U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

15-31 October 2023

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

Table of Contents

1. Swedish-Estonian telecommunications cable damaged by 'external force or tampering' – 25 OCT
2. Mitigating The Quantum Threat Today – 23 OCT
3. Upgrade networks or suffer on the battlefield, general warn – 20 OCT
4. Isreal Selects SpaceX's Starlink for Wartime Communications – 18 OCT
5. Meta's AI message on Instagram don't seem to be encrypted – 14 OCT

Items of Interest

1. China Set To Become World's Biggest Military Power? US Congress Paints A Worrying Picture – 25 OCT
2. US cybersecurity agency funding under fire from Sen. Rand Paul – 24 OCT
3. Former NSA worker pleads guilty to trying to sell US secrets to Russia – 23 OCT
4. NATO to adopt first-ever counter-drone doctrine for member nations – 20 OCT
5. DOD to brief Congress early next year on zero-trust progress – 19 OCT
6. How US Could Respond if Russia Shoots Down Satellite – 18 OCT
7. Army Faces Fight Just to Survive in the Arctic – 17 OCT
8. Navy's new Neptune cloud management office gaining steam – 16 OCT

Russia-Ukraine Situation

1. Russia-Ukraine Situation Report
2. The Drive/The Warzone Ukraine Situation Report
3. Institute for The Study of War
4. Israel-Hamas war complicates Western Support to Ukraine – 23 OCT
5. Ukraine continues to snap up Chinese DJI drones for its defense – 23 OCT
6. Russian economy becomes heavily reliant on China – 22 OCT
7. Destruction From Ukraine's First ATACMS Strike Now Apparent – 18 OCT
8. Ukraine's digital natives drive C4 capabilities – 17 OCT

Israel-Hamas Situation

1. The Drive Israel-Gaza Update
2. Institute for The Study of War Iran Update
3. Netanyahu Says War in Gaza will be 'long and difficult – 28 OCT
4. Israel's using widespread GPS tampering to deter Hezbollah's missiles – 23 OCT
5. Hamas-linked app offers window into cyber infrastructure, possible links to Iran – 19 OCT

Cyber

1. Israel's Check Point says cyberattacks rising, sees higher profit (Reuters, 30 OCT, Steven Scheer)

   Israel has seen a jump in cyberattacks since the Oct. 7 raids by Hamas, but Check Point Software Technologies (CHKP.O) has continued to operate as planned despite the ensuing war and expects higher annual profits than previously thought, it said on Monday.

   Gil Shwed, CEO of the Israeli-based company, said 98% of its customers were outside Israel and it had successfully launched new technologies and completed acquisitions.

2. **Microsoft on the state of OT security. Zero-days affect industrial routers. Israeli and Palestinian hacktivists target ICS. (The Cyber Wire, 25 OCT)**

   At a glance.

   - Zero-days affect industrial routers.
   - Israeli and Palestinian hacktivists target ICS.
   - Johnson Controls sustains cyberattack.
   - Ransomware attack on Clorox.
   - Colonial Pipeline says new ransomware claims are due to an unrelated third-party breach.
   - Coinmining as an (alleged, potential) front for espionage or stage for sabotage.
   - Nearly 100,000 ICS services exposed to the Internet.
   - Microsoft on the state of OT security.
   - CISA views China as the top threat to US critical infrastructure.
   - FBI anticipates an increase in Chinese and Russian targeting of the energy sector.
   - Joint advisory warns of Beijing's "BlackTech" threat activity.
   - NSA releases ICS intrusion detection signatures.
   - CISA's push for hardware bills of materials.
   - Improving security for open-source ICS software.
   - Homeland Security IG finds flaws in TSA pipeline security regulations.
   - EPA withdraws water system cybersecurity memorandum.
   - Cybersecurity in the US industrial base.
   - Most organizations are struggling with IoT security.
   - CISA ICS advisories.

3. **Dangerous new malware can crack encrypted USB drives (Tech Radar, 23 OCT, Sead Fadilpašić)**

   TetrisPhantom seen targeting government devices to hack official secrets.

   Cybersecurity researchers from Kaspersky have uncovered a sophisticated new piece of malware called TetrisPhantom seen compromising secure USB drives to steal

sensitive information from government endpoints in the Asia-Pacific region.

Secure USB drives have an encrypted partition whose files can only be accessed with a password, and through specialized software, like the one called UTetris. This method is generally used to safely transfer data between systems, including air-gapped endpoints, BleepingComputer reports.

4. **China Crackdown on Cyber Scams in Southeast Asia Nets Thousands but Leaves Networks Intact (SecurityWeek, 23 OCT, AP News)**

Zhang Hongliang, a former restaurant manager in central China, took various gigs in and outside China to support his family after losing his job during the COVID-19 pandemic.

In March, a job offer to teach Chinese cooking at a restaurant led him into a cyber scam compound in Myanmar, where he was instead ordered to lure Chinese into giving up their savings for fake investment schemes via social media platforms.

Iranian Hackers Lurked for 8 Months in Government Network (SecurityWeek, 20 OCT, Ionut Arghire)

Iran-linked hacking group Crambus spent eight months inside a compromised network of a Middle Eastern government, Broadcom's Symantec cybersecurity unit reports.

Symantec uses the Crambus name for clusters of activity that other cybersecurity firms are tracking as APT34 (also known as Cobalt Gypsy, OilRig, and Helix Kitten), and MuddyWater (aka Mango Sandstorm, Mercury, Seedworm, and Static Kitten).

5. **FBI: Thousands of Remote IT Workers Sent Wages to North Korea to Help Fund Weapons Program (SecurityWeek, 19 OCT, AP News)**

Thousands of information technology workers contracting with U.S. companies have for years secretly sent millions of dollars of their wages to North Korea for use in its ballistic missile program, FBI and Department of Justice officials said.

The Justice Department said Wednesday that IT workers dispatched and contracted by North Korea to work remotely with companies in St. Louis and elsewhere in the U.S. have been using false identities to get the jobs. The money they earned was funneled to the North Korean weapons program, FBI leaders said at a news conference in St. Louis.

6. **North Korean Hackers Exploiting Recent TeamCity Vulnerability (SecurityWeek, 19 OCT, Ionut Arghire)**

Multiple North Korean threat actors have been observed exploiting a recent vulnerability in JetBrains' TeamCity continuous integration and continuous deployment (CI/CD) server, Microsoft warns.

Tracked as CVE-2023-42793, the critical-severity flaw allows unauthenticated attackers to execute code remotely on vulnerable on-premises TeamCity instances and gain administrator-level permissions.

7. **Police seize Ragnar Locker leak site (CyberScoop, 19 OCT, AJ Vicens)**

Law enforcement agencies from more than a dozen countries seized a website used by the criminal hacking group known as Ragnar Locker to leak stolen data and information, according to a message posted to the site's front page.

The seizure is the latest in a string by global law enforcement agencies to take down the public facing websites and infrastructure of ransomware groups..

8. **[Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability](#) (Microsoft, 18 OCT, Microsoft Threat Intelligence)**

   Since early October 2023, Microsoft has observed two North Korean nation-state threat actors – Diamond Sleet and Onyx Sleet – exploiting CVE-2023-42793, a remote-code execution vulnerability affecting multiple versions of JetBrains TeamCity server. TeamCity is a continuous integration/continuous deployment (CI/CD) application used by organizations for DevOps and other software development activities.

   In past operations, Diamond Sleet and other North Korean threat actors have successfully carried out software supply chain attacks by infiltrating build environments. Given this, Microsoft assesses that this activity poses a particularly high risk to organizations who are affected. JetBrains has released an update to address this vulnerability and has developed a mitigation for users who are unable to update to the latest software version.

9. **[Former Navy IT Manager Sentenced to Prison for Hacking, Selling PII](#) (SecurityWeek, 18 OCT, Ionut Arghire)**

   A former US Navy IT manager was sentenced to five years and five months in prison for hacking into a database, stealing personally identifiable information (PII), and selling it on the dark web.

   The man, Marquis Hooper, 32, of Selma, California, who was a chief petty officer, opened under false pretenses an account at a private company operating a database containing the PII of millions of individuals.

[Back to Table of Contents](#)

10. **[Tens of Thousands of Cisco Devices Hacked via Zero-Day Vulnerability](#) (SecurityWeek, 18 OCT, Eduard Kovacs)**

    Tens of thousands of Cisco devices have reportedly been hacked through the exploitation of the newly disclosed IOS XE zero-day vulnerability tracked as CVE-2023-20198.

    Cisco warned customers on Monday that a critical IOS XE zero-day has been exploited by threat actors to gain elevated privileges on devices. The company is working on a patch and in the meantime, it has urged customers to implement mitigations.

11. **[US Gov Expects Widespread Exploitation of Atlassian Confluence Vulnerability](#) (SecurityWeek, 17 OCT, Ionut Arghire)**

    US cybersecurity agency CISA, the FBI, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) warn organizations of potential widespread exploitation of a recent zero-day vulnerability in Atlassian Confluence Data Center and Server.

    Tracked as CVE-2023-22515 (CVSS score of 9.8), the bug has been exploited by a nation-state threat actor since September 14, roughly two weeks before Atlassian released patches for it.

12. **[Cisco Devices Hacked via IOS XE Zero-Day Vulnerability](#) (SecurityWeek, 17 OCT, Eduard Kovacs)**

    Cisco is warning customers that a new zero-day vulnerability impacting the company's IOS XE software is being exploited to hack devices.

    The critical vulnerability is tracked as CVE-2023-20198 and it has been described as a privilege escalation issue impacting the IOS XE web user interface, which comes with

the default image. A remote, unauthenticated attacker can exploit the vulnerability to create an account that has the highest privileges — level 15 access — and use it to take control of the device. The vulnerability can be exploited from the network or directly from the internet if the targeted device is exposed to the web.

13. **Spyware Caught Masquerading as Israeli Rocket Alert Applications (SecurityWeek, 16 OCT, Ionut Arghire)**

    In the wake of the Israel-Gaza conflict, threat actors have been observed targeting Israeli rocket alerting applications to spread fear and mobile spyware, Cloudflare reports.

    With thousands of rockets launched since Hamas attacked Israel on October 7, individuals in Israel rely on several mobile applications to receive timely alerts about incoming airstrikes and seek safety.

Electronic Warfare

1. **Most Sustained 'GPS Spoofing' Ever! Israel Thwarts Hezbollah Rockets By Tampering With GPS Signals? (The Eurasian Times, 25 OCT, Sakshi Tiwari)**

    The Israel Defense Forces (IDF) have reportedly been tampering with the GPS signals over its northern airspace as fears of an all-out war between Israel and the Lebanon-based Hezbollah militant group looms.

    To defend itself against Hezbollah missile strikes, Israel is scrambling GPS signals over most of its northern airspace, perhaps even putting Israeli people and commercial airliners at risk.

    This is significant as it comes against escalating tensions between the two sides, with Hezbollah reportedly firing missiles and drones on targets inside Israel.

2. **US Army tags electronic warfare, deep sensing as top priorities (Janes, 25 OCT, Carlo Munoz)**

    The US Army's top officer is leading an effort to implement changes to the ground service's strategy for capability development on electronic warfare (EW) and deep-sensing intelligence, surveillance, and reconnaissance (ISR) operations, identifying both areas as top priorities for research, development, and procurement.

    "I think we recognise that EW is an area that the army has probably made limited investment in as a capability during two decades of counter-terrorism operations in Iraq and Afghanistan," US Army General Randy George told reporters during a briefing at the Association of the US Army's (AUSA's) annual symposium in Washington, DC in October.

    "As we look at the army's role as part of a joint force, globally employed especially in the Indo Pacific region … we want to look at the EW portfolio and figure out where we need to place, you know, investment, and what areas we can potentially accelerate," he said.

3. **Nigerian Army has acquired electronic warfare capabilities – COAS Gen. Lagbaja (Daily Post, 23 OCT, Francis Ugwu)**

    The Chief of Army Staff (COAS), Lt.-Gen. Taoreed Lagbaja, says the Nigerian Army has acquired electronic warfare capabilities and is now taking advantage of the convergence of electronic and cyber warfare.

Lagbaja said this on Monday in Abuja, at the opening of the Maiden Cyber Security Workshop of the Nigerian Army Cyber Warfare School (NACWS).

The News Agency of Nigeria (NAN) reports that the theme of the workshop is, 'Role of Information Technology to national security against upcoming threats and cyber-attacks'.

4. **China may struggle in electromagnetic spectrum fighting, Pentagon says (C4ISR, 23 OCT, Colin Demarest)**

The Chinese military is wrestling with shortcomings in fights where access to and control of the electromagnetic spectrum is hotly contested, according to a U.S. Department of Defense assessment.

The spectrum is a critical resource in modern conflicts, as its manipulation enables navigation, communication, deception and even weapons guidance. A dizzying amount of electronic jamming and spoofing is expected in a fight between world powers.

5. **Army may add electronic warfare training as early as boot camp (Task and Purpose, 23 OCT, Patty Nieberg)**

From battlefield radios to Bluetooth trackers on supplies and equipment, soldiers may start training on electromagnetic warfare skills as early as basic training.

Three basic battlefield skills all soldiers learn early in their training is to "shoot, move and communicate." But in the modern battlefield, firing a weapon or using a radio is almost certain to light up a sensor, reveal a soldier's location and perhaps lead to fatal consequences for units, said Maj. James Armstrong, an instructor at the U.S. Army Cyber School.

"Just like your artillery has a very big audible visual signature when it lights up, so does your radio," said Armstrong. "It doesn't mean that you just turn everything off and don't talk. It means you've got to be smart about how you use it."

6. **Ukrainian govt expedites production of electronic warfare equipment (Euromaidan, 21 OCT, Orysia Hrudka)**

This move follows a previous successful initiative that accelerated the domestic drone market, making it more accessible to the military and reinforcing Ukraine's defense capabilities.

The Ukrainian government has taken steps to accelerate the production of Radio Electronic Warfare (REW) equipment, streamlining the process for getting this vital technology into the hands of the military. REW equipment will now be approved for deployment based on joint departmental testing or an evaluation of claimed tactical and technical characteristics.

7. **Azerbaijan reveals details of electronic warfare of Karabakh separatists (Caliber, 19 OCT, Mushvig Hehdiyev)**

The State Security Service of Azerbaijan announced on October 19 the launch of an investigation into criminal cases of extensive deployment of radioelectronic warfare by the disarmed Armenian army formations in the country's Karabakh (Garabagh) region.

According to the Service, in 2021-2023, civilian flights operated by Azerbaijan Airlines and foreign air carriers faced serious navigation problems over Karabakh and surrounding areas due to the intensive application of radio interference systems by the illegal army formations of the Armenian Armed Forces.

8. **[US Army and Lockheed Martin pave the way for advanced EW capabilities] (Army-Technology, 19 OCT, Harry McNeil)**

   Successful testing of the Multi-Function Electronic Warfare-Air Large (MFEW-AL) system signifies a leap forwards in electronic warfare technology.

   The United States Army and Lockheed Martin have successfully tested the Multi-Function Electronic Warfare-Air Large (MFEW-AL) system, marking a step towards enhancing electronic warfare capabilities.

9. **[Azerbaijan captures Russian-made electronic warfare systems in Karabakh] (Defense Blog, 19 OCT, Dylan Malyasov)**

   Azerbaijani forces have seized the modern Russian-made Repellent-1 electronic warfare system and the Pole-21M jamming system from Armenia-backed disbanded Karabakh forces.

   The Repellent-1 EW system, known for its advanced capabilities, was a primary "gift." This system is designed to detect and jam enemy electronic communication and radar signals.

Information Advantage

Back to Table of Contents

1. **[Ukraine at D+614: Riots and disinformation]. (The Cyber Wire, 31 OCT)**

   Ukraine's incremental advance near Bakhmut and in western Zaporizhia Oblast have been independently confirmed, the Institute for the Study of WAR (ISW) reports. The ISW also quotes Russian milbloggers who continue to criticize the use of poorly trained Storm-Z penal formations in murderously costly, ill-supported frontal assaults against Ukrainian positions in Avdiivka. The milbloggers call the attacks "meat assaults" and say the Storm-Z units are expended in a few days of operation, losing between 40% and 70% of their personnel in these engagements. (A comparative note: US targeted doctrine considers a unit that's taken 20% losses to have been destroyed, effectively rendered permanently incapable of combat operations.)

2. **[Chinese Influence in Pacific Island Countries, 11–23 October 2023] (U.S. Army Asian Studies Detachment, 24 OCT)**

   This report covers news articles of significance from Pacific Island Countries, such as Fiji, Papua New Guinea, Solomon Islands, Vanuatu, Micronesia, Kiribati, Marshall Islands, Nauru, and Palau. It highlights cultural, economic, diplomatic, public health, security, and military activities and developments involving China.

3. **[Taliban in Afghanistan Plans Join China's Belt and Road Initiative] (U.S. Army Asian Studies Detachment, 23 OCT)**

   On 19 October 2023, Afghanistan's minister of commerce announced that the Taliban government plans to officially join Chinese President Xi Jinping's Belt and Road Initiative (BRI). The Taliban will send a technical team to China to discuss joining the initiative. In September 2023, China became the first country to appoint a charge d'affaires in Kabul. The Taliban government expressed interest in Chinese investment, as Afghanistan has valuable resources. Chinese companies have already held talks with the Taliban administration about potential projects, such as the Metallurgical Corp. of China Ltd.

4. **BRI - Belt and Road Initiative - Highlights, 19 October 2023 (U.S. Army Asian Studies Detachment, 23 OCT)**

   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.

5. **One Belt, One Road & One DEBT! Is China Looking To Boost The BRI As Many Hit By Debt Trap Concerns? (The Eurasian Times, 19 OCT, Vaishali Basu Sharma)**

   Representatives from about 130 countries have gathered at the Chinese capital as President Xi Jinping's signature policy, the Belt and Road Initiative (BRI), which he described as the 'project of the century,' completes ten years.

   India has boycotted the two-day Belt and Road Forum for International Cooperation (BRFIC) over the controversial CPEC, which is being laid through the Pakistan-occupied Kashmir, and the financial viability of Beijing's projects in smaller countries.

   The two-day summit to mark BRI's 10th anniversary is hoped to reinvigorate the project. Russian President Vladimir Putin, Hungary's Prime Minister Viktor Orban, Indonesian President Joko Widodo, Argentina's President Alberto Fernandez, and Thai Premier Srettha Thavisin are also attending.

Back to Table of Contents

6. **Chinese military boosting its ability to defeat kamikaze drones (DefenseScoop, 19 OCT, Jon Harper)**

   The People's Liberation Army is focusing on beefing up its defenses against adversaries' tactical unmanned aerial systems, according to a new Pentagon report.

   Loitering munitions — also known as kamikaze drones or one-way attack drones — and other small UAS have been featured prominently on the battlefields in Ukraine and have appeared in other locations. Nations around the world, including the United States, are developing and fielding them — and China is taking note.

7. **North Korea: Intense Crackdowns on Illegal Mobile Phone Use (U.S. Army Asian Studies Detachment, 17 OCT)**

   On 10 October 2023, Daily NK reported that in early September 2023 the Ministry of State Security ordered the North Hamgyong Province state security bureau to conduct strict crackdowns on the use of Chinese mobile phones.

Signal

1. **Swedish-Estonian telecommunications cable damaged by 'external force or tampering' (Janes, 25 OCT, Kate Tringham)**

   An undersea telecommunications cable between Sweden and Estonia has been damaged by means of external force or tampering, the Swedish government has confirmed.

   The incident has been linked to the suspected sabotage of the Balticconnector undersea gas pipeline and telecommunications cable that connects Finland and Estonia in early October.

2. **Mitigating The Quantum Threat Today (Forbes, 23 OCT, David Williams)**

   Headlines this year regularly report on breakthroughs in quantum computing, and the predicted growth of quantum computing power is exponential, outstripping even the unprecedented speed of development of classical computing as modeled by Moore's Law. The cryptanalytic threat of quantum computing, particularly the "store data; decrypt later" approach, is drawing ever nearer. Unsurprisingly, the U.S. government is among those most alert to the danger.

3. **Upgrade networks or suffer on the battlefield, generals warn (C4ISR Net, 20 OCT, Colin Demarest)**

   Maj. Gen. Paul Stanton leafed through his notebook.

   He was sitting alone on stage during the last day of the Association of the U.S. Army's annual conference, held in early October in Washington. The Army officer had just been asked about remarks made by the service's newly sworn-in chief of staff, Gen. Randy George.

   "Under continuous transformation, he did say the No. 1 priority and focus area is the network," Stanton said, looking up from his notes and smiling. "Our Army senior leadership understands the significance of being able to move the right data to the right place at the right time."

4. **Israel Selects SpaceX's Starlink for Wartime Communications (Tesmanian, 18 OCT, Evelyn Janeidy Arevalo)**

   In response to the ongoing conflict with Hamas that escalated on October 7, Israel's Minister of Communications, Shlomo Karhi, has unveiled a plan to secure crucial wartime communications with SpaceX's Starlink satellite internet service. The announcement, made on October 17, signifies a significant step in the nation's efforts to maintain communication infrastructure as it prepares to launch a ground offensive in the Gaza Strip aimed at eliminating the threat posed by Hamas.

5. **Meta's AI messages on Instagram don't seem to be encrypted (Mashable, 14 Oct, Cecily Mauran)**

   A heads-up before you bare your soul to an AI persona.

   Before you go pouring your heart out to Billie, "your ride-or-die older sister" played by Kendall Jenner, or an AI grandpa named Brian on Instagram, know that your messages might not be private.

   Meta's AI personas, now live in beta, are a collection of characters — some played by

celebrities and creators — that users can chat with on Messenger, Instagram, and WhatsApp. However, it appears that messages with these characters on Instagram are not end-to-end encrypted.

Items of Interest

1. **China Set To Become World's Biggest Military Power? US Congress Paints A Worrying Picture (The Eurasian Times, 25 OCT, Prakash Nanda)**

   It may not be militarily significant that China has deployed its 44th naval escort taskforce for "routine operations" to the Middle East amid rising regional tensions following the conflict between Israel and Hamas. But strategically speaking, it is said to have conveyed a strong message.

   The fact that China's deployment last week took place soon after the US sent a powerful arsenal to the Middle East is being interpreted by the US strategic elites that, more than Russia, China poses fundamental challenges to American power.

1. **US cybersecurity agency funding under fire from Sen. Rand Paul (C4ISRNet, 24 OCT, Molly Weisner)**

   Sen. Rand Paul, a top critic of the federal government's cybersecurity watchdog, says the agency is overstepping its authority by trying to regulate the flow of information online.

2. **Former NSA worker pleads guilty to trying to sell US secrets to Russia (C4ISRNet, 23 OCT, Colleen Slevin)**

Back to Table of Contents

   A former National Security Agency employee from Colorado pleaded guilty Monday to trying to sell classified information to Russia.

   Federal prosecutors agreed to not ask for more than about 22 years in prison for Jareh Sebastian Dalke when he is sentenced in April, but the judge will ultimately decide the punishment.

3. **NATO to adopt first-ever counter-drone doctrine for member nations (C4ISRNet, 20 OCT, Elisabeth Gosselin-Malo)**

   NATO is expected to adopt its first-ever counter-drone doctrine, which will in part advise member states on layered approaches to defend against unmanned aerial systems and the common training of operators.

4. **DOD to brief Congress early next year on zero-trust progress (DefenseScoop, 19 OCT, Mark Pomerleau)**

   The Department of Defense is expected to brief Congress in January on progress made toward achieving so-called zero trust, according to a senior official.

   Zero trust is a cybersecurity concept and framework that assumes networks are already compromised and require constant monitoring and authentication to protect critical information.

5. **How US Could Respond if Russia Shoots Down Satellites (News Week, 18 OCT, Isabel Van Brugen**

   The chief of the U.S. Space Force has outlined how Washington could respond if

Moscow shoot down Western commercial satellites.

General Chance Saltzman said at a press conference in Hawaii on September 20 that U.S. military space capabilities are under threat from nations like China and Russia and outlined how Washington could respond should Moscow attack SpaceX's Starlink broadband network, which Ukraine uses for Internet connectivity in Russia's full-scale invasion, Ars Technica reported.

6. **Army Faces Fight Just To Survive In the Arctic (The Drive/The War Zone, 17 OCT, Thomas Newdick)**

Critical high-tech gear doesn't work in the Arctic, with batteries draining in minutes, howitzers freezing up, and vehicles breaking down.

The U.S. Army faces a host of challenges in moving beyond just surviving in and around the ever-more strategic Arctic region to actually being able to operate there effectively. Many standard weapons and other equipment, as well as typical tactics, techniques, and procedures, literally do not work in this part of the world. This, in turn, is prompting calls for new and innovative approaches to many problems, many of which might be easily solvable in more temperate climes.

7. **Navy's new Neptune cloud management office gaining steam (DefenseScoop, 16 OCT, Jon Harper)**

The Navy component of the sea services' new cloud management office is up and running, according to a senior official from the program executive office for digital and enterprise services.

Back to Table of Contents

The nascent outfit, known as Neptune, is intended to serve as a single point of entry for the acquisition and delivery of cloud services across the Department of the Navy. A memo formally establishing the organization was signed off in June.

Russia-Ukraine

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

Russia-Ukraine Situation Report, 30 October 2023
Russia-Ukraine Situation Report, 27 October 2023
Russia-Ukraine Situation Report, 26 October 2023
Russia-Ukraine Situation Report, 25 October 2023
Russia-Ukraine Situation Report, 24 October 2023
Russia-Ukraine Situation Report, 23 October 2023
Russia-Ukraine Situation Report, 20 October 2023
Russia-Ukraine Situation Report, 19 October 2023
Russia-Ukraine Situation Report, 18 October 2023
Russia-Ukraine Situation Report, 17 October 2023
Russia-Ukraine Situation Report, 16 October 2023

2. **The Drive/The Warzone Ukraine Situation Report:**

Ukraine Situation Report: Zelensky Vows To Up The Pressure On And Around Crimea – 24 OCT
Ukraine Situation Report: Multiple Russian Attacks On Avdiivka Repulsed – 23 OCT

Ukraine Situation Report: ATACMS May Spur Russian Force Relocations, U.K. Intel Says – 20 OCT

Ukraine Situation Report: Russia Recruiting Serbian Fighters – 18 OCT

Ukraine Situation Report: Russia's Localized Offensive "Failing," Ukraine Claims – 16 OCT

3. Institute for The Study of War

Russian Offensive Campaign Assessment, October 31, 2023
Russian Offensive Campaign Assessment, October 30, 2023
Russian Offensive Campaign Assessment, October 27, 2023
Russian Offensive Campaign Assessment, October 26, 2023
Russian Offensive Campaign Assessment, October 25, 2023
Russian Offensive Campaign Assessment, October 24, 2023
Russian Offensive Campaign Assessment, October 23, 2023
Russian Offensive Campaign Assessment, October 22, 2023
Russian Offensive Campaign Assessment, October 21, 2023
Russian Offensive Campaign Assessment, October 20, 2023
Russian Offensive Campaign Assessment, October 19, 2023
Russian Offensive Campaign Assessment, October 18, 2023
Russian Offensive Campaign Assessment, October 17, 2023
Russian Offensive Campaign Assessment, October 16, 2023

Back to Table of Contents

4. Israel-Hamas war complicates Western support to Ukraine (Caliber.az, 23 OCT, Fuad Shahbazov)

U.S. President Joe Biden is preparing to host European leaders Charles Michel and Ursula von der Leyen in the White House at a summit set to deliver a message of unity on conflicts in Gaza and Ukraine. As fighting rages on in Ukraine, Israel's war against Hamas, the armed group that rules Gaza, threatens to spill over across the Middle East.

Drawing parallels between Russia's invasion of Ukraine and Hamas's assault, European Commission President Ursula von der Leyen said that "these two crises, however different, call on Europe and America to take a stand together" in order to "shelter our democracies".

5. Ukraine continues to snap up Chinese DJI drones for its defense (C4ISRNet, 23 OCT, Elisabeth Gosselin-Malo)

Ukrainian Prime Minister Denys Shmyhal said the country's forces are leaning heavily on Chinese DJI drones in the defense of their country, a claim that the manufacturer has since declared was news to them.

The Oct. 8 statement made by Denys Shmyhal at the Kyiv International Economic Forum that Ukraine is effectively buying 60% of DJI's global output of Mavic quadcopter drones, even though the vendor officially prohibits selling to militaries, highlights how commercial technology with military utility can permeate conflict zones practically unimpeded.

6. Russian economy becomes heavily reliant on China (Caliber.az, 22 OCT, Mikhail Shereshevskiy)

With the outbreak of the conflict in Ukraine, the Russian economy has become increasingly dependent on the Chinese economy. China is gradually replacing Western

countries that have partially severed economic relations with Russia. Trade turnover between China and Russia this year could reach $200 billion. The influence of China is diverse and develops along many lines.

7. **Destruction From Ukraine's First ATACMS Strike Now Apparent (The Drive/The War Zone, 18 OCT, Joseph Trevithick, Tyler Rogoway)**

   Satellite images show how effective cluster munition versions of ATACMS are for striking air bases full of soft targets out in the open.

   The War Zone has obtained satellite imagery showing the aftermath of Ukraine's first strikes using U.S.-supplied Army Tactical Missile System short-range ballistic missiles, or ATACMS, on the airport in the Russian-occupied city of Berdyansk yesterday. What can be seen looks to be broadly in line with the destruction Ukrainian officials said they had wrought on the facility using their newly delivered cluster munition-filled missiles.

8. **Ukraine's digital natives drive C4 capabilities (Janes, 17 OCT, Giles Ebbutt)**

   Ukraine's progress in digital transformation (DT) has been one of the reasons behind its resilience in the conflict with Russia, and this has been due as much to cultural attitudes as technology, according to Gerard Elzinga, head of digital capabilities, NATO digital staff.

   Speaking at the at the Armed Forces Communications Electronics Association's (AFCEA's) TechNet Europe 2023 conference in London, Elzinga said that Ukraine's development of digital capabilities for defence and security had been in progress for some time before Russia's invasion.

Israel-Hamas

1. **The Drive Israel-Gaza Update**

   Israel-Gaza Situation Report: Arrow Interceptor Dows Ballistic Missile Over Red Sea (Updated) - 31 OCT
   Israel-Gaza Situation Report: IDF Moving TO Cut Off Gaza City From South - 30 OCT
   Israel-Gaza Situation Report: Merkava Tanks Roll Down Gaza Beach (Updated) - 29 OCT
   Israel-Gaza Situation Report: Israel Officially Begins "Second Stage" Of The War - 28 OCT
   Israel-Gaza Situation Report: Major Expansion Of Ground Operation Into Gaza Underway - 27 OCT
   Israel-Gaza Situation Report: Israeli Armor Rolls Into Gaza For "Targeted Raid" – 26 OCT
   Israel-Gaza Situation Report: Delay Of Ground Offensive Agreed To – 25 OCT
   Israel-Gaza Situation Report: Hamas Frogmen Attempt To Infiltrate Near Israeli Base – 24 OCT
   Israel-Gaza Situation Report: Israel Conducts Limited Gaza Ground Raid (Updated) – 23 OCT
   Israel-Gaza Situation Report: U.S. Flows Missile Defenses Into Middle East – 22 OCT
   Israel-Gaza Situation Report: IDF's Gaza Operation Plan Laid Out – 20 OCT
   Israel-Gaza Situation Report: Netanyahu Warns Of "A Long War" To Come – 19 OCT
   Israel-Gaza Situation Report: Biden Tells Israel Not To Be Consumed By Rage – 18 OCT
   Many Killed In Massive Explosion At Gaza Hospital (Updated) – 17 OCT

Israel Gets Coy On Gaza Ground Assault – 17 OCT

3. 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, OCTOBER 31, 2023
IRAN UPDATE, OCTOBER 30, 2023
IRAN UPDATE, OCTOBER 29, 2023
IRAN UPDATE, OCTOBER 28, 2023
IRAN UPDATE, OCTOBER 27, 2023
IRAN UPDATE, OCTOBER 26, 2023
IRAN UPDATE, OCTOBER 25, 2023
IRAN UPDATE, OCTOBER 24, 2023
IRAN UPDATE, OCTOBER 23, 2023
IRAN UPDATE, OCTOBER 22, 2023
IRAN UPDATE, OCTOBER 21, 2023
IRAN UPDATE, OCTOBER 20, 2023
IRAN UPDATE, OCTOBER 19, 2023
IRAN UPDATE, OCTOBER 18, 2023
IRAN UPDATE, OCTOBER 17, 2023
ISRAEL–HAMAS WAR (IRAN UPDATES), OCTOBER 17, 2023
IRAN UPDATE, OCTOBER 16, 2023
IRAN UPDATE, OCTOBER 15, 2023

1. Netanyahu says war in Gaza will be 'long and difficult' (DW, 28 OCT)

Israeli Prime Minister Benjamin Netanyahu has said fighting inside the Gaza Strip will be "long and difficult," with Israeli ground forces now operating in the Palenstinian territory for more then 24 hours.

"The war in the [Gaza} Strip will be long and difficult and we are prepared for it," Netanyahu told a news conference after meeting families of hostages held in Gaza.

2. Israel's using widespread GPS tampering to deter Hezbollah's missiles (Politico, 23 OCT, Matt Berg)

Israel is scrambling GPS signals over most of its northern airspace to protect itself from Hezbollah missile strikes — potentially endangering Israeli civilians and commercial aircraft in the process.

A group of researchers at the University of Texas at Austin who have tracked GPS signals in the region for years noticed a strange pattern emerging after the Hamas militant group's surprise attack on Oct. 7: Planes flying near the Mediterranean sea briefly disappeared from sight over many parts of Israel.

That's a sign of "GPS spoofing," a technique in which the location of an airplane — or precision-guided missile — or any object that uses GPS is rendered inaccurate.

3. **Hamas-linked app offers window into cyber infrastructure, possible links to Iran (CyberScoop, 19 OCT, AJ Vicens)**

An Android app designed to share updates for supporters of Hamas' military wing is linked to a long-running Hamas-linked cyber espionage group, according to analysis by the security firm Record Future that sheds light on how the group is attempting to spread its messaging amid ongoing fighting with Israel.

The app in question was posted to a Telegram channel associated with the Izz al-Din al-Qassam Brigades four days after fighting began and was configured to communicate with a news site linked to the group.

Back to Table of Contents