U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

16 - 30 November 2023

Prepared by: Threat Management Office CCoE
Fort Gordon, GA 30905
POC: Jeffrey Hardimon & Kevin Bird
706-849-9259

Table of Contents

11. Addressing the State of AI's Impact on Cyber Disinformation/Misinformation – 15 NOV

Signal

1. US Army developing intel analysis, combat weather apps – 28 NOV
2. Huawei Eyes Connectivity Similar To SpaceX's Starlink After Maiden Satellite Test – 26 NOV
3. China Telecom Develops Network Cloud Infrastructure Platform Kit - 17 NOV
4. From PKI to PQC: Devising a strategy for the transition - 16 NOV
5. Quantum Sensors vs. Quantum Computers: IDTechEx Takes a Look at the Next 10 Years - 16 NOV
6. Lockheed Martin to demonstrate space-based 5G network - 16 NOV
7. US Calls Chinese ASAT Missiles 'Biggest Threat' To The Country; Says Poses 'Double Trouble' In Space - 16 NOV

Items of Interest

1. North Korea's First Satellite No Threat To US Navy, Pyongyang Knows It Has Long Way To Go: Experts – 29 NOV
2. Cartel Narco Tank With Cope Cage Anti-Drone Armor Emerges – 28 NOV
3. Kim Jong Un reviews satellite photos of U.S. bases in Hawaii, South Korea: state media – 28 NOV
4. China's J-11 Flanker-L 'Softens' US Air Force; US Resumes 'Mil-To-Mil' Contact With PLA To Deflate Tensions – 25 NOV
5. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 22, 2023 – 22 NOV
6. North Korea claims it successfully put spy satellite into orbit – 21 NOV
7. US renews concerns over N. Korea-Russia military cooperation – 21 NOV
8. North Korea warns Japan of impending spy satellite launch – 21 NOV
9. Seoul warns North Korea not to launch spy satellite and hints 2018 military deal could be suspended - 20 NOV
10. Aging Population & Low Birth Rate, China Struggles To Fill PLA Ranks; To Become Aged Society In 25 Years - 20 NOV
11. China-Taiwan Weekly Update, November 17, 2023 - 17 NOV
12. China Wants 'Nuclear Parity' With US; Could Achieve The Scary Milestone By Mid-2030s – Congressional Panel - 17 NOV
13. Taiwan's Civilian Simulation of a Chinese Military Invasion Exposes Weaknesses in Basic Infrastructure - 17 NOV

Israel-Hamas Conflict

1. The Drive Israel-Gaza Update
2. Institute for The Study of War Iran Update:
3. Truce in Israel-Hamas war extended by a day, minutes before it was set to expire – 27 NOV
4. Shadowy hacking group targeting Israel shows outsized capabilities – 27 NOV
5. Israel-Hamas war live: Hamas says 'truce agreement' is close - 21 NOV
6. Jordan doubts Israel can destroy Hamas as Gaza war rages - 18 NOV

Russia-Ukraine Conflict

1. Russia-Ukraine Situation Report
2. The Drive/The Warzone Ukraine Situation Report:

3. Institute for The Study of War
4. Shahed-136 With Cellular Modem Found In Ukraine: What It Means – 30 NOV
5. Putin won't make peace in Ukraine before 2024 US election – 29 NOV
6. Russia launches largest drone attack since start of Ukraine invasion – 25 NOV
7. Germany to supply Ukraine with IRIS-T systems in $1.4 billion package – 24 NOV
8. Ukraine conflict: Ukrainian air defense employs passive sensors for detection and tracking – 24 NOV
9. Soviet-Era M-55 Spy Plane May Be Headed To Support The War In Ukraine – 21 NOV
10. The World's Attention is on Gaza, and Ukrainians Worry War Fatigue Will Hurt Their Cause – 18 NOV
11. China is the main supplier of dual use goods needed to run Russia's military machine – 16 NOV

Cyber

1. **US Sanctions Cryptocurrency Mixer Sinbad for Aiding North Korean Hackers (SecurityWeek, 30 NOV, Ionut Arghire)**

The US Department of the Treasury on Wednesday announced sanctions against cryptocurrency mixer Sinbad, for laundering stolen cryptocurrency for the North Korean state-sponsored hacking group Lazarus.

Sinbad, the Treasury says, is the preferred mixing service for Lazarus, and is responsible for laundering millions of dollars in stolen cryptocurrency for the nation state threat actor.

Operating on the Bitcoin blockchain, the mixer obfuscates the origin, destination, and counterparties of illicit transactions, and is believed to be a successor to the Blender.io mixer, which was previously sanctioned for aiding Lazarus.

Sinbad, the Treasury says, also obfuscates transactions linked to other malicious activities, including sanctions evasion, drug trafficking, and illicit sales on dark web marketplaces.

According to the US, Sinbad was involved in laundering a "significant portion" of the $100 million in cryptocurrency stolen from Atomic Wallet in June 2023, of the $620 million stolen from Axie Infinity in March 2022, and of the $100 million stolen in June 2022 from Horizon Bridge.

2. **Ransomware gang broken up in Ukraine as a result of international operation (DefenseScoop, 28 NOV, AJ Vicens)**

Back to Table of Contents

Authorities in Ukraine arrested five people in recent days as part of an international investigation into ransomware attacks, Ukrainian and European authorities said 28NOV2023.

Police in Ukraine arrested a 32-year-old man they say was the "leader" of a group, as well as "his four most active accomplices," according to a Google translation of a statement issued by the Ukrainian Cyber Police.

The crew's attacks impacted victims in 71 countries, according to the statement, using ransomware variants including LockerGoga, MegaCortex, HIVE and Dharma. The arrests are the continuation of an investigation that began in 2019 and included 12 arrests in 2021.

The attackers successfully encrypted more than 250 servers "belonging to large corporations, resulting in losses exceeding several hundred million" euros, authorities said.

3. **UK, Korea Warn of DPRK Supply Chain Attacks Involving Zero-Day Flaws (Security Week, 27 NOV, Ionut Arghire)**

The UK National Cyber Security Centre (NCSC) and Korea's National Intelligence Service (NIS) have issued a fresh warning on Democratic People's Republic of Korea (DPRK) state-sponsored hackers targeting government, financial, and defense organizations via software supply chain attacks.

As part of the observed supply chain attacks, the DPRK threat actors employed zero-day and n-day vulnerabilities, and exploited multiple flaws in series "to precisely attack a specific target", NCSC and NIS note in the alert.

In an attack carried out in March 2023, the hackers exploited a bug in the MagicLine4NX security authentication software for initial access and a zero-day issue in a network-linked system for lateral movement.

4. **Hackers Hijack Industrial Control System at US Water Utility (Security Week, 27 NOV, Eduard Kovacs)**

Municipal Water Authority of Aliquippa in Pennsylvania confirms that hackers took control of a booster station, but says no risk to drinking water or water supply.

The Municipal Water Authority of Aliquippa in Pennsylvania has confirmed that hackers took control of a system associated with a booster station over the weekend, but said there was no risk to the water supply.

The company provides water and sewer services to more than 6,600 customers in Aliquippa and portions of Hopewell, Raccoon and Potter Townships.

A representative of the water utility told KDKA-TV that the compromised system is associated with a booster station that monitors and regulates water pressure for Raccoon and Potter Townships.

5. **North Korean Software Supply Chain Attack Hits North America, Asia (Security Week, 24 NOV, Eduard Kovacs)**

North Korean hackers breached a Taiwanese company and used its systems to deliver malware to the US, Canada, Japan and Taiwan in a supply chain attack.

A North Korean threat group breached a Taiwanese software company and leveraged its systems to deliver malware to devices in North America and Asia, Microsoft reported this week.

Back to Table of Contents

The threat actor is tracked by the tech giant as Diamond Sleet (Zinc). Previously described as a sub-group of the notorious Lazarus, the hacker gang has been conducting attacks for data theft, espionage, destruction and financial gain. In the past, it was observed targeting security researchers, penetration testers, and cybersecurity and tech company employees.

Microsoft discovered recently that Diamond Sleet had targeted CyberLink Corp, a Taiwan-based software company specializing in audio, video and photo editing applications.

6. **Diamond Sleet supply chain compromise distributes a modified CyberLink installer (Microsoft, 22 NOV)**

Microsoft Threat Intelligence has uncovered a supply chain attack by the North Korea-based threat actor Diamond Sleet (ZINC) involving a malicious variant of an application developed by CyberLink Corp., a software company that develops multimedia software products. This malicious file is a legitimate CyberLink application installer that has been modified to include malicious code that downloads, decrypts, and loads a second-stage payload. The file, which was signed using a valid certificate issued to CyberLink Corp., is hosted on legitimate update infrastructure owned by CyberLink and includes checks to limit the time window for execution and evade detection by security products. Thus far, the malicious activity has impacted over 100 devices in multiple countries, including Japan, Taiwan, Canada, and the United States.

Microsoft attributes this activity with high confidence to Diamond Sleet, a North Korean threat actor. The second-stage payload observed in this campaign communicates with infrastructure that has been previously compromised by Diamond Sleet. More recently, Microsoft has observed Diamond Sleet utilizing trojanized open-source and proprietary software to target organizations in information technology, defense, and media.

7. **Russian hackers use Ngrok feature and WinRAR exploit to attack embassies (Bleeping Computer, 19 Nov, Ionut Ilascu)**

After Sandworm and APT28 (known as Fancy Bear), another state-sponsored Russian hacker group, APT29, is leveraging the CVE-2023-38831 vulnerability in WinRAR for cyberattacks.

APT29 is tracked under different names (UNC3524,/NobleBaron/Dark Halo/NOBELIUM/Cozy Bear/CozyDuke, SolarStorm) and has been targeting embassy entities with a BMW car sale lure.

The CVE-2023-38831 security flaw affects WinRAR versions before 6.23 and allows crafting .RAR and .ZIP archives that can execute in the background code prepared by the attacker for malicious purposes.

8. Researchers Dive Into Activities of Indian Hack-for-Hire Firm Appin (SecurityWeek, 17 NOV, Ionut Arghire)

For over a decade, Indian firm Appin Software Security has been offering offensive security training and covert hacking services targeting governments and private organizations worldwide, SentinelOne reports.

Informally known as Appin Security Group (ASG), the Appin group of companies can be tied to much of the current Indian advanced persistent threat (APT) activity, with some of its former employees forming newer competitors and others moving into the cyber defense industry.

Considered the original hack-for-hire company in India, Appin has been operating since at least 2009, targeting entities in the US, Bangladesh, Canada, China, Kuwait, India, Myanmar, Pakistan, UAE, and other locations.

Back to Table of Contents

Attacks against Pakistani government officials started over a decade ago, involving keyloggers that exfiltrated social media, email account, and government website credentials, along with other personal information, SentinelOne notes.

9. Israeli Man Who Made $5M From Hacking Scheme Sentenced to Prison in US (SecurityWeek, 17 NOV, Eduard Kovacs)

An Israeli private investigator who made nearly $5 million by hacking companies and individuals has been sentenced to 80 months in prison in the United States, the Justice Department announced on Thursday.

Authorities said the man, 52-year-old Aviram Azari, was arrested on computer hacking, wire fraud and identity theft charges when he traveled to the United States in September 2019.

According to the Justice Department, Azari owned and operated an Israel-based ‘intelligence firm’ named Aviram Hawk or Aviram Netz.

Between 2014 and 2019, the company was hired by various clients to obtain intelligence on specified targets. Azari obtained the intelligence by hiring different hacking groups, including one located in India, to access online accounts and steal information, often by leveraging spear-phishing emails.

Targets included hedge funds, tech companies, journalists, and climate change activists. Investigators identified roughly 300 targets, including 100 for which successful hacking was confirmed.

10. **Russian Hacking Group Sandworm Linked to Unprecedented Attack on Danish Critical Infrastructure (Infosecurity-Magazine, 16 NOV, James Coker)**

Notorious Russian nation-state threat actor Sandworm has been linked to the largest ever cyber-attack targeting critical infrastructure in Denmark.

The incident took place in May 2023 and saw the attackers targeted 22 companies involved in operating Danish critical infrastructure, according to SektorCERT, a non-profit that helps protect organizations in this sector.

SektorCERT found evidence connecting some of these attacks to Sandworm, a group thought to operate under the Russian intelligence agency GRU. Sandworm was behind the attacks that took down power in parts of Ukraine in 2015 and 2016.

11. **Bad Bots Account for 73% of Internet Traffic: Analysis (Security Week, 16 NOV, Kevin Townsend)**

The top five categories of Bad Bot attacks are fake account creation, account takeovers, scraping, account management, and in-product abuse.

Arkose Labs has analyzed and reported on tens of billions of bot attacks from January through September 2023, collected via the Arkose Labs Global Intelligence Network.

Bots are automated processes acting out over the internet. Some perform useful purposes, such as indexing the internet; but the majority are Bad Bots designed for malicious ends. Bad Bots are increasing dramatically — Arkose estimates that 73% of all internet traffic currently (Q3, 2023) comprises Bad Bots and related fraud farm traffic.

Back to Table of Contents

The top five categories of Bad Bot attacks are fake account creation, account takeovers, scraping, account management, and in-product abuse. These haven't changed from Q2, other than in-product abuse replacing card testing. The biggest increases in attacks from Q2 to Q3 are SMS toll fraud (up 2,141%), account management (up 160%), and fake account creation (up 23%).

Electronic Warfare

1. **Lockheed Martin, Northrop Grumman score awards for Army's 'launched effects' initiative (DefenseScoop, 29 NOV, Mark Pomerleau)**

   The Army has awarded Lockheed Martin and Northrop Grumman agreements to work on a project designed to deploy sensors and jammers from the air, according to a Wednesday announcement.

   The other transaction agreements are for phase 1 of what the Army calls its Launched Effects program, which envisions small drones or payloads released by larger aircraft, either manned or unmanned. These smaller systems could include a variety of payloads and have the ability to loiter over a target, being either recoverable or expendable.

   This first of multiple phases, worth around $100,000 for each vender payload, will develop a statement of work for the effort for the next two phases and mature existing payloads from technology readiness level 6 to 7, and then integrate them within the infrared and electronic warfare realms.

   The Army said the overall value for the program OTA is expected to be around $37 million across the three phases.

2. **The Economist: Russia's EW superiority emerges as Ukraine's key weakness on frontline (Euromaidan Press, 27 NOV, Iryna Voichuk)**

Back to Table of Contents

   Ukraine confronts Russian advanced electronic warfare capabilities, facing a shortage of Western EW assistance, hindered by US export limits and the fears of NATO technology falling to China.

   While Ukraine actively employs drones against Russian forces, effectively destroying military equipment and strongholds, it nevertheless faces significant vulnerabilities to Russian electronic warfare (EW) systems, the Economist states. Moreover, although Western nations have concentrated their military aid on tangible hardware such as tanks and missiles, they have allocated relatively little towards aiding Ukraine in countering Russia's formidable EW capabilities.

   The Russian army has "adopted about 60 types of modern EW equipment, which have better characteristics, high mobility, increased security, short set-up and tear-down time, the introduction of new technical solutions, automation tools, special software," General Valerii Zaluzhnyi, Commander-in-Chief of the Ukrainian Armed Forces says in his essay.

3. **Electronic signal jamming from Ukraine, Gaza confuses civilian pilots far from battlefields (The Sydney Morning Herald, 22 NOV, Selam Gebrekidan)**

   Electronic warfare in the Middle East and Ukraine is affecting air travel far from the battlefields, unnerving pilots and exposing an unintended consequence of a tactic that experts say will become more common.

   Planes are losing satellite signals, flights have been diverted and pilots have received false location reports or inaccurate warnings that they were flying close to terrain, according to European Union safety regulators and an internal airline memo viewed by The New York Times.

   The US Federal Aviation Administration has also warned pilots about GPS jamming in the Middle East.

4. **New 'Attack' EA-37B Moniker For USAF Electronic Warfare Jets (The Drive/The Warzone, 21 NOV, Joseph Trevithick)**

The switch from EC-37B to EA-37B reflects the aircraft's capabilities, which could go well beyond jamming enemy radars and other emitters.

The U.S. Air Force has quietly changed the designation of its new electronic warfare jet from EC-37B to EA-37B. The service says this new moniker better reflects the aircraft's roles and missions, which it says includes attacking and destroying certain targets. The War Zone has long highlighted how powerful active electronically scanned array (AESA) antennas like the ones on the EA-37B could be used to send out highly focused beams of electromagnetic energy that can damage electronics within aircraft, missiles, and other systems.

The Air Force announced the designation change for what has become the EA-37B last week, but said at that time that the new nomenclature had been formally applied back in October. The Air Force formally took delivery of the first of these jets in September. The service currently plans to acquire 10 in total and hopes they will begin entering operation service next year.

The EA-37B/EC-37B is a heavily modified Gulfstream G550 business jet. It leverages the Israeli-developed Conformal Airborne Early Warning (CAEW) configuration, which notably has large 'cheek' fairings on either side of the fuselage among other distinctive features.

5. **Touted As 'Biggest Threat' To Russian Military, Moscow's EW Manages To Deflate M982 Excalibur Shells? (The EurAsian Times, 20 NOV, Ashish Dangwal)**

Back to Table of Contents

Once acknowledged by Russian fighters as a bigger threat than HIMARS, the effectiveness of US-supplied high-precision Excalibur shells has significantly withered in the ongoing conflict, attributed to advancements in Russian electronic warfare.

"This is probably the most dangerous part of the delivery. These Excalibur munitions are equipped with a seeker and can adjust their flight path upon approaching the target. They are GPS-and intertidal-guided," a DPR People's Militia spokesperson had earlier said.

"There can be only one countermeasure – effective counter-battery activities, with strikes at warehouses where those munitions are stored and vehicles transporting them to launchers. They must be prevented from ever being delivered to firing positions," he had added.

6. **New Technologies Could Help Resolve Ukraine's Artillery Challenges (Forbes, 19 NOV, Vikram Mittal)**

In a recent interview with The Economist, General Zaluzhny, the Commander-in-Chief of the Armed Forces of Ukraine, discussed the challenges faced by Ukrainian forces which have ultimately resulted in a stalemate with Russia. He emphasized that many of these issues are linked to artillery, highlighting that the Russian military presently holds a tactical advantage in that field. The Russians achieved this advantage by fielding new technologies that allow them to precisely hit Ukrainian targets while also limiting the effectiveness of Ukrainian artillery. He stressed the need for Ukraine to develop and deploy their own advanced technologies to regain the upper hand in the war.

7. **Ukraine is thinking more like Silicon Valley to defend itself against Russia's electronic warfare (Business Insider, 19 NOV, Lloyd Lee)**

- Russian jamming is a major source of frustration for Ukraine as it impacts comms and weapons.
- As a countermeasure, Ukraine has taken several steps to develop new warfare tech.
- This summer, the country hosted a hackathon to seek out technology that can fight Iranian-made drones.

8. **Electronic Warfare System Hunting Drones Wanted By SOCOM (The Drive/The War Zone, 17 NOV, Joseph Trevithick)**

Specialized seekers would help loitering munitions find and destroy electronic warfare systems, but could have other applications.

Small loitering munitions, also known as kamikaze drones, with new specialized seekers would be a valuable additional tool for finding and taking out enemy land-based electronic warfare systems, according to U.S. Special Operations Command. This underscores the threat posed by electronic warfare capabilities that potential adversaries, especially China and Russia, have already fielded and new systems they are continuing to develop. It also speaks to ongoing discussions about the roles of U.S. special operations in any future high-end conflict after decades of focusing on counter-terrorism, counter-insurgency, and other lower-intensity operations.

Back to Table of Contents

A contracting notice posted online discusses the core requirements U.S. Special Operations Command (SOCOM) has for what it is currently calling the Counter-Electronic Countermeasure Seeker, or CECMS.

9. **Ukraine conflict: Ukraine deploying indigenously developed SIGINT system (Janes, 16 NOV, Olivia Savage)**

Ukraine has developed and is deploying a signals intelligence (SIGINT) system on the frontline called Eter, the Ukrainian Minister for digital transformation, Mykhailo Fedorov said on 14 November.

Eter is a radio-electronic intelligence complex developed by Ukraine-based company Falcons and supported by the defence technology cluster Brave1. It comprises three direction finding (DF) systems for the detection of communication signals, unmanned aerial vehicles (UAVs), and electronic warfare systems, the company states.

The complex can operate for up to 24 hours in automatic mode, employ correlation-interferometric DF methods, and can detect equipment using frequency-hopping spread spectrum (FHSS) techniques, the company detailed. A number of complexes can also be connected to form a large network.

The company deliberately omits the range of the system on its website.

10. **The Most Critical Weapon in Ukraine and Israel Isn't Guns. It's Electronics (The Daily Beast, 15 NOV, David Axe)**

Powerful radio jammers have become crucial in modern warfare—and it's a tool Ukrainians need more than ever in order to defeat Russia.

A recording of a live video feed from a Russian military drone, apparently intercepted by Ukrainian forces and posted online, hints at an increasingly important front in Russia's 22-month wider war on Ukraine—an electronic front.

Look past the infantry battles, air raids, and naval maneuvering that dominate the news from the 600-mile front in Ukraine: You'll see that there's also a battle raging in the electromagnetic spectrum. And it might be one of the decisive battles as the wider war grinds toward its third year.

This electronic warfare isn't just evident in Ukraine. It's central to Israel's strategy in its assault on the Hamas terror group in Palestine, too. And if the Chinese Communist Party ever makes good on its threat to invade Taiwan, a move that could draw the United States and China into a major war, it's a safe bet the fighting will expand across the electromagnetic spectrum.

Back to Table of Contents

Information Advantage

1. **Hundreds of Malicious Android Apps Target Iranian Mobile Banking Users (SecurityWeek, 30 NOV, Ionut Arghire)**

A malicious campaign targeting mobile banking users in Iran is relying on hundreds of Android applications for credential and credit card information theft, mobile security firm Zimperium reports.

The campaign was brought to light in July, when Sophos reported on 40 malicious applications that circulated between December 2022 and May 2023, targeting the users of four Iranian banks, namely Bank Mellat, Bank Saderat, Resalat Bank, and Central Bank of Iran.

The malicious apps were found to harvest banking login credentials and credit card data, to intercept SMS messages to bypass multi-factor authentication, and to hide their icons to prevent removal. Masquerading as their legitimate counterparts available through the popular Iranian marketplace Cafe Bazaar, the applications were being distributed via phishing websites.

In addition to targeting the four banking applications, the samples in the first iteration check the infected devices for the presence of other apps as well, without actively targeting them, suggesting that the malware developers are planning to expand their attacks. In total, the malicious software targets 12 banking applications, while also checking devices for the presence of cryptocurrency wallets, likely to start targeting them in the future.

Back to Table of Contents

2. **China Diplomatic and Political Highlights, 28 November 2023 (U.S. Army Asian Studies Detachment, 28 NOV)**

This semi-weekly report is a compilation of English-language news articles related to China's diplomatic and political affairs, derived primarily from China-based news sources.

3. **Army releases first doctrinal publication focused on information (DefenseScoop, 27 NOV, Mark Pomerleau)**

The Army unveiled its first doctrinal publication focused solely on the information dimension of military action.

The highly anticipated document (ADP 3-13 INFORMATION), released publicly on 27NOV2023, was many years in the works. It aims to provide a framework for creating and exploiting information advantages during operations as well as at home station, according to officials.

The U.S. military, as a whole, has begun a shift, recognizing the importance information plays not only in conflict but in everyday life. Adversaries have sought to exploit the information realm on a daily basis — within the so-called gray zone, below the threshold of armed conflict — as a means of undermining U.S. and allied interests without having to confront them in direct military conflict.

Army Doctrinal Publication 3-13, Information “represents an evolution in how Army forces think about the military uses of data and information, emphasizing that everything Army forces do, to include the information and images it creates, generates effects that contribute to or hinder achieving objectives,” Lt. Gen. Milford Beagle, commander of the Combined Arms Center, wrote in the foreword. “As such, creating and exploiting

information advantages is the business of all commanders, leaders, and Soldiers.”.

4. Focus: New crypto front emerges in Israel's militant financing fight (Reuters, 27 NOV, Tom Wilson and Elizabeth Howcroft)

A new front has emerged in Israel’s fight against the funding of Iran-backed militant groups from Hamas to Hezbollah: A fast-growing crypto network called Tron that until recently attracted less scrutiny than Bitcoin.

Quicker and cheaper than Bitcoin, the Tron network has overtaken its rival as a platform for crypto transfers associated with groups designated as terror organizations by Israel, the United States and other countries, according to interviews with seven financial crime experts and blockchain investigations specialists.

A Reuters’ analysis of crypto seizures announced by Israeli security services since 2021 reflects the trend, showing for the first time a sharp rise in the targeting of Tron wallets and a fall in Bitcoin wallet seizures. “Earlier it was Bitcoin and now our data shows that these terrorist organizations tend to increasingly favor Tron,” said Mriganka Pattnaik, CEO of New York-based blockchain analysis firm Merkle Science, citing Tron’s faster transaction times, low fees, and stability.

Merkle Science says it counts law enforcement agencies in the United States, Britain and Singapore as clients. Israel’s National Bureau for Counter Terror Financing (NBCTF), which is responsible for such seizures, froze 143 Tron wallets between July 2021 and October 2023 that it believed were connected to a “designated terrorist organization” or used for a “severe terror crime,” the Reuters analysis found.

Back to Table of Contents

The Oct. 7 attacks by Hamas on Israel killed around 1,200 people. Israel’s subsequent bombardment and ground invasion of Gaza has killed some 14,000 people. In its response, Israel has also stepped up scrutiny of Hamas’ financing.

5. Taiwan/China: Cross-Strait Relations Report, 22 November 2023 – 22 NOV

This is a weekly report regarding Cross-Strait relations between China and Taiwan, based on local media reports. The report contains official information from both the Ministry of Foreign Affairs of the People's Republic of China and the Taiwan Affairs Office. A summary of the report topics can be viewed in the contents.

6. Foreign Reflections on U.S. Exercises and Operations, 22 November 2023 – 22 NOV

This report contains reporting of foreign reactions in the Asia-Pacific region to U.S. bilateral and multilateral exercises, and other United States Department of Defense activities such as weapons transfers and sales, military exchanges, and military operations. This report iteration covers relevant reporting from China, Taiwan, Russia, North Korea, India, the Philippines and Indonesia. The next report will be released on 01 December and will cover 22 - 30 November 2023.

7. Social engineering attacks lure Indian users to install Android banking trojans (Microsoft, 20 NOV)

Microsoft has observed ongoing activity from mobile banking trojan campaigns targeting users in India with social media messages designed to steal users’ information for financial fraud. Using social media platforms like WhatsApp and Telegram, attackers are sending messages designed to lure users into installing a malicious app on their mobile device by impersonating legitimate organizations, such as banks, government services, and utilities. Once installed, these fraudulent apps exfiltrate various types of sensitive

information from users, which can include personal information, banking details, payment card information, account credentials, and more.

While not a new threat, mobile malware infections pose a significant threat to mobile users, such as unauthorized access to personal information, financial loss due to fraudulent transactions, loss of privacy, device performance issues due to malware consuming system resources, and data theft or corruption. In the past, we observed similar banking trojan campaigns sending malicious links leading users to download malicious apps, as detailed in our blog Rewards plus: Fake mobile banking rewards apps lure users to install info-stealing RAT on Android devices.

8. Aberdeen University research warns of serious implications for misinformation and identity theft from facial AI (Grampian Online, 18 NOV, David Porter)

White faces generated by artificial intelligence (AI) now appear more real than human faces, according to new research from The Australian National University (ANU) and the University of Aberdeen.

In the study, more people thought AI-generated White faces were human than the faces of real people.

The same wasn't true for images of people of colour.

9. "We are getting very good at identifying a Russian campaign," Microsoft weighs in on disinformation and national security at recent events (Windows Central, 17 NOV, Jez Corden)

Back to Table of Contents

Russia is frequently accused of seeding disinformation as part of its hybrid warfare tactics. Microsoft has been at the fore of this new cyberwarfare front.

What you need to know

- Microsoft President Brad Smith and Microsoft CEO Satya Nadella recently shared some thoughts about Microsoft's place within the U.S. security apparatus.
- At an event in Paris, Smith detailed how Microsoft is using AI to help combat state-level disinformation campaigns.
- In comments to CNBC, CEO Satya Nadella outlined how Microsoft is shielding itself from China, in an increasingly restrictive U.S. tech trade regime.

10. BRI - Belt and Road Initiative - Highlights, 15 November 2023 (U.S. Army Asian Studies Detachment, 17 NOV)

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.

ASD is publishing BRI-related reports on PiX, the Protected Internet eXchange Portal, which can be viewed at the following URL: hxxps://pixtoday.net/article/article/220079.

11. **Addressing the State of AI's Impact on Cyber Disinformation/Misinformation (Security Week, 15 NOV, Rik Ferguson)**

By embracing a strategy that combines technological advancements with critical thinking skills, collaboration, and a culture of continuous learning, organizations can safeguard against AI's disruptive effects.

The recent rapid rise of artificial intelligence continues to be a game-changer in many positive ways, even though we are still touching the very fringes of its potential. New and previously unimaginable medical treatments, safer, cleaner and more integrated public transport, more rapid and accurate diagnoses, and environmental breakthroughs are all within the credible promise of AI today. Yet, within this revolution, a shadow looms.

Both China and Russia have made no secret of their desire to "win the AI race" with current and pledged investments ranging from hundreds of millions to billions of dollars in AI research and development. While companies like OpenAI, IBM and Apple might be top of mind when asked to name the major players in artificial intelligence, we should not forget that for every Amazon there's an Alibaba, for every Microsoft a Baidu, and for every Google a Yandex. It is inevitable that states, activists, and advanced threat actors will leverage the power of AI to turbocharge disinformation campaigns.

Back to Table of Contents

Signal

1. **[US Army developing intel analysis, combat weather apps] (Janes, 28 NOV, Carlo Munoz)**

   The US Army is developing a new slate of advanced software designed to improve collection, dissemination, and exploitation of battlefield intelligence at the tactical level, according to a service solicitation.

   The software development effort, known as the 'Intel Apps' programme, is being spearheaded by Project Manager, Intelligence Systems & Analytics (IS&A) under the army's Program Executive Office – Intelligence, Electronic Warfare & Sensors (PEO IEW&S) directorate. The programme, as designed, will "provide leap ahead [intelligence] tasking, collection, processing, exploitation and dissemination [of] advanced software capability" for army units, according to the 20 November request for proposals (RFP).

   Intel Apps, once mature, "will displace and replace" the service's current intelligence systems and analytics software embedded in the army's Command Post Computing Environment (CPCE), programme officials said in the RFP.

2. **[Huawei Eyes Connectivity Similar To SpaceX's Starlink After Maiden Satellite Test] (WCCF Tech, 26 NOV, Ramish Zafar)**

   Chinese personal computing and technology firm Huawei has become one of the few companies of its kind in the world to test out a low Earth orbit (LEO) satellite internet network similar to SpaceX's Starlink satellite internet service. Starlink is the world's largest LEO constellation, and it owes its size to SpaceX's workhorse Falcon 9 rocket, which has made rocket launches a regular occurrence of daily life in the 21st century. Details of Huawei's test were shared on the Chinese social media platform Weibo, with slides from a presentation showing that the LEO satellite test delivered download speeds of as much as 660 Mbps.

Back to Table of Contents

3. **[China Telecom Develops Network Cloud Infrastructure Platform Kit] (U.S. Army Asian Studies Detachment, 17 NOV)**

   This report highlights the selected products from the "Recommended Catalogue of Scientific and Technological Innovation Achievements of Central Enterprises (2022 Version)" published by the State-owned Assets Supervision and Administration Commission of the State Council (SASAC).

4. **[From PKI to PQC: Devising a strategy for the transition] (Help Net Security, 16 NOV, Zeljka Zorz)**

   Quantum computers capable of breaking currently used encryption algorithms are an inevitability. And since the US, China and Europe are sprinting to win that arms race, we know that day is coming sooner rather than later.

   Will organizations be ready to counter this threat to their data, though?

   The Ponemon Institute recently canvassed 1,426 IT and IT security practitioners knowledgeable about their organizations' approach to post-quantum cryptography, and found that 61% of them worry that their organization will not be ready to address the security implications of post-quantum computing.

5. **[Quantum Sensors vs. Quantum Computers: IDTechEx Takes a Look at the Next 10 Years] (PR Newswire, 16 NOV, IDTechEx)**

   Quantum technologies are evolving at a rapid pace. Spurred by the promise of exponentially faster computation and classically unachievable sensitivity, billions of dollars are being poured into the development of quantum computers and quantum

sensors. However, despite their shared use of quantum phenomena, including tunneling, entanglement, and superposition, each market's characteristics and ten-year outlook are quite distinct. Drawing on comprehensive reports covering both quantum technologies, IDTechEx separates hype from reality to compare the opportunities over the next decade.

6. Lockheed Martin to demonstrate space-based 5G network (Space News, 16 NOV, Sandra Erwin)

Lockheed Martin announced Nov. 16 it plans to launch a payload to orbit next year to demonstrate 5G connectivity from space. The experiment is part of a larger project, known as 5G.MIL, that the company started in 2020 in response to military demand for high-speed wireless communications.

By branching the latest cellular technology into space, the company ultimately hopes to forge what it calls an “all-domain network” — or a seamless communications web between space assets, aircraft, ships and ground forces.

7. US Calls Chinese ASAT Missiles ‘Biggest Threat’ To The Country; Says Poses ‘Double Trouble’ In Space (The EurAsian Times, 16 NOV, Sakshi Tiwari)

As the Space Force approaches its fourth birthday, Chief of Space Operations General Bradley Chance Saltzman identified one of its biggest threats – China’s anti-satellite (ASAT) missile capabilities.

During the Cold War, the US and the Soviet Union carried out many ASAT tests to ace the space race against one another. However, by 1980, these tests had been discontinued due to criticism that they generated excessive amounts of debris, endangering the lives of astronauts and important space assets.

Back to Table of Contents

China joined the elite league of countries with anti-satellite capabilities, as demonstrated in a test in 2007. It used a modified ballistic missile to destroy one of its weather satellites, resulting in the largest-ever space debris field with over 3,000 trackable pieces.

Items of Interest

1. **North Korea's First Satellite No Threat To US Navy, Pyongyang Knows It Has Long Way To Go: Experts (The EurAsian Times, 29 NOV, Parth Satam)**

   North Korea's first satellite launch and photographing of critical US, allied military, and civilian centers does give Pyongyang elementary space surveillance capabilities but does not significantly or decisively threaten the US Navy, experts believe.

   Pyongyang would instead need a host of other satellites and space launch capabilities to credibly shift the military balance in its favor and is far from being a space power.

   This does not mean the country's general military capabilities should be underestimated, especially given how it has introduced a series of new ballistic missiles, drones, cruise missiles, and submarines.

2. **Cartel Narco Tank With Cope Cage Anti-Drone Armor Emerges (The Drive/The Warzone, 28 NOV, Joseph Trevithick)**

   A drug cartel has adopted a major battlefield innovation in an attempt to help fend off growing drone attacks against its vehicles.

   AMexican drug cartel recently employed an improvised armored truck, also commonly referred to as a "Narco Tank," with what looks to be a metal screen over the front section of the vehicle. This is reminiscent of the so-called "cope cages" that have become a fixture on tanks and other armored vehicles on both sides of the conflict in Ukraine and that have also now emerged on Israeli tanks. These screens are primarily intended to provide extra protection against drones, something that cartels in Mexico are now regularly employing against government security forces and each other.

Back to Table of Contents

3. **Kim Jong Un reviews satellite photos of U.S. bases in Hawaii, South Korea: state media (Raw Story, 25 NOV, Agence France-Presse)**

   North Korean state media said Saturday that leader Kim Jong Un has reviewed images taken by his country's new spy satellite of "major target regions" including the US military base at Pearl Harbor, Hawaii and sites across South Korea.

   Pyongyang successfully put a military spy satellite into orbit earlier this week, but South Korea said it was too early to determine if the satellite was functioning as the North claims.

   Experts have said putting a working reconnaissance satellite into orbit would improve North Korea's intelligence-gathering capabilities, particularly over South Korea, and provide crucial data in any military conflict.

4. **China's J-11 Flanker-L 'Softens' US Air Force; US Resumes 'Mil-To-Mil' Contact With PLA To Deflate Tensions (The EurAsian Times, 25 NOV, Parth Satam)**

   The US Navy has welcomed the resumption of military coordination with the People's Liberation Army (PLA), its new top naval officer has announced. The 'military-to-military' (mil-to-mil) contacts, as they are known, come in the backdrop of increased encounters of its aircraft with Chinese fighter planes, which both sides were worried would veer into a war.

   The military dialogue was cut off following former US Speaker Nancy Pelosi's visit to Taiwan in August 2022. The mil-to-mil ties were restored following the November 16 meeting between Presidents Joe Biden and Xi Jinping in San Francisco.

5. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 22, 2023 (ISW, 22 NOV, Nils Peterson, Matthew Sperzel, and Daniel Shats)

The China–Taiwan Weekly Update focuses on the Chinese Communist Party's paths to controlling Taiwan and relevant cross–Taiwan Strait developments.

Key Takeaways

1) The Taiwan People's Party-Kuomintang (TPP-KMT) deal to form a joint presidential ticket broke down after the parties failed to reach a consensus on who would head the ticket. TPP candidate Ko Wen-je is signaling he is prepared to run as a solo candidate but left open the possibility of reaching a new deal by November 24.
2) The PRC Ministry of Foreign Affairs denied the validity of alternative regional security frameworks in response to the Philippines' calls to establish an ASEAN-led South China Sea code of conduct.
3) CCP General Secretary Xi Jinping called for convening a "more authoritative international peace conference" to promote a "just and lasting solution to the Palestinian issue" during a speech at a special BRICS leaders video summit on November 21.

6. North Korea claims it successfully put spy satellite into orbit (C4ISRNET, 21 NOV, Hyung-Jin Kim and Mari Yamaguchi)

Back to Table of Contents

North Korea claimed Wednesday to have successfully placed a spy satellite into orbit with its third launch attempt this year, demonstrating the nation's determination to build a space-based surveillance system during protracted tensions with the United States.

The North's claim could not immediately be independently confirmed. But the launch was certain to invite strong condemnation from the United States and its partners because the U.N. bans North Korea from conducting satellite launches, calling them covers for tests of missile technology.

The North's space authorities said in a statement that its space launch vehicle placed the Malligyong-1 satellite into orbit on Tuesday night following liftoff from the country's main launch center and an intended flight.

The statement said that leader Kim Jong Un observed the launch. It said the fired spy satellite would enhance North Korea's war readiness in response to its rivals' hostile military moves and that more would be launched at an early date.

7. US renews concerns over N. Korea-Russia military cooperation (The Korea Herald, 21 NOV, Yonhap)

The US Department of State reiterated its concerns Monday over military cooperation between North Korea and Russia, as Pyongyang is gearing up for a space rocket launch to put a military spy satellite into orbit.

Pyongyang has notified Japan's Coast Guard of a plan to conduct the launch between Nov. 22 and Dec. 1, Japanese media reported, despite Seoul's warning against what would be its third such launch attempt this year.

8. North Korea warns Japan of impending spy satellite launch (UPI, 21 NOV, Thomas Maresca)

North Korea notified Tokyo of its plans to launch a satellite as soon as Wednesday, Japan's Coast Guard said on Tuesday, marking the third attempt this year by the isolated

regime to place a military spy satellite into orbit.

The launch is scheduled for a window from Nov. 22 to Nov. 30, with the projectile expected to splash down in either the Yellow Sea or the East China Sea, the Coast Guard said.

9. Seoul warns North Korea not to launch spy satellite and hints 2018 military deal could be suspended (AP News, 20 NOV, Hyung-Jin Kim)

South Korea's military warned North Korea not to go ahead with its planned spy satellite launch, suggesting Monday that Seoul could suspend an inter-Korean agreement to reduce tensions and resume front-line aerial surveillance in response.

North Korea failed in its first two attempts to put a military spy satellite into orbit earlier this year and didn't follow through with a vow to make a third attempt in October. South Korean officials said the delay was likely because North Korea is receiving Russian technology assistance and that a launch could happen in coming days.

10. Aging Population & Low Birth Rate, China Struggles To Fill PLA Ranks; To Become Aged Society In 25 Years (The EurAsian Times, 20 NOV, Lt Gen. PR Shankar (Retired))

It is now well-established that China's declining demography is a cause for concern. I was, therefore, reading up on the subject when I came across the graph below, which indicates China's population aged over 65.

It caught my attention since it resembled a typical run rate graph in limited overs cricket, where the scoring rates in the slog overs become steep. The thought that came to my mind is that China seems to have entered the slog-overs in its demographic decline.

Back to Table of Contents

The usual thinking is that China, with its 'great leaps' in technology, military, and economy under the able leadership of Xi Jinping and his hyper-enthusiastic band of Communist apparatchiks will tackle the problem with their customary efficiency and zeal to march onward to a Tianxia.

However, they will not, simply because they cannot. They might be heading into something they or the world have not bargained for. Let me try to forecast it by deciphering the figures.

11. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 17, 2023 (ISW, 17 NOV, Nils Peterson, Matthew Sperzel, and Daniel Shats)

The China–Taiwan Weekly Update focuses on the Chinese Communist Party's paths to controlling Taiwan and relevant cross–Taiwan Strait developments.

Key Takeaways

1. The Chinese Communist Party (CCP) is expanding its suppression of dissents by targeting overseas Chinese expatriate critics.
2. Cambodia, Laos, and Vietnam will participate in the Aman Youyi 2023 military exercise with People's Liberation Army forces for the first time, which buttresses CCP efforts to construct a Sino-centric regional security order.
3. US President Joe Biden and PRC President Xi Jinping announced the resumption of US-PRC military-to-military talks and cooperation to combat illegal fentanyl production after their meeting in San Francisco.
4. The Taiwan People's Party (TPP) and Kuomintang (KMT) overcame the biggest hurdle to forming a joint presidential ticket on November 15 and plan to announce the ticket order on November 18.
5. The PRC continued using the Israel-Hamas War to bolster its image as a fair,

responsible broker in contrast to the "biased" United States while framing Israel as the driver of the war. The PRC has also expanded its diplomatic outreach in the Middle East while building its image as an important and fair broker in the region.

12. China Wants 'Nuclear Parity' With US; Could Achieve The Scary Milestone By Mid-2030s – Congressional Panel (The EurAsian Times, 17 NOV, Ashish Dangwal)

In a startling revelation, a Congressional Commission disclosed that China is rapidly advancing towards achieving nuclear parity with the United States and Russia, with a target set for the mid-2030s.

The Pentagon has been closely monitoring China's nuclear activities, and officials have regularly voiced their concerns about the lack of transparency surrounding the extent of China's nuclear arsenal.

On November 15, the Commission on the Strategic Posture of the United States told US lawmakers that the magnitude and pace of China's nuclear weapons buildup is 'unprecedented' and 'very surprising.'

At present, the US and Russia are believed to have around 5500-6000 nuclear weapons with about 1600 active deployed strategic nuclear warheads, according to estimates by the Federation of American Scientists.

13. Taiwan's Civilian Simulation of a Chinese Military Invasion Exposes Weaknesses in Basic Infrastructure (U.S. Army Asian Studies Detachment, 17 NOV)

Back to Table of Contents

On 30 October 2023, the Taiwan Center for Security Studies at a Taiwan University held a military simulation, which hypothesizes a China invasion scenario in 2027. The scenario showed a potential blind spot on Taiwan's semiconductor industry, vulnerabilities to a coal blockade, inability to cope with casualties, and potential issues of receiving military aid in the ongoing war. A former Taiwan Navy Admiral and Vice Minister of Defense said many Western simulations use outdated data, particularly in the amphibious landing potential of Taiwan's beaches

.

Israel-Hamas Conflict

1. The Drive/The Warzone Israel-Gaza Update

Israel-Gaza Situation Report: Bloodshed In Jerusalem Doesn't Stop Ceasefire – 30 NOV

Israel-Gaza Situation Report: Ceasefire Holds Despite Skirmish – 28 NOV

Israel-Gaza Situation Report: Ceasefire Extended 48 Hours, More Hostages Freed – 27 NOV

Israel-Gaza Situation Report: First Hostages Released After Ceasefire Begins - 24 NOV

Israel-Gaza Situation Report: Deal Reached For Four Day Ceasefire – 22 NOV

Israel-Gaza Situation Report: Deal To Release Hostages "Closer Than Ever" – 20 NOV

Israel-Gaza Situation Report: Ground Offensive Could Shift South – 17 NOV

2. Institute for The Study of War Iran Update:

The Iran Update provides insights into Iranian and Iranian-sponsored activities abroad that undermine regional stability and threaten US forces and interests. It also covers events and trends that affect the stability and decision-making of the Iranian regime.

Back to Table of Contents

Iran Update, November 30, 2023

Iran Update, November 29, 2023

Iran Update, November 28, 2023

Iran Update, November 27, 2023

Iran Update, November 26, 2023

Iran Update, November 25, 2023

Iran Update, November 24, 2023

Iran Update, November 22, 2023

Iran Update, November 21, 2023

Iran Update, November 20, 2023

Iran Update, November 19, 2023

Iran Update, November 18, 2023

Iran Update, November 17, 2023

Iran Update, November 16, 2023

3. Truce in Israel-Hamas war extended by a day, minutes before it was set to expire (AP News, 27 NOV, Wafaa Shurafa et al.)

Israel and Hamas on 30NOV2023 agreed to extend a temporary truce by another day minutes before it was set to expire, said Qatar, which has been mediating between the two sides.

Negotiations on extending it came down to the wire, with last-minute disagreements over the hostages to be freed by Hamas in exchange for another day of a halt in fighting.

Word of the extension came just as the truce was to expire at 7 a.m. (0500 GMT) 30NOV2023. The Qatari Foreign Ministry said the truce was being extended under the same terms as in the past, under which Hamas has released 10 Israeli hostages per day in exchange for the release of 30 Palestinian prisoners.

The announcement followed a last-minute standoff earlier Thursday, with Hamas saying Israel had rejected a proposed list that included seven living captives and the remains of three who the group said were killed in previous Israeli airstrikes. Israel later said Hamas submitted an improved list, paving the way for the extension.

4. Shadowy hacking group targeting Israel shows outsized capabilities (CyberScoop, 27 NOV, AJ Vicens)

A hacking campaign displaying what researchers say is some of the most advanced publicly known tradecraft targeting Israel in recent years is showing signs of active development and evolution, a troubling development that has so far blended into the noise of near constant cyber operations targeting Israel.

There's been no shortage of cyberattacks of varying severity targeting Israeli institutions, particularly in the wake of Hamas' Oct. 7 attack, but the tradecraft and capabilities displayed by the so-far unattributed group is far more sophisticated, said Nicole Fishbein, a researcher with Intezer.

Dubbed "WildCard," the group in question appears to be linked to a nearly year-long attack targeting the Israel Electric Corporation, which is Israel's largest electrical supplier, between April 2016 and February 2017 that researchers at the time called "Electric Powder."

Following Hamas's Oct. 7 attack on Israel and amid the subsequent fighting, hacking groups have targeted with Israel with a variety of operations, but these have consisted mostly of distributed denial-of-service attacks, the posting of hacked data, and improvised claims of exaggerated access to water treatment facilities and other critical infrastructure from some Iranian-backed cyber groups, experts have said.

Back to Table of Contents

5. Israel-Hamas war live: Hamas says 'truce agreement' is close (DW, 21 NOV)

The Hamas militant group is negotiating via Qatari mediators on a temporary truce, while the US has said a hostage deal could be close. Meanwhile, Israel has said around 10,000 of its troops are in Gaza. DW has more.

6. Jordan doubts Israel can destroy Hamas as Gaza war rages (Reuters, 18 NOV, Alexander Cornwell and Andrew Gray)

Jordan's foreign minister voiced doubt on Saturday that Israel could reach its goal of obliterating Hamas with its heavy bombardment and invasion of the Gaza Strip long dominated by the Palestinian Islamist movement.

"Israel says it wants to wipe out Hamas. There's a lot of military people here, I just don't understand how this objective can be realised," Ayman Safadi said at the annual IISS Manama Dialogue security conference in Bahrain.

Russia-Ukraine Conflict

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

Russia-Ukraine Situation Report, 30 November 2023
Russia-Ukraine Situation Report, 29 November 2023
Russia-Ukraine Situation Report, 28 November 2023
Russia-Ukraine Situation Report, 27 November 2023
Russia-Ukraine Situation Report, 22 November 2023
Russia-Ukraine Situation Report, 21 November 2023
Russia-Ukraine Situation Report, 20 November 2023
Russia-Ukraine Situation Report, 17 November 2023
Russia-Ukraine Situation Report, 16 November 2023

2. The Drive/The Warzone Ukraine Situation Report:

Ukraine Situation Report: Storms Held Up Russian Assault On Avdiivka – 29 NOV
Ukraine Situation Report: Huge Storm's Impact On Russian Defenses – 27 NOV
Ukraine Situation Report: Soldier Describes "Zombie" Warfare In Avdiivka – 24 NOV
Ukraine Situation Report: New Ground-Based Air Defense Coalition Announced – 22 NOV
Ukraine Situation Report: The Muddy Season Has Arrived – 20 NOV
Ukraine Situation Report: First Person Video Drone Relentlessly Hunts Down A Russian Van – 16 NOV

Back to Table of Contents

3. Institute for The Study of War

Russian Offensive Campaign Assessment, November 30, 2023
Russian Offensive Campaign Assessment, November 29, 2023
Russian Offensive Campaign Assessment, November 28, 2023
Russian Offensive Campaign Assessment, November 27, 2023
Russian Offensive Campaign Assessment, November 26, 2023
Russian Offensive Campaign Assessment, November 25, 2023
Russian Offensive Campaign Assessment, November 24, 2023
Russian Offensive Campaign Assessment, November 22, 2023
Russian Offensive Campaign Assessment, November 21, 2023
Russian Offensive Campaign Assessment, November 20, 2023
Russian Offensive Campaign Assessment, November 19, 2023
Russian Offensive Campaign Assessment, November 18, 2023
Russian Offensive Campaign Assessment, November 17, 2023
Russian Offensive Campaign Assessment, November 16, 2023

4. Shahed-136 With Cellular Modem Found In Ukraine: What It Means (The Drive/The War Zone, 30 NOV, Howard Altman & Tyler Rogoway)

Here are the possibilities of what the addition of improvised cellular communications to Russia's Shahed drones means.

The largest single attack against Ukraine by Russian Shahed-136 type drones last week led to an unusual discovery. Technicians from a Ukrainian drone training and

development company said they found a 4G modem with a SIM card from the Ukrainian Kyivstar telecom firm inside some of the downed drones. This could have implications of varying degrees of impact.

The Victory Drone company initially suggested on Telegram that the SIM card and modem could be used by Russia to track the remains of down drones, gain additional navigation via cell phones or telemetry "to adjust the flight mission in real-time."

5. Putin won't make peace in Ukraine before 2024 US election (Reuters, 29 NOV, Humeyra Pamuk and Simon Lewis)

Russian President Vladimir Putin will not make peace in Ukraine before he knows the results of the November 2024 U.S. election, a senior U.S. State Department official said on Tuesday, amid concerns that a potential victory for former President Donald Trump could upend Western support for Kyiv.

Trump, who is seeking reelection in 2024 and is the leading candidate for the Republican presidential nomination, has been sharply critical of U.S. support for Kyiv.

A senior official briefing reporters after a meeting of NATO foreign ministers in Brussels said the alliance reiterated its support for Ukraine knowing that a peace agreement in the next year is unlikely.

Asked whether they were expressing a personal opinion or the view of the U.S. government, the official said it was a "widely shared premise."

A Reuters/Ipsos poll conducted in mid-November showed Trump and U.S. President Joe Biden locked in a tight race, with Trump leading Biden 51% to 49% when respondents were asked to pick between the two. That result was within the poll's credibility interval of about four percentage points.

Back to Table of Contents

6. Russia launches largest drone attack since start of Ukraine invasion (C4ISRNET, 25 NOV, Associated Press)

Russia on Saturday launched its most intense drone attack on Ukraine since the beginning of its full-scale invasion in 2022, targeting the capital city for over six hours, military officials said.

"Kyiv was the main target," Ukrainian Air Force Commander Mykola Oleshchuk wrote on his Telegram channel.

In total, Russia launched 75 Iranian-made Shahed drones against Ukraine, of which 74 were destroyed by air defenses, Ukraine's air force said.

The attack was "the most massive air attack by drones on Kyiv," said Serhii Popko, head of the Kyiv city administration. Ukrainian air force spokesman Yurii Ihnat confirmed later that the air defenses shot down 66 air targets over the capital and surrounding region throughout the morning.

At least five civilians were wounded in the hours-long assault, which saw several buildings damaged by falling debris from downed drones, including a kindergarten. The wounded included an 11-year-old child, according to Kyiv mayor Vitali Klitschko.

7. Germany to supply Ukraine with IRIS-T systems in $1.4 billion package (C4ISRNET, 24 NOV, Rudy Ruitenberg)

Germany will provide Ukraine with an additional four IRIS-T SLM medium-range air defense systems as part of a military aid package worth more than €1.3 billion ($1.4 billion), the German Defence Ministry said in a statement Thursday. The systems will be supplied from 2025.

The package also includes drones and drone-defense systems, demining vehicles, satellite communications, electronic warfare equipment, directional anti-tank mines and artillery shells, aimed at addressing acute needs of the Ukrainian armed forces, according to the ministry.

Germany has become the biggest supplier of military aid to Ukraine behind the U.S., after initial reluctance to provide arms. German Defence Minister Boris Pistorius earlier this month confirmed plans to boost the country's military support for Ukraine, in response to media reports the government is seeking to double the aid to €8 billion in 2024.

IRIS-T systems and a second Patriot tracking radar handed over in October will reach Ukraine this year, once Ukrainian personnel have completed their training, the ministry said.

8. Ukraine conflict: Ukrainian air defense employs passive sensors for detection and tracking (Janes, 24 NOV, Christopher Petrov)

Representatives from Skyfortress – a Ukrainian non-governmental organisation – have disclosed details of work to develop and install an acoustic sensor network for the detection and tracking of aerial threats.

Speaking at SAE Media Group's Air and Missile Defence conference in London, the representatives said the Skyfortress detection and tracking system combines cheap and domestically designed passive sensors to detect, track, and classify airborne threats. It consists of an array of acoustic sensors that gather information and feed this into Ukraine's national air-defence command-and-control network, known as 'Virazh'..

Back to Table of Contents

9. Soviet-Era M-55 Spy Plane May Be Headed To Support The War In Ukraine (The Drive/The Warzone, 21 NOV, Thomas Newdick)

Developed in Soviet times as a high-altitude surveillance aircraft, the M-55 Mystic-B recently appeared carrying a signals intelligence pod.

Russia is likely considering returning to service its Cold War-era M-55 high-altitude spy plane, to provide additional intelligence-gathering capabilities over the battlefields of Ukraine. This is the recent assessment of the U.K. Ministry of Defense, and it follows the appearance of photos showing the rarely-seen aircraft at a Russian test facility, fitted with an electronic intelligence (ELINT) payload.

In one of its regular intelligence updates, the U.K. Ministry of Defense assesses that Russia is "likely considering bringing the Soviet-era M-55 Mystic-B high-altitude reconnaissance aircraft back into service." In fact, the M-55 never made it into operational military service with the Soviet Union or Russia, with only four examples being flown. The last of these to remain active was more recently used for civilian research of the stratosphere and the Earth's surface, under the name Geofizika.

10. The World's Attention is on Gaza, and Ukrainians Worry War Fatigue Will Hurt Their Cause (Military.com, 18 NOV, Hanna Arhirova)

When Tymofii Postoiuk and his friends set up an online fundraising effort for Ukraine, donations poured in from around the globe, helping to purchase essential equipment for Ukrainian armed forces.

As the fighting with Russia wore on and war fatigue set in, the donations slowed down, but money continued to come in steadily. Then the Israel-Hamas war broke out on Oct. 7.

11. China is the main supplier of dual-use goods needed to run Russia's military machine (Intellinews, 16 NOV, Ben Aris)

Last month, Russian President Vladimir Putin visited Beijing to meet with his Chinese counterpart, Xi Jinping, as Ukraine's counteroffensive against Russian invaders stalled. Beijing has been a mainstay of support for Russia and while Xi has been very careful not to cross the red line of supplying the Kremlin with lethal aid, the torrent of machines, equipment, and manufactured goods crossing the border into Russia has been vital for the Russian military machine.

Open-source trade data indicates a surge in imports of Chinese-manufactured goods with crucial military applications. This material has played a significant role in Russia's ability to fortify its positions on Ukrainian soil and maintain its military's equipment and supplies for resisting counteroffensives, the Atlantic Council said in a report.

Back to Table of Contents