said today that it’s proving “hard to orchestrate” each service’s individual zero trust efforts into something cohesive.

5. DoD official envisions faster ‘secure pipeline’ to help small business tech contractors protect information (Breaking Defense, 07 JUN, Jaspreet Gill)

"In my mind, these are some of these avenues that we're looking at at an idea phase now to see if we can put resources behind it," said Robert Vietmeyer, director for cloud and software modernization.

The Defense Department is considering extending a “secure pipeline” to small businesses to help them protect the department’s controlled unclassified information (CUI) while also speeding up their software deliveries, according to an official in the DoD Chief Information Office (CIO).

“One of the challenges we’re finding dealing with the smaller industries and others that haven’t worked in the defense space is our adversaries will attack our weakest links, and if folks aren’t ready for nation-state advanced persistent threat attacks, our sensitive information can be compromised,” Robert Vietmeyer, director for cloud and software modernization, said at a virtual Potomac Officers Club event today.

6. Expand National Quantum Initiative to keep up with China, say officials, experts, legislators (Breaking News, 07 JUN, Sydney J. Freedberg)

With 2018 National Quantum Initiative Act up for renewal, the House Science Committee held a hearing on how to expand the NQI’s support to government, academic, and industry R&D – with Chinese competition much in mind.

The US and China are neck and neck in quantum technology, witnesses warned the House Science Committee today. And if the US is to gain the edge, officials and experts argued, Washington should step up the National Quantum Initiative’s support to academic researchers still struggling to get access to experimental equipment and to startup companies still struggling to get investors.

Quantum computing has implications across a host of national security applications, from quickly cracking traditional encryption to building ultra-precise sensors and navigation systems. But while the US government has played with the technology for years, no one can say how close it is to practical applications.

7. Army Assesses Cyber Posture of Its Weapons, Control Systems Ahead of Zero Trust (GovCIO, 05 JUN, Anastasia Obis)

The U.S. Army is tasked with evaluating its weapons and control systems, as well as the Mission Partner Environment cyber posture to ensure it addresses zero trust principles.

As the U.S. Army looks to stand up a unified network based on zero trust principles, it will soon be assessing its weapons systems, control systems and the Mission Partner Environment to gain a clearer understanding of what cybersecurity implementation would look like on those systems in accordance with the zero trust framework.

The Defense Department's weapons systems are more software-reliant and networked than ever, making them vulnerable to cyber attacks. Developing secure weapons systems is highly challenging due to new and legacy systems living side by side and also supply chain disruptions, among other factors.

8. GDIT drastically upping investments in DoD emerging tech areas like AI, zero trust (Breaking Defense, 02 JUN, Jaspreet Gill)

GDIT President Amy Gilliland spoke to Breaking Defense about how the tech company is redirecting its investments to meet the technological demands of the day, including incorporating lessons from Ukraine.

General Dynamics Information Technology is pouring more money towards areas that the Pentagon deems emerging and critical to the future of warfighting, like artificial intelligence, in a move that the company president told Breaking Defense is a culmination of lessons learned over the past few years, particularly in the aftermath of Russia's invasion of Ukraine.

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 June 2023
Russia-Ukraine Situation Report, 14 June 2023
Russia-Ukraine Situation Report, 13 June 2023
Russia-Ukraine Situation Report, 12 June 2023
Russia-Ukraine Situation Report, 09 June 2023
Russia-Ukraine Situation Report, 08 June 2023
Russia-Ukraine Situation Report, 06 June 2023
Russia-Ukraine Situation Report, 05 June 2023
Russia-Ukraine Situation Report, 02 June 2023
Russia-Ukraine Situation Report, 01 June 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Ukraine Situation Report: Kyiv Claims Small Gains In The Face Of "Very Tough Resistance" – 15 JUN
Ukraine Situation Report: Fierce Fighting Near Mokri Yaly River – 13 JUN
Ukraine Situation Report: U.S. Sending More Bradleys – 12 JUN
Ukraine Situation Report: Advances Made In Grueling Fight – 11 JUN
Ukraine Situation Report: Putin Chimes In On 'Intense Fighting' – 09 JUN
Ukraine Situation Report: Offensive Brings Claims Of Limited Breakthroughs – 08 JUN
Ukraine Situation Report: 'Partisans' Threaten Crimean Incursion Next – 07 JUN
Ukraine Situation Report: Offensive Going Better Than Expected, U.S. Says – 06 JUN
Ukraine Situation Report: Su-24 Spotted Carrying Two Storm Shadows – 03 JUN
Ukraine Situation Report: Long-Range Strike Hits Russian-Held Port City On Sea Of Azov – 02 JUN

3. Deutsche Welle (DW) Ukraine updates

Ukraine updates: Kryvyi Rih targeted by more Russian strikes – 15 JUN
Ukraine updates: Odesa hit by deadly Russian missile attack – 14 JUN
Ukraine updates: Russia strikes Zelenskyy's hometown – 13 JUN
Ukraine updates: Kyiv claims first counteroffensive gains – 12 JUN
Ukraine updates: Kakhovka dam blast threatens water supply – 11 JUN
Ukraine updates: Kyiv claims advances near Bakhmut – 05 JUN

4. Russian Capture Of Ukrainian Leopard Tank, Bradleys Seen In Video (The Drive, 13 JUN, Thomas Newdick)

The Russian Ministry of Defense has released video showing the capture of Leopard 2 and Bradley fighting vehicles in an incident last week.

The Russian Ministry of Defense has released a video showing a German-made Leopard 2 main battle tank and U.S.-made M2 Bradley infantry fighting vehicles that it says were captured by its forces in Ukraine. The footage provides us with our closest yet look at examples of these vehicles lost in the recent counteroffensive, with the scene showing the aftermath of the failed breaching operation last week, an incident that we have since looked at in depth.

5. Ukraine Accuses Russia Of Blowing Up Another Dam (The Drive, 12 JUN, Thomas Newdick)

A dam along the Mokri Yaly River in eastern Ukraine is the latest such barrier to have been breached by Russian forces, Kyiv claims.

Ukraine has accused Russia of blowing up another dam as part of its efforts to blunt the Ukrainian counteroffensive underway in the south and east of that country. Details are still emerging, but the dam in question is along the Mokri Yaly River, in western Donetsk, in a region where Ukrainian forces are said to have made their biggest gains. The incident comes six days after a significant portion of the larger Kakhovka dam was blown up, causing extensive flooding in the Kherson region, with both sides blaming each other for the destruction. You can read our coverage of the earlier incident here.

The exact location of the dam is in the village of Klyuchove, in Russian-held territory. So far, there has not been independent verification of the dam's destruction, although a time-lapse video presented below, from the Sentinel Hub satellite data provider, does appear to show almost all the water leaving the Staromlynivske Reservoir behind the dam. While Ukrainian accounts suggest some kind of explosion breaching the dam, it remains possible that Russian forces may have simply opened sluices to drain the reservoir as quickly as possible.

6. Russia's improved weaponry and tactics pose challenges to Ukraine's counteroffensive (AP News, 12 JUN)

7. AP Exclusive: Drone footage of collapsed dam shows devastation, no evidence to back Russian claims (AP News, 08 JUN)

Exclusive drone footage of the collapsed Ukrainian dam and surrounding villages under Russian occupation showed the ruined structure falling into the flooded river, hundreds of submerged homes, greenhouses, even a church — and no evidence of an attack from above, as Russia alleges.

An Associated Press team flew a drone over the devastation on Wednesday, a day after the destruction of the Kakhovka dam on the Dnieper River.

The bulk of the dam itself is submerged, but the parts of buildings still visible above the rushing waters had no scorch marks or shrapnel scars typical of a bombardment that Russia has accused Ukraine of carrying out.

Ukraine in turn has alleged that Russian forces, who controlled the dam, blew it up from within. The AP images offered a limited snapshot, making it difficult to categorically rule out any scenario. The dam had been weakened by months of Russian neglect and water had been washing over it for weeks.

8. Chinese 'Tiger' Roars In Ukraine War; Pro-Russia Troops Flaunt

Chinese Military Vehicles For SMO (The EurAsian Times, 08 JUN, Sakshi Tiwari)

For the first time, Chinese-origin "Tiger" Armored Personnel Carriers (APCs) manufactured by Shaanxi Baoji Special Vehicles have been spotted with pro-Russian military forces despite Chinese claims that it has not supplied military aid to Moscow.

On June 7, Chechen leader Ramzan Kadyrov showed a video flaunting what he called the "new vehicles purchased for Chechen units participating in the SMO" at his palace.

The footage featured over eight Shaanxi Baoji Special Vehicles Manufacturing Co. "Tiger" armored personnel carriers.

Since the start of the invasion, Ramzan Kadyrov's unit Akhmat has been officially a part of the Russian Guard and the Ministry of Internal Affairs of the Russian Federation and has been actively taking part in the war against Ukraine.

The armored vehicles were seen to be unarmed, although they do have a weapon mount. This may be the first incident where Russian-allied troops are directly fighting the war against Ukraine and have received Chinese military vehicles.

"We have purchased (since the beginning of the war – ed.) more than a thousand items of military equipment for our soldiers, including 128 items of armored vehicles," Chechen government officials said.

9. Ukraine's Big Offensive Kicks Off To Tough Resistance (The Race, 08 JUN, Howard Altman)

With Ukraine's counteroffensive fully underway, there are reports of casualties as it rushes Russian positions in Zaporizhzhia and Donetsk.

Ukraine's long-awaited counteroffensive is now fully underway as its troops, backed by NATO-donated Leopard-2 tanks and other armor, have pressed forward on multiple vectors across the battlefield. Heavy losses are being reported as Ukrainian forces attempt to punch through long-entrenched Russian positions in Zaporizhzhia and Donetsk oblasts.

10. Xi Jinping Calls for "Speeding up the Modernization of National Security" (U.S. Army Asian Studies Detachment, 06 JUN)

Chinese President Xi Jinping presided over the National Security Commission on 30 May 2023. Xi stated efforts must be made to prepare for "actual combat." Chinese state media quoted an associate dean as saying the commission referred to challenges such as a geopolitical or financial crisis, but also a "danger of war."

11. Who are the Freedom of Russia Legion and Russian Volunteer Corps? (Reuters, 05 June, Tom Balmforth & Max Hunderz)

Two armed groups, the Russian Volunteer Corps (RVC) and Freedom of Russia Legion, say they have carried out attacks in Russia's western Belgorod region in recent weeks.

Kyiv has denied any role and said the attackers are Russian citizens.

12. Crippled Russia Is 'Re-Importing' Military Hardware From India Amid Shortage Of Components – Reports (The EurAsian Times, 05 JUN, Sakshi Tiwari)

Faced with difficulties in procuring crucial components for producing some advanced equipment, Russia is suspected to be "repurchasing" some equipment that it previously

sold to Asian partners, India and Myanmar.

These claims were made by the Japanese news outlet Nikkei Asia which reportedly analyzed customs clearance data before making the assumption. The publication said the survey found documents of Russian repurchases of missile and tank parts that had previously been shipped to Myanmar and India.

The report contends that Russia may be reimporting parts to upgrade older weaponry intended for use in Ukraine with assistance from nations with which it has strong military ties.

13. Foreign Reflections on U.S. Exercises and Operations, 5 June 2023 (U.S. Army Asian Studies Detachment, 05 JUN)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 25 May to 1 June 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, India, Japan, North Korea, the Philippines, and South Korea.

14. The Taliban Is Using U.S. And Russian Weapons To Fight Iran (19 Forty Five, 04 JUN, Maya Carlin)

A skirmish along the Iranian-Afghanistan border broke out last weekend, resulting in a gun fight that killed three people.

Video footage depicting the debacle circulated widely on social media, which covered the aftermath of a dispute about water. In the footage, Taliban fighters in the Nimroz province of Afghanistan used American-made armored Humvees and a Navistar 7000 transport truck on the border.

The Taliban fighters appear to be operating an M240 machine gun, AK riles and RPG-7 Launcher with PG-7V rocket from inside the vehicle. According to Al-Jazeera, Tehran claimed that the three killed were Iranian while the Taliban purported that one of the deaths was from its side.

15. Attacks in Russia 'destroy myth of Putin's invincible army' (DW, 02 JUN, Maria Katamadze)

Recent drone attacks and the shelling of a Russian border town have forced residents to flee their homes, sowing panic and fear. The Kremlin has downplayed the raids, but experts think they reveal Putin's weaknesses.

16. Russia Claims It Foiled Tank-Backed Incursion Across Its Border (The Drive, 01 JUN, Howard Altman)

This was the second incursion operation Russia says it has fought off in just over a week, but still there was damage within its own borders.

Self-proclaimed anti-Putin partisans say they staged another cross-border raid several miles into Belgorod Oblast early Thursday morning local time. The Russian Defense Ministry (MoD), however, claims after intense artillery fire inside Russia, its forces repelled the attackers, who were backed with tanks, before they could penetrate Russian territory.

The partisans - the far-right Russian Volunteer Corps (RDK) and the Freedom For Russia Legion - claimed as of Thursday afternoon local time that they still occupied parts of the region, destroyed several Russian artillery and mortar systems and captured another armored vehicle. The Russian Defense Ministry (MoD) disputed that, saying the attempted incursion, conducted by “Ukrainian terrorist groups with up to two

motorized companies" was unsuccessful and that those taking part were wiped out.