U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

01 - 15 December 2023

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

Table of Contents

Items of Interest

1. CHINA-TAIWAN WEEKLY UPDATE, DECEMBER 15, 2023 – 15 DEC
2. NATO Fighters Scrambled As Russian Drone Violates Romanian Airspace – 14 DEC
3. 15 Air National Guardsmen disciplined in Discord server leak – 11 DEC
4. Iraq scrambles to contain fighting between US troops and Iran-backed groups, fearing Gaza spillover – 11 DEC
5. Taiwanese Pilot Planned CH-47 Defection To China: Reports – 11 DEC
6. Resisting China's Gray Zone Military Pressure on Taiwan – 07 DEC
7. Rocket Launcher Disguised As Fuel Truck Seen Firing In Iraq – 05 DEC

Israel-Hamas Conflict

1. The Drive Israel-Gaza Update
2. Institute for The Study of War Iran Update:
3. Guided Parachute System Used By Israel For First Time In Gaza – 11 DEC
4. THE ORDER OF BATTLE OF HAMAS' IZZ AL DIN AL QASSEM BRIGADES, PART 1: NORTH AND CENTRAL GAZA – 08 DEC
5. Feds: Iran-linked hacking campaign a 'clarion call' for digital defenses – 04 DEC

Russia-Ukraine Conflict

1. Russia-Ukraine Situation Report
2. The Drive/The Warzone Ukraine Situation Report:
3. Institute for The Study of War
4. THE HIGH PRICE OF LOSING UKRAINE – 14 DEC
5. Ukraine's innovative edge counters Russian mass, official says – 14 DEC
6. Drones, jammers in Ukraine signal new era of warfare, Del Toro says – 12 DEC
7. Cyberattack Cripples Ukraine's Largest Telecom Operator – 12 DEC
8. Russia Installs "Emotional Support Cages" Over Its Trenches To Defend Itself From Ukraine's Kamikaze UAVs – 12 DEC

Cyber

1. **Microsoft seizes infrastructure of top cybercrime group (CyberScoop, 12 DEC, AJ Vicens)**

Microsoft took sweeping action against a cybercrime operation responsible for creating roughly 750 million fraudulent Microsoft accounts and various websites used to enable a bevy of cybercrime activities, the company said Wednesday.

The announcement comes nearly a week after Microsoft obtained a court order from the Southern District of New York allowing it to seize U.S.-based infrastructure and websites used by a group the company tracks as Storm-1152. The group is one of several that "enable scores of cybercriminals to carry out their malicious activities more efficiently and effectively," Amy Hogan-Burney, Microsoft's associate general counsel for cybersecurity policy and protection, wrote in a blog post on the company's website.

The group "plays a significant role in the highly specialized cybercrime-as-a-service ecosystem," Hogan-Burney wrote, offering fraudulent Microsoft accounts as well as services to bypass CAPTCHA puzzles, which are designed to reduce inauthentic, spammy behavior by forcing a human to answer questions or solve puzzles to access certain web services. Microsoft described the group as "the number one seller and creator of fraudulent Microsoft accounts."

The investigation also identified several individuals based in Vietnam that Microsoft said were instrumental in developing and maintaining the websites associated with the activity, producing step-by-step videos explaining how to use their products to exploit fraudulent Microsoft accounts and even providing chat services to customers.

Back to Table of Contents

2. **Sandman Cyberespionage Group Linked to China (SecurityWeek, 12 DEC, Ionut Arghire)**

The recently outed advanced persistent threat (APT) actor Sandman appears linked to China, SentinelOne, Microsoft, and PwC say in a joint report.

The hacking group was brought into the spotlight at the LABScon security conference, standing out because of the sophisticated modular backdoor LuaDream, which has been built using the cross-platform programming language Lua.

Initial reporting drew attention to Sandman's targeting of telecom providers in the Middle East, Europe, and South Asia, likely for cyberespionage purposes, but did not link the activity to any known APTs.

The joint report, however, draws links between the observed Sandman APT attacks and the activity of STORM-0866/Red Dev 40, a suspected China-based threat actor known to be using the KeyPlug backdoor.

3. **North Korean Hackers Developing Malware in Dlang Programming Language (SecurityWeek, 11 DEC, Ionut Arghire)**

The North Korea-linked hacking group Lazarus has been observed deploying Dlang malware in attacks against organizations in the manufacturing, agriculture, and physical security sectors, Cisco's Talos security researchers report.

Released in 2001, Dlang, or simply D, is a multi-paradigm system programming language built upon the idea of C++, but drawing inspiration from C#, Eiffel, Java, Python, Ruby, and other high-level languages as well.

Dlang is considered an uncommon programming language for malware development, but has started attracting malware developers, likely due to its versatility and easy

learning curve. Dlang allows developers to cross-compile applications for multiple architectures.

Since March 2023, Lazarus, an advanced persistent threat (APT) actor sponsored by the North Korean government, has been observed using three malware families built using Dlang, namely the NineRAT and DLRAT remote access trojans (RATs), and the BottomLoader downloader.

4. **Alleged Chinese cyberattacks target US power and water systems (Silicon Angle, 11 DEC, Duncan Riley)**

U.S. government officers and cybersecurity experts are warning that the Chinese military is allegedly attempting to infiltrate critical infrastructure, including power and water utilities and transportation systems in the U.S.

The Washington Post reported, referencing unnamed officials and security experts, that hackers allegedly affiliated with China's People's Liberation Army have burrowed into the computer systems of about two dozen critical entities over the past year. The intrusions are said to be part of broader efforts to develop ways to sow panic, create chaos and snarl logistics in the event that war breaks out between the U.S. and China.

5. **11TH DECEMBER – THREAT INTELLIGENCE REPORT (Check Point, 11 DEC)**

For the latest discoveries in cyber research for the week of 11th December, please download our Threat Intelligence Bulletin

Back to Table of Contents

6. **U.S., SOUTH KOREA, AND JAPAN JOIN FORCES TO TACKLE NORTH KOREA'S LAZARUS GROUP CRYPTO HACKERS (Cryptopolitan, 09 DEC, Florence Muchai)**

In a significant development, the United States, South Korea, and Japan have taken a decisive step towards collaborative cybersecurity efforts to tackle the persistent threat North Korea's Lazarus Group crypto hackers pose.

The emergence of North Korea as a key player in the realm of cyber warfare has raised alarms among nations striving to protect their digital infrastructure. With a track record of sophisticated cyber-attacks and increasing reliance on cryptocurrency to circumvent international sanctions, North Korea's cyber capabilities have become a focal point for security concerns.

7. **10 Of The Most Advanced Cyber Warfare Tools (Slash Gear, 07 DEC, Aaron Greenbaum)**

Militaries have fielded countless deadly weapons, ranging from muskets to tanks, and recently nations have leveraged the power of the internet in what is colloquially known as cyber warfare. Armies can now wage information wars by hacking into private servers and stealing information, spying on hijacked devices, and directly destroying federal property — everything Bond-era spies did, but executed remotely.

8. **UK says Russia behind cyber espionage aimed at undermining democracy (AP News, 07 DEC, Sylvia Hua)**

Russia's intelligence services have targeted high-profile British politicians, civil servants and journalists with cyberespionage as part of years-long attempts to interfere in U.K. politics, Britain's government said Thursday.

The Foreign Office said Russia's FSB agency was responsible for a range of sustained cyberespionage operations in the U.K., including targeting British lawmakers from multiple parties from at least 2015 through to this year and selectively leaking and

amplifying sensitive information to serve Russian interests.

9. Star Blizzard increases sophistication and evasion in ongoing attacks (Microsoft, 07 DEC, Microsoft Threat intelligence)

Microsoft Threat Intelligence continues to track and disrupt malicious activity attributed to a Russian state-sponsored actor we track as Star Blizzard (formerly SEABORGIUM, also known as COLDRIVER and Callisto Group). Star Blizzard has improved their detection evasion capabilities since 2022 while remaining focused on email credential theft against the same targets. Star Blizzard, whose activities we assess to have historically supported both espionage and cyber influence objectives, continues to prolifically target individuals and organizations involved in international affairs, defense, and logistics support to Ukraine, as well as academia, information security companies, and other entities aligning with Russian state interests. Microsoft continues to refine and deploy protections against Star Blizzard's evolving spear-phishing tactics.

Microsoft is grateful for the collaboration on investigating Star Blizzard compromises with the international cybersecurity community, including our partners at the UK National Cyber Security Centre, the US National Security Agency Cybersecurity Collaboration Center, and the US Federal Bureau of Investigation.

Back to Table of Contents

10. 4TH DECEMBER – THREAT INTELLIGENCE REPORT (Check Point, 04 DEC)

For the latest discoveries in cyber research for the week of 4th December, please download our Threat Intelligence Bulletin.

11. Cybercriminals are exploiting AI tools like ChatGPT to craft more convincing phishing attacks, alarming cybersecurity experts (Tech Radar, 01 DEC, Kristina Terech)

If you've noticed a spike in suspicious-looking emails in the last year or so, it might be partly due to one of our favorite AI chatbots - ChatGPT. I know - plenty of us have had intimate and private conversations where we've learned about ourselves with ChatGPT, and we don't want to believe ChatGPT would help scam us.

According to cybersecurity firm SlashNext, ChatGPT and its AI cohorts are being used to pump out phishing emails at an accelerated rate. The report is founded on the firm's threat expertise and surveyed more than three hundred cybersecurity professionals in North America. Namely, it's claimed that malicious phishing emails have increased by 1,265% - specifically credential phishing, which rose by 967% - since the fourth quarter of 2022. Credential phishing targets your personal information like usernames, IDs, passwords, or personal pins by impersonating a trusted person, group, or organization through emails or a similar communication channel.

Electronic Warfare

1. **[Czech Republic receives new electronic surveillance system](#) (Janes, 15 DEC, Olivia Savage)**

   The Army of the Czech Republic (ACR) has received the first of two new deployable passive electronic surveillance systems following an official handover ceremony to the 532nd Electronic Warfare Battalion on 13 December.

   The system, known as the Deployable Passive Electronic Support Measures Tracker (DPET), is replacing the in-service Vera-S/M, although it will remain in the armament of the army and be used for training and use by Active Reserve units, according to an announcement by the Armed Forces of the Czech Republic.

   The DPET will be in service over the next 10–15 years following delivery of the second and final system in 2024

2. **[Drones, jammers in Ukraine signal new era of warfare, Del Toro says](#) (C4ISRNet, 12 DEC, Colin Demarest)**

   Russia's invasion of Ukraine, now nearing the end of its second year, has ushered in a "new era of war" in which drones and electronic warfare are having outsize impacts, the secretary of the U.S. Navy said.

   Both Russian and Ukrainian militaries are employing unmanned aerial systems to scout, target and attack while simultaneously using jammers and spoofers to defend the skies above or the trenches they've dug. The cat-and-mouse game is deadly, with each side trying to outthink and outbuild the other.

[Back to Table of Contents](#)

3. **[How China is challenging the U.S. military's dominance in space](#) (NBC News, 12 DEC, Courtney Kube & Dan De Luce)**

   China's rapidly growing arsenal of anti-satellite weapons could cripple America's military in a crisis and the U.S. is scrambling to shore up its defenses miles above the Earth.

   China is testing and developing an array of weapons and tools that could destroy, disable or hijack satellites that the U.S. military heavily relies on to operate around the world, Defense Department officials and experts say.

   In recent years, China has rapidly closed the gap with the U.S. in space. Beijing is ramping up the pace of its satellite launches and mastering capabilities that only the United States had a decade ago, experts say.

4. **[Global conflicts spur a 'race' to develop, field electronic warfare systems: Navy secretary](#) (Breaking Defense, 12 Dec, Justin Katz)**

   "It is imperative that we, in concert with our allies and partners, remain committed to prioritizing our warfighters' freedom of action and ability to achieve spectrum superiority," Navy Secretary Carlos Del Toro said, citing the prominence of EW capabilities in Ukraine and the Middle East.

   Navy Secretary Carlos Del Toro today said the conflicts in Ukraine and elsewhere have sparked a "race" to more rapidly develop and field electronic warfare capabilities, warning it is an "imperative" for the US to keep pace with its adversaries.

5. **[EDEX 2023: China displays new JN1199 High Power Communication](#)**

Electronic Warfare System (Army Recognition, 05 DEC)

At EDEX 2023, the editorial team of Army Recognition had the opportunity to examine the JN1199 High Power Communication Electronic Warfare System. This system, emerging from the Chinese electronics industry, represents a significant advancement in air defense operations.

6. Ukraine makes new push to defeat Russia's electronic warfare (CNN, 29 NOV, Clare Sebastian)

In early November, drone video surfaced online appearing to show a targeted strike blowing up three antennas on the roof of an apartment block. The Ukrainian drone commander who posted it claimed to have destroyed a Russian Pole-21 electronic warfare system on the eastern front near Donetsk.

Ukraine is already racing to catch up with Russia when it comes to electronic warfare.

This attack also shows how Kyiv is rushing to destroy Moscow's technology on the battlefield – a sign of how important it may be for the future of the war.

Back to Table of Contents

Information Advantage

1. **[AI threats pose great cyber risks to smaller companies, experts tell House panel] (CyberScoop, 12 DEC, Christian Vasquez)**

Attacks by malicious hackers using artificial intelligence could swamp smaller companies that are already overwhelmed by cybercrime, experts warned lawmakers during a congressional hearing Tuesday.

Testifying before the House Homeland Security and Governmental Affairs subcommittee on cybersecurity and infrastructure protection, experts from the private sector discussed AI-related threats, including increased efficiency for malicious hackers to develop malware, spread disinformation and elevate the scale of attacks at a time when smaller businesses are constantly being impacted by hacks.

Bringing up the famous and complex Stuxnet virus that took down the Iranian nuclear plant, Alex Stamos, chief trust officer at SentinelOne, said that developing the worm required a substantial number of resources. With AI, Stamos warned, such operations could become less costly for attackers.

Stamos said that one key thing that the Cybersecurity Infrastructure and Security Agency can do is get an incident reporting regime up and running. The agency is set to require critical infrastructure owners and operators to notify them of any major cyber incident.

2. **Europe Reaches a Deal on the World's First Comprehensive AI Rules (DefenseScoop, 09 DEC, Associated Press)**

Back to Table of Contents

European Union negotiators clinched a deal Friday on the world's first comprehensive artificial intelligence rules, paving the way for legal oversight of AI technology that has promised to transform everyday life and spurred warnings of existential dangers to humanity.

Negotiators from the European Parliament and the bloc's 27 member countries overcame big differences on controversial points including generative AI and police use of face recognition surveillance to sign a tentative political agreement for the Artificial Intelligence Act.

The result came after marathon closed-door talks this week, with the initial session lasting 22 hours before a second round kicked off Friday morning.

Officials were under the gun to secure a political victory for the flagship legislation. Civil society groups, however, gave it a cool reception as they wait for technical details that will need to be ironed out in the coming weeks. They said the deal didn't go far enough in protecting people from harm caused by AI systems.

3. **Foreign Reflections on U.S. Exercises and Operations, 08 December 2023 (U.S. Army Asian Studies Detachment, 08 DEC)**

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, Russia, North Korea, Japan, and India.

4. **Russian influence and cyber operations adapt for long haul and**

exploit war fatigue (Microsoft, 07 DEC, Clint Watts)

Since July 2023, Russia-aligned influence actors have tricked celebrities into providing video messages that were then used in pro-Russian propaganda. These videos were then manipulated to falsely paint Ukrainian President Volodymyr Zelensky as a drug addict. This is one of the insights in the latest biannual report on Russian digital threats from the Microsoft Threat Analysis Center: "Russian Threat Actors Dig In, Prepare to Seize on War Fatigue"

As described in more detail in the report, this campaign aligns with the Russian government's broader strategic efforts during the period from March to October 2023, across cyber and influence operations (IO), to stall Ukrainian military advances and diminish support for Kyiv.

5. South Korea's S2W Promotes Dark Web Data Collection, Analysis Tool at Security Equipment Exhibition (U.S. Army Asian Studies Detachment, 06 DEC)

South Korea's S2W promoted its products at one of the largest comprehensive risk management tradeshows in Japan, RISCON TOKYO (Security & Safety Trade Expo) 2023, held in Tokyo, from 11 to 13 October 2023. The exhibition is a platform that markets advanced products and services focusing on disaster risk reduction, business risk management, and security. The event draws 300 exhibitors, mostly domestic ones but several from United States, Singapore, South Korea, and China.

6. BRI – Belt and Road Initiative – Highlights, 1 December 2023 (U.S. Army Asian Studies Detachment, 06 DEC)

Back to Table of Contents

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.

7. Foreign Reflections on U.S. Exercises and Operations, 1 December 2023 (U.S. Army Asian Studies Detachment, 01 DEC)

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, Russia, North Korea, South Korea, Japan and the Philippines.

8. BRI - Belt and Road Initiative - Highlights, 1 December 2023 (U.S. Army Asian Studies Detachment, 01 DEC)

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.

Back to Table of Contents

Signal

1. **[US, China Out to Stop Quantum Computers Stealing World's Secrets] (Asian Financial, 14 DEC)**

   One expert has predicted quantum computers might be capable of cracking the encryption that protects most digital communications by 2025

   US and Chinese security chiefs are in a desperate race to protect their secrets from quantum computers which, it's predicted, could render current encryption methods useless in just two years time.

   In February, a Canadian cybersecurity firm delivered an ominous forecast to the US Department of Defense. Everyone's secrets are now at risk of exposure, warned the team from Quantum Defen5e (QD5).

2. **[SpaceX's Starlink Ready to Boost Arctic Military Communications Says US Air Force] (High North News, 11 DEC, Malte Humpert)**

   Starlink satellites could soon be used to provide space-based communication for the US military across the Arctic following a successful test program. But outsourcing communication needs to a private entity also entails risks, as Starlink's role in the Ukraine War has shown.

   Following the expansion of SpaceX's network of satellites into Arctic latitudes in 2022 and 2023 the system is now deemed ready and reliable for military use. Following a nine-months test program, which ended in June, the US Air Force concluded that the system worked well in the region's harsh environmental conditions.

Back to Table of Contents

   The U.S. military, including the U.S. Coast Guard, have long-expressed concern about unreliable communications in the polar regions. The Arctic lacks many of the traditional land-based communication and satellite-based connections typically found in other parts of the world.

3. **[Navigating The Quantum Era: The Shift To Quantum-Safe Cryptography] (Forbes, 07 DEC, Suman Sharma)**

   As the quantum computing revolution approaches, it presents a formidable challenge to the cryptographic foundation of digital security. This article delves into the vulnerabilities of existing cryptographic algorithms to quantum attacks, examines the resilience of symmetric cryptography and introduces the concept of quantum-safe cryptography—an essential area of knowledge for engineers and technologists preparing for a quantum-secure future.

4. **[Protecting credentials against social engineering: Cyberattack Series] (Microsoft, 04 DEC, Microsoft Incident Response)**

   Our story begins with a customer whose help desk unwittingly assisted a threat actor posing as a credentialed employee. In this fourth report in our ongoing Cyberattack Series, we look at the steps taken to discover, understand, and respond to a credential phishing and smishing (text-based phishing) cyberattack that targeted a legitimate, highly-privileged user with social engineering—allowing the cyberattacker to impersonate the victim and weaponize a help desk to remove their multifactor authenticated device and register their own.

5. **[Signal rejects "dangerously misleading" security flaw allegations] (Tech Radar, 01 DEC, Chiara Castro)**

France bans ministers from using WhatsApp, Signal and Telegram on security grounds

France has recently banned its ministers and their teams from using popular communication software WhatsApp, Telegram and even what's perhaps known as the most private encrypted messaging app out there, Signal, due to claimed security vulnerabilities.

This is something that has rather angered the outspoken president of Signal, Meredith Whittaker, who dismissed the allegations as "dangerously misleading."

Back to Table of Contents

Items of Interest

1. **CHINA-TAIWAN WEEKLY UPDATE, DECEMBER 15, 2023 (ISW, 14 DEC, Nils Peterson, Matthew Sperzel, Daniel Shats, Ian Jones, Frank Hoffman, and Kyle Lim)**

   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) DPP presidential candidate Lai Ching-te made significant gains in the polls while support for KMT candidate Hou Yu-ih plateaued.
   2) Chinese Coast Guard and Maritime Militia vessels took aggressive actions against Philippine government vessels near the Spratly Islands in the South China Sea on December 9 and 10.
   3) A loss of Compacts of Free Association funding for Palau, Micronesia, and the Marshall Islands would enable the CCP to expand its leverage points over these countries.
   4) PRC Foreign Minister Wang Yi emphasized the need for an immediate ceasefire to the Israel-Hamas War during separate conversations with American and Iranian officials. Wang's comments are consistent with the PRC's efforts to use the Israel-Hamas War to bolster its image as a fair, responsible broker in contrast to the "biased" United States.

2. **NATO Fighters Scrambled As Russian Drone Violates Romanian Airspace (The Drive/Warzone, 14 DEC, Thomas Newdick)**

Back to Table of Contents

   German and Romanian fighters were sent up to investigate the Russian drone, which crashed in Romanian territory.

   Russian drones targeting Ukraine entered NATO airspace over Romania during the night, leading to the scramble of NATO fighters deployed in that country. The Romanian Ministry of Defense has confirmed that at least one of those drones exploded in its territory, although it was not shot down. Meanwhile, Romania has summoned Russia's envoy over what is the latest in a series of drone violations of its airspace.

3. **15 Air National Guardsmen disciplined in Discord server leak (C4ISRNet, 11 DEC, Meghann Myers)**

   The Air Force has taken action against 15 members of Airman 1st Class Jack Teixeira's chain of command for their roles in a security breakdown that enabled the 21-year-old National Guardsman to remove classified information from his office and post it online.

   While the service maintains that Teixeira acted alone, the Air Force's investigation turned up four separate instances where Teixeira was observed looking at or discussing intelligence a person in his role would have no business accessing. His supervisors were aware of the issues, yet chose not to report them to security officials until months into his activities, according to an investigation released Monday.

4. **Iraq scrambles to contain fighting between US troops and Iran-backed groups, fearing Gaza spillover (AP News, 11 DEC, Kareem Chehayeb & Qassim Abdul-Zahra)**

   Dozens of attacks on U.S. military facilities by Iran-backed factions in Iraq over the past two months as the Israel-Hamas war has raged have forced Baghdad into a balancing act that's becoming more difficult by the day.

A rocket attack on the sprawling U.S. Embassy in Baghdad on Friday marked a further escalation as Iraqi officials scramble to contain the ripple effects of the latest Middle East war.
Iran holds considerable sway in Iraq and a coalition of Iran-backed groups brought Iraqi Prime Minister Mohammed Shia al-Sudani to power in October 2022. At the same time, there are some 2,000 U.S. troops in Iraq under an agreement with Baghdad, mainly to counter the militant Islamic State group.

5. Taiwanese Pilot Planned CH-47 Defection To China: Reports (The Drive/The Warzone, 11 DEC, Oliver Parken)

As part of the plot, the pilot was also allegedly offered safe passage for his family to Thailand should a Chinese invasion of Taiwan occur.

A Taiwanese pilot, allegedly planning to defect to the People's Republic of China (PRC), was reportedly offered $15 million USD to deliver a CH-47 Chinook helicopter to the People's Liberation Army Navy (PLAN). As part of the defection scheme, the individual was supposedly set to land the Chinook on a PLAN vessel in the Taiwan Strait. Along with the money offered, the pilot was also apparently assured by Chinese officials that his family would be given safe passage out of Taiwan should a potential conflict between the country and China erupt.

The pilot in question has been named as Lt. Col. Hsieh of the Republic of China Army (ROCA) as part of an indictment released by Taiwan's High Court Prosecutors Office today. Hsieh was arrested back in August following a tip-off, a Taiwan court heard today, which foiled the defection scheme. According to reports, Hsieh — as well as a wider spy ring within the Taiwanese military connected to his defection — has been on the radar of Taiwanese law enforcement since the spring. Prior to today's revelations, lawmakers previously indicted a group of active and retired Taiwanese officers on November 27 on the grounds of spying for Beijing.

Back to Table of Contents

6. Resisting China's Gray Zone Military Pressure on Taiwan (CNAS, 07 DEC, Jacob Stokes)

The People's Republic of China (PRC or China) has sharply escalated its pressure campaign targeting the Republic of China (ROC or Taiwan) in recent years. Beijing appears likely to use Taiwan's upcoming presidential election in January 2024 as a pretext to apply more pressure on the self-governing island, particularly in the "gray zone" using China's military, the People's Liberation Army (PLA), along with other tools of state power. There is no precise and commonly agreed upon definition of what gray zone activities are and are not. In general, though, the concept refers to actions that fall into the space between, on one side, peace and, on the other, full-scale kinetic war.1 Gray zone activities are coercive and aggressive but designed to stay below the threshold of triggering major conflict.

7. Rocket Launcher Disguised As Fuel Truck Seen Firing In Iraq (The Drive/The Warzone, 05 DEC, Joseph Trevithick)

Iranian-backed militants are using launchers hidden inside civilian vehicles to attack American forces in Iraq and Syria.

Earlier this week, Iranian-backed militants in Iraq fired 122mm artillery rockets at U.S.-led coalition forces in neighboring Syria using an improvised array of launchers disguised inside a modified tanker truck. A video clip, seen in the social media post below, has emerged showing this vehicle in action.

.

Israel-Hamas Conflict

1. The Drive/The Warzone Israel-Gaza Update

Israel-Gaza Situation Report: Ground Campaign Has "Many More Months To Go" – 15 DEC

Israel-Gaza Situation Report: Biden-Netanyahu Friction Increasing – 12 DEC

Israel-Gaza Situation Report: U.S. Vetoes U.N. Ceasefire Demand – 08 DEC

Israel-Gaza Situation Report: IDF Expands Ground Operation Into The South – 05 DEC

Israel-Gaza Situation Report: Ceasefire Ends – 01 DEC

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.

Iran Update, December 15, 2023

Iran Update, December 14, 2023

Iran Update, December 13, 2023

Iran Update, December 12, 2023

Iran Update, December 11, 2023

Iran Update, December 10, 2023

Iran Update, December 09, 2023

Iran Update, December 08, 2023

Iran Update, December 07, 2023

Iran Update, December 06, 2023

Iran Update, December 05, 2023

Iran Update, December 04, 2023

Iran Update, December 03, 2023

Iran Update, December 02, 2023

Iran Update, December 01, 2023

Back to Table of Contents

3. Guided Parachute System Used By Israel For First Time In Gaza (The Warzone, 11 DEC, Howard Altman)

The Israeli Air Force (IAF) on Monday, 11DEC2023, announced the first operational use of its new "Guided Supply" parachute guidance system during combat in Gaza. The IAF said it recently used the system to conduct the first airdrop of this war, delivering about seven tons of water to hundreds of soldiers fighting in Khan Yunis. Beyond the introduction of a new system to the battlefield, the IAF's deployment of this system highlights the challenges Israel faces keeping its troops supplied during a fierce fight in urban pockets that are difficult to access.

Guided Supply "is an advanced operational system that enables parachuting equipment to ground forces using precise navigational capabilities," the Israeli Defense Forces (IDF) said in a media release, which does not offer further details. We don't know if this is their version of the U.S.-made Joint Precision Airdrop System (JPADS) GPS-assisted parachute kits or a JPADS system the U.S. provided. Either way, though, it represents the IAF's first operational use of this system.

While the IDF offered scant details about the Guided Supply system, the IAF Flight Test Squadron had previously tested an unnamed guided airdrop system, the IAF said in a January 2019 media release that has since had its access restricted for undisclosed reasons. However, according to a Google cached version, in 2015, the IDF had purchased “a limited amount of such systems” for testing, with the possible procurement of additional systems in the future. The tests were conducted by the same 103 Squadron that recently used the new Guided Supply system.

4. THE ORDER OF BATTLE OF HAMAS’ IZZ AL DIN AL QASSEM BRIGADES, PART 1: NORTH AND CENTRAL GAZA (ISW, 08 DEC, Brian Carter)

The al Qassem Brigades are the military component of Hamas and the means by which Hamas seeks to destroy the Israeli state and form an Islamic state in Palestine. Hamas is a highly organized group that views terrorism and military action as the only method through which it can destroy the Israeli state. The al Qassem Brigades are commanded by Mohammad Deif and are subordinated to the overall Hamas political leadership responsible to Ismail Haniyeh. They coordinate closely with the Hamas political leader in the Gaza Strip, Yahya Sinwar. Hamas defines itself as a "Palestinian national liberation and resistance movement” intent on establishing an Islamic Palestinian state that stretches “from the River Jordan...to the Mediterranean and from Ras al Naqurah...to Umm al Rashrash.” It is also a member of Iran’s ”Axis of Resistance,” the regional coalition of states and groups that Tehran has built as part of its effort to destroy Israel and expel the United States from the Middle East. Hamas states that "armed resistance” is a "strategic choice” to protect the Palestinian people and rejects "any attempt to undermine [Hamas’] resistance.” Hamas is fighting alongside other Palestinian resistance groups such as Palestinian Islamic Jihad and the Popular Front for the Liberation of Palestine, with which it engages in operational and tactical coordination.

Back to Table of Contents

5. Feds: Iran-linked hacking campaign a ‘clarion call’ for digital defenses (CyberScoop, 04 DEC, Christian Vasquez)

U.S. cybersecurity officials are warning utilities to increase basic cyber protections amid the active targeting of several water facilities by an Iranian-linked hacking group.

The targeting of the Israeli company Unitronics by Cyber Av3ngers, a hacking group with ties to Iran’s Islamic Revolutionary Guard Corps, has highlighted basic vulnerabilities in the water sector. The hackers are not known for sophisticated cyberattacks and often exaggerate the impact of their operations. The hacking spree targeting Unitronics appears to be aimed at influencing the perception of Israeli technologies and had little operational impact on the water facilities.

“We have seen no access to operational systems at these water facilities, nor have we seen any impact to the provision of safe drinking water to the targeted populations,” Eric Goldstein, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency, told reporters Monday, 04DEC2023.

Goldstein did not provide exact figures on the impacted water facilities, but an alert from CISA, the FBI, the National Security Agency, the Environmental Protection Agency and the Israel National Cyber Directorate noted “continued malicious cyber activity.” A government official said last Thursday that the number of affected facilities was less than 10, and so far only a municipal water facility in Aliquippa, Pa., has been identified as a victim.

Russia-Ukraine Conflict

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

Russia-Ukraine Situation Report, 08 December 2023
Russia-Ukraine Situation Report, 07 December 2023
Russia-Ukraine Situation Report, 06 December 2023
Russia-Ukraine Situation Report, 05 December 2023
Russia-Ukraine Situation Report, 04 December 2023

2. The Drive/The Warzone Ukraine Situation Report:

Ukraine Situation Report: Ballistic Missiles Target Kyiv After Biden Meeting – 13 DEC
Ukraine Situation Report: Renewed Large-Scale Assault On Avdiivka – 11 DEC
Ukraine Situation Report: Cruise Missile Strikes Return To Kyiv – 08 DEC
Ukraine Situation Report: Stalled U.S. Military Aid To Kyiv Becoming A Crisis – 07 DEC
Ukraine Situation Report: Deluge Of Rodents A Common Enemy – 04 DEC
Ukraine Situation Report: "We Did Not Achieve The Desired Results," Zelensky Says – 01 DEC

3. Institute for The Study of War

Back to Table of Contents

Russian Offensive Campaign Assessment, December 15, 2023
Russian Offensive Campaign Assessment, December 14, 2023
Russian Offensive Campaign Assessment, December 13, 2023
Russian Offensive Campaign Assessment, December 12, 2023
Russian Offensive Campaign Assessment, December 11, 2023
Russian Offensive Campaign Assessment, December 10, 2023
Russian Offensive Campaign Assessment, December 09, 2023
Russian Offensive Campaign Assessment, December 08, 2023
Russian Offensive Campaign Assessment, December 07, 2023
Russian Offensive Campaign Assessment, December 06, 2023
Russian Offensive Campaign Assessment, December 05, 2023
Russian Offensive Campaign Assessment, December 04, 2023
Russian Offensive Campaign Assessment, December 03, 2023
Russian Offensive Campaign Assessment, December 02, 2023
Russian Offensive Campaign Assessment, December 01, 2023

4. THE HIGH PRICE OF LOSING UKRAINE (ISW, 14 DEC, Frederick W. Kagan, Kateryna Stepanenko, Mitchell Belcher, Noel Mikkelsen & Thomas Bergeron)

The United States has a much higher stake in Russia's war on Ukraine than most people think. A Russian conquest of all of Ukraine is by no means impossible if the United States cuts off all military assistance and Europe follows suit. Such an outcome would bring a battered but triumphant Russian army right up to NATO's border from the Black Sea to the Arctic Ocean. The Ukrainian military with Western support has destroyed nearly 90% of the Russian army that invaded in February 2022 according to US intelligence sources, but the Russians have replaced those manpower losses and are ramping up their industrial base to make good their material losses at a rate much faster than their pre-

war capacity had permitted.

5. Ukraine's innovative edge counters Russian mass, official says (C4ISRNET, 14 DEC, Colin Demarest)

The Ukrainian military is repelling attacks from numerically superior Russian forces by combining new-school inventiveness and technology with old-school tactics on the battlefield, according to one official.

While Moscow's war machine dwarfs its neighbor, with more manpower and built-up materiel at its disposal, Kyiv has for nearly two years withstood bombardment in both the physical and digital worlds.

Maj. Gen. Borys Kremenetskyi, the defense attaché with the Embassy of Ukraine in the U.S., on Dec. 13 credited his besieged country's endurance to an "asymmetric approach" that confronts volume and brute force with scrappiness and creativity. Hobbyist toys including first-person-view drones have been transformed into anti-armor and personnel weapons, and cellphones have become tools for detection of missiles and other overhead attacks.

The U.S. and its European allies have sought to swing the balance in Ukraine's favor, injecting billions of dollars of weapons, ammunition, combat vehicles and training into the fight. Norway on Wednesday promised to donate more National Advanced Surface-to-Air Missile Systems, or NASAMS, worth approximately $31 million.

6. Drones, jammers in Ukraine signal new era of warfare, Del Toro says (C4ISRNET, 12 DEC, Colin Demarest)

Back to Table of Contents

Russia's invasion of Ukraine, now nearing the end of its second year, has ushered in a "new era of war" in which drones and electronic warfare are having outsize impacts, the secretary of the U.S. Navy said.

Both Russian and Ukrainian militaries are employing unmanned aerial systems to scout, target and attack while simultaneously using jammers and spoofers to defend the skies above or the trenches they've dug. The cat-and-mouse game is deadly, with each side trying to outthink and outbuild the other.

The U.S. Department of Defense is pouring billions of dollars into the development of drones, EW and a mix of the two.

The Navy this year tested Lockheed Martin's Advanced Off-Board Electronic Warfare pod, meant to be mounted aboard helicopters to detect and deceive anti-ship missiles, and separately linked what one commander described as "unmanned and unmanned" at the Integrated Battle Problem exercise in the waters off California.

7. Cyberattack Cripples Ukraine's Largest Telecom Operator (SecurityWeek, 12 DEC, SecurityWeek News)

Kyivstar, the largest mobile network operator in Ukraine, was hit by a massive cyberattack on Tuesday, 12DEC2023, disrupting mobile and internet communications for millions of citizens.

Kyivstar has nearly 25 million mobile subscribers and more than 1 million home internet customers.

Kyivstar CEO Oleksandr Komarov claimed the cyberattack was "a result of" the war with Russia and that the company's IT infrastructure had been "partially destroyed".

A system used to send air raid alerts in parts of Kyiv was also impacted.

Kyivstar parent company, Netherlands-based VEON Ltd., confirmed that Kyivstar had

been the target of a widespread attack on the morning of December 12, 2023, calling it "one of the largest cyberattacks in the history of the global telecom market."

The damaging attack appears to be the most impactful event in cyberspace to hit Ukraine since Russia's invasion in February 2022, when a cyberattack on Viasat crippled communications on the KA-SAT satellite network used by Ukraine's government and military, also impacting tens of thousands of modems across Europe

8. Russia Installs "Emotional Support Cages" Over Its Trenches To Defend Itself From Ukraine's Kamikaze UAVs (The EurAsian Times, 12 DEC, Parth Satam)

After tanks, armored fighting vehicles, and artillery guns, Russian trenches have also begun sporting 'cope cages' to protect themselves from kamikaze drones. This is in response to an emerging tactic of using first-person view (FPV) loitering munitions even for anti-infantry use.

Small units of soldiers in bunkers and defensive lines are hit solely with the UAVs while overhead drones direct the strikes. This lessens the employment of own troops in close-quarter battles that might lead to casualties.

In some cases, the civilian-commercial drones could also be slung with small explosives that are dropped on soldiers, trenches, or bunkers on the ground – besides fast-flying unmanned aerial vehicles (UAV) retrofitted with front-armed warheads.

Back to Table of Contents