U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

01-15 November 2023

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

Table of Contents

3. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 10, 2023 - 10 NOV
4. FBI Highlights Emerging Initial Access Methods Used by Ransomware Groups - 08 NOV
5. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 2, 2023 - 02 NOV

Israel-Hamas Conflict

1. The Drive Israel-Gaza Update
2. Institute for The Study of War Iran Update:
3. Israeli Raid On Gaza's Largest Hospital Underway - 14 NOV
4. What will happen to Gaza after the Israel-Hamas conflict? - 14 NOV
5. Hamas militants had prepared for a 'second phase' of terrorist attacks in Israel, report says - 13 NOV
6. A Hamas leader pronounced dead in 2014 has been living in underground tunnels and masterminded the October 7 attacks, Israeli intel says - 12 NOV
7. Beyond the Front Lines: How the Israel-Hamas War Impacts the Cybersecurity Industry - 10 NOV
8. The mastermind of Hamas' October 7 terrorist attacks is cornered in a bunker, says Israel - 10 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. If the West Cuts Aid to Ukraine, Russia Will Win, If the West Leans in, Ukraine Can Win – 15 NOV
5. Resistance fighters blew up a Russian military headquarters and killed 3 officers in occupied territory, Ukraine says - 13 NOV
6. Russia's Military Restructuring And Expansion Hindered By The Ukraine War - 12 NOV
7. Russia and Ukraine are building up huge armies, but they both have the same problem with using them in battle - 12 NOV

Cyber

1. **Australian Intelligence Report Identifies China as Major Backer of Cyber Crime (VOA News, 15 NOV, Phil Mercer)**

   Australia's digital spy agency has identified China as the major backer of serious hacking against Australian companies and critical infrastructure.

   The Australian Signals Directorate, or ASD, Wednesday released its cyber threat report for the past year.

   It stated that serious attacks on federal government agencies or critical infrastructure that led to the "extensive compromise" of sensitive data have increased from two to five in the past year.

2. **Ransomware Group Leaks Files Allegedly Stolen From Boeing (SecurityWeek, 13 NOV, Eduard Kovacs)**

   The notorious LockBit ransomware group has leaked gigabytes of files allegedly stolen from the systems of aerospace giant Boeing.

   LockBit recently named Boeing on its leak website, claiming that "a tremendous amount of sensitive data" has been stolen, but later removed the company from its site, saying that negotiations had started.

Back to Table of Contents

   Boeing was later once again added to the LockBit website and data allegedly stolen from its systems has now been leaked, indicating that the company has refused to pay a ransom. Over 40 Gb worth of archive and backup files are available for download.

   Boeing has confirmed that parts of its distribution business have been hit by a cyberattack. The aerospace giant is aware that a ransomware group has released information allegedly taken from its systems, but it has yet to share any information on the scope of the potential data breach.

3. **Sandworm, a Russian Threat Actor, Disrupted Power in Ukraine Via Cyberattack (Tech Republic, 13 NOV, Cedric Pernet)**

   Any company that is strategic could be targeted for the same kind of actions as this cyberattack. Follow these tips to mitigate your company's risk to this cybersecurity threat.

   Mandiant, a cybersecurity company owned by Google, has revealed the details of a 2022 cyberattack run by Russian threat actor Sandworm. The threat actor compromised a Ukrainian critical infrastructure organization to manipulate its operational technology environment, resulting in a power outage that coincided with mass missile strikes. Then, Sandworm tried to cause more disruption and remove all evidence of its operation two days later by deploying and running a variant of the CADDYWIPER malware.

4. **Israel and Ukraine Face Shared Cyber Threats (FDD, 13 NOV)**

   Russia is responsible for recent cyberattacks against Israel, a senior Ukrainian official told Politico on November 10. Victor Zhora, deputy chair of the State Service of Special Communications and Information Protection of Ukraine, explained that Kyiv is seeing the "same tactics as Russia used in Ukraine in the Israeli conflict," including distributed denial of service attacks by the pro-Kremlin KillNet group. Calling Russia a "global evil" that is targeting both countries, Zhora affirmed that Ukraine "consider[s] Israel to be a partner." Zohra made the comments on the sidelines of a cybersecurity conference in Washington, DC.

5. **In Other News: EU Government Surveillance, Rewards for Iranian**

Hackers, Evolution of Chinese Spying (Security Week, 10 Nov)

Noteworthy stories that might have slipped under the radar: EU regulation enables government surveillance, US offering rewards for Iranian hackers, evolution of Chinese spying.

SecurityWeek is publishing a weekly cybersecurity roundup that provides a concise compilation of noteworthy stories that might have slipped under the radar.

We provide a valuable summary of stories that may not warrant an entire article, but are nonetheless important for a comprehensive understanding of the cybersecurity landscape.

Each week, we will curate and present a collection of noteworthy developments, ranging from the latest vulnerability discoveries and emerging attack techniques to significant policy changes and industry reports.

6. US Government Issues Guidance on SBOM Consumption (Security Week, 10 NOV, Ionut Arghire)

CISA, NSA, and ODNI issue new guidance on managing open source software and SBOMs to maintain awareness on software security.

The US cybersecurity agency CISA, the NSA, and the Office of the Director of National Intelligence (ODNI) on Thursday released new guidance for software vendors and suppliers on securing the software supply chain.

Back to Table of Contents

The document (PDF) can help organizations assess their security measures throughout the software lifecycle, including managing open source software (OSS) and software bills of materials (SBOM), and provides recommendations that can be applied across different phases of the software supply chain.

7. Microsoft announces new steps to help protect elections (Microsoft, 07 NOV, Brad Smith)

Over the next 14 months, more than two billion people around the world will have the opportunity to vote in nationwide elections. From India to the European Union, to the United Kingdom and United States, the world's democracies will be shaped by citizens exercising one of their most fundamental rights. But while voters exercise this right, another force is also at work to influence and possibly interfere with the outcomes of these consequential contests.

As detailed in a new threat intelligence assessment published today by Microsoft's Threat Analysis Center (MTAC), the next year may bring unprecedented challenges for the protection of elections. As described in this report, "Protecting Election 2024 from Foreign Malign Influence," the world in 2024 may see multiple authoritarian nation states seek to interfere in electoral processes. And they may combine traditional techniques with AI and other new technologies to threaten the integrity of electoral systems.

8. New MacOS Malware Linked to North Korean Hackers (Security Week, 07 NOV, Kevin Townsend)

New macOS malware, tracked by Jamf as ObjCShellz, is likely being used by North Korean hackers to target crypto exchanges

A new macOS malware probably used by North Korean hackers to target crypto exchanges has been found by security firm Jamf. The group behind the malware is thought to be the same group behind the recently reported KandyKorn malware.

In its report on KandyKorn, Kaspersky describes the group as 'Lazarus', an overarching term for North Korean hackers. Jamf describes this group as BlueNoroff, a specific group within Lazarus that is "financially motivated, frequently targeting cryptocurrency exchanges, venture capital firms, and banks."

9. **North Korean Hackers Use New 'KandyKorn' macOS Malware in Attacks (SecurityWeek, 03 NOV, Ionut Arghire)**

The notorious North Korean hacking group Lazarus has used new macOS and Windows malware in recent attacks, security researchers warn.

In one of the attacks, blockchain engineers at a cryptocurrency exchange platform were targeted with a Python application designed to provide initial access, ultimately resulting in the loading of binaries in memory.

As part of the attack, Lazarus impersonated members of the blockchain community on a public Discord channel, convincing the victim to download an archive containing malicious code.

10. **A new world of security: Microsoft's Secure Future Initiative (Microsoft, 02 NOV, Brad Smith)**

The past year has brought to the world an almost unparalleled and diverse array of technological change. Advances in artificial intelligence are accelerating innovation and reshaping the way societies interact and operate. At the same time, cybercriminals and nation-state attackers have unleashed opposing initiatives and innovations that threaten security and stability in communities and countries around the world.

In recent months, we've concluded within Microsoft that the increasing speed, scale, and sophistication of cyberattacks call for a new response. Therefore, we're launching today across the company a new initiative to pursue our next generation of cybersecurity protection – what we're calling our Secure Future Initiative (SFI).

.

Back to Table of Contents

Electronic Warfare

1. **Ukrainian Forces neutralize 2 key Russian Borisoglebsk electronic warfare systems in Donetsk Region (Army Recognition, 10 NOV)**

   Ukrainian Armed Forces have successfully targeted and destroyed two critical Russian RB-301B Borisoglebsk-2 systems near Novopetrykivka in the Donetsk region. The operation, announced on November 09, 2023, through a video released by the 58th Infantry Brigade on their official Facebook account, marks a notable achievement against Russian electronic capabilities.

2. **Soldiers' winning idea hides friendly radio calls in a sea of noise (Defense One, 06 NOV, Jennifer Hlad)**

   A U.S. Army unit was preparing to go to the National Training Center last November when they discovered a problem: an adversary with electronic-warfare gear could “easily identify people talking on their radios…so they needed a way to counteract that.”

   Lacking time to fix the problem, the unit handed it off to the Third Infantry Division’s Marne Innovation Team, said Capt. Chris Flournoy, one of the team’s innovation officers. Staff Sgt. Michael Holloway, an electronic warfare soldier, came up with a solution: a low-cost decoy emitter.

Back to Table of Contents

3. **Ukraine destroys Russian Leer-2 electronic warfare system (Army Recognition, 06 NOV,)**

   On November 2, 2023, the Ukrainian Armed Forces successfully targeted and destroyed a Russian electronic warfare system known as "Leer-2" in the Donetsk region.

   The operation was carried out by the 3rd Regiment of Special Operations Forces (SOF) during reconnaissance activities in the direction of Donetsk. The tactical group "Medoid" identified the enemy's "Leer-2" complex. After tracking the movement of the equipment and waiting for it to stop, operators of the reconnaissance complex Shark directed Ukrainian artillery to strike the target.

4. **The significance of electronic warfare in the cyber domain (Electronics 360, 03 NOV, N. Mughees)**

   The cyber domain has become increasingly important within military and security contexts. It refers to the online world where all the digital conversations and meetings take place, and includes all the computers, networks and other electronic devices that work together to provide communication and a wide range of digital services. Electronic warfare capabilities are increasingly computerized and linked, including everything from communication networks to command-and-control systems to vital infrastructure. Because of this mutual dependence, interruptions or assaults in the cyber realm might have consequences in the electronic warfare domain, and vice versa.

5. **After watching Russia's and Ukraine's electronic warriors battle it out, the US military wants to 'dial up' up its own 'jamming power' (Business Insider, 30 OCT, Michael Peck)**

   Electronic warfare has become a major factor in the Ukraine war, with each side using it to jam the other's radios and radars and to knock their drones out of the sky.

   The value of electronic-warfare capabilities is not a new lesson, but the war in Ukraine has shown how quickly those capabilities — and means of countering them — have evolved. That's

why the US Air Force is eager to deploy a new generation of electronic-warfare aircraft and drones.

6. **Ukraine Launches Piranha AVD 360 Electronic Warfare System to Counter Russian Drones (Army Recognition, 03 NOV)**

   Ukraine has developed a new electronic warfare (EW) system, the Piranha AVD 360, designed to protect armored vehicles and soldiers from hostile drone operations. The announcement was made by the Ukrainian Deputy Prime Minister responsible for Innovation, Education, Science, and Technological Development - Minister of Digital Transformation, Mykhailo Fedorov.

7. **A New Micro Kind Of Electronic Warfare May Be Unfolding In Gaza (Forbes, 03 NOV, Eric Tegler)**

   Electronic warfare has long been an exercise in combating adversaries with powerful equipment. In Gaza, thwarting tiny, low power drones and countermeasures will be key.

   While terrorist organizations like Hamas have historically been regarded as uninterested in and incapable of prosecuting electronic warfare (EW), their inclinations and capabilities have changed markedly in the last eight years or so.

Back to Table of Contents

Information Advantage

1. **[10 AI terms everyone should know](#) (Microsoft, Susanna Ray)**

   The term “AI” has ben used in computer science since the 1950s, but most people outside the industry didn’t start talking about it until the end of 2022. That’s because recent advances in machine learning led to big breakthroughs that are beginning to have a profound impact on nearly every aspect of our lives. We ‘re here to help break down some of the buzzwords so you can better understand AI terms and be part of the global conversation.

2. **[South Korea exposes huge Chinese disinformation campaign involving 38 news websites](#) (Independent, 15 NOV, Shweta Sharma)**

   South Korea’s intelligence agency says two Chinese firms involved in creating fake wesbites.

   South Korea’s intelligence agency said it has identified 38 Korean-language news websites that are suspected of being run by Chinese companies with some allegedly spreading pro-China and anti-US content.

   South Korea’s National Intelligence Service (NIS) said two Chinese public relations firms were involved in creating fake websites in the country masquerading as members of the Korea Digital News Association.

   It said these fake websites used domain names similar to companies in South Korea and published articles from local news outlets without permission.

[Back to Table of Contents](#)

3. **[UK cybersecurity center says 'deepfakes' and other AI tools pose a threat to the next election](#) (Daily Mail, 14 NOV, AP)**

   Britain´s cybersecurity agency said Tuesday that artificial intelligence poses a threat to the country´s next national election, and cyberattacks by hostile countries and their proxies are proliferating and getting harder to track.

   The National Cyber Security Center said "this year has seen the emergence of state-aligned actors as a new cyber threat to critical national infrastructure" such as power, water and internet networks.

4. **[Information disorder in the Israel-Hamas war highlights shifts in the fight against online misinformation](#) (ISD, 09 NOV, Jared Holt)**

   Swathes of US news-seekers have turned to social media influencers for information about the Israel-Hamas war, hoping to find voices of clarity and information they can trust in addition to or apart from traditional news outlets. But those searching for news on social media platforms will find a cruel battlefield of another kind.

   A motley crew of news amateurs, grassroots commentators, and bad actors lead charges across an information combat zone that ISD analysts have found to include pro-terrorist content that is illegal and violent, violent graphic imagery that’s accessible to children, and state actors that exploit the crisis for ulterior agendas. Rhetoric conveying antisemitic and anti-Muslim attitudes has snowballed on platforms, mirroring surges in offline hate.

5. **[India Opposes China’s Belt and Road Initiative](#) (U.S. Army Asian Studies Detachment, 08 NOV)**

   India’s External Affairs Ministry spokesperson Arindam Bagchi said that China did not invite India for the 10th anniversary of the Belt and Road Forum held in Beijing. Bagchi reiterated that India is opposing the Belt and Road Initiative (BRI) because it lacks respect for Indian sovereignty and territorial integrity.

6. **Pentagon debuts new data and AI strategy after Biden's executive order (C4ISR Net, 02 NOV, Noah Robertson & Colin Demarest)**

The U.S. Department of Defense released a new strategy on its use of data analytics and artificial intelligence as it pushes for additional investment in AI, advanced pattern recognition and autonomous technologies including drones.

The document is a more mature version of a blueprint first published in 2018, in which the Pentagon predicted AI would "transform every industry" and impact all facets of national security. It takes into account AI's significant growth in the defense industrial base, according to Chief Digital and AI Officer Craig Martell.

Back to Table of Contents

Signal

1. **[How To Align Passwordless With Zero Trust](#) (Forbes, 10 NOV, Michael Engle)**

   Every day, more and more new malware threats appear—and organizations worldwide scramble to react. The situation is chaotic, if not entirely overwhelming.

   Of course, part of a good cybersecurity defense is detecting and blocking dangerous payloads. Yet, often overlooked is the role of identity verification, which goes beyond authentication, in achieving zero-trust security. Knowing who is using applications—and whether they are authorized at any given moment—is at the heart of protecting a business.

   Passwords have run their course. They are the weakest link in the cyber world.

2. **[Blu Wireless develops mobile V-band mmWave radio](#) (Janes, 09 NOV, Rakend P.)**

   PhantomBlu from Blu Wireless is the first mobile V-band self-forming and self-healing mesh network radio, utilising millimeter-wave (mmWave) technology to provide multi-gigabit per second network throughput with lowest probability of detection.

[Back to Table of Contents](#)

   A V-band radio operating in 57–71GHz frequency band, PhantomBlu successfully completed live trials aboard moving platforms with a speed of 300 km/h, Macy Summers, president and CEO of Blu Wireless Inc, told Janes.

   The system trials were undertaken by various military organisations including the US Department of Defense (DoD) and the British and French militaries. “Initial productions are expected in 2024–25 and full rate productions [will] likely start after that,” Summers said.

   “The system creates automated wireless network and achieved up to 3Gbps at 500 m, 1.0 Gbpsat 1.5 km, and up to 100 Mbpsthroughput at 4 km of distance,” Summers said. Such high-speed data communication makes the system suitable for tactical communication networks' requirements for transferring voice, data, and video in Denied, Disrupted, Intermittent, or Limited (DDIL) bandwidth environments.

3. **[Scientist Claims Quantum RSA-2048 Encryption Cracking Breakthrough](#) (Tom’s Hardware, 03 NOV, Mark Tyson)**

   Researcher says that a smartphone can now crack RSA-2048

   A commercial smartphone or Linux computer can be used to crack RSA-2048 encryption, according to a prominent research scientist. Dr Ed Gerck is preparing a research paper with the details but couldn’t hold off from bragging about his incredible quantum computing achievement (if true) on his LinkedIn profile. Let us be clear: the claims seem spurious, but it should be recognized that the world isn’t ready for an off-the-shelf system that can crack RSA-2048, as major firms, organizations, and governments haven’t yet transitioned to encryption tech that is secured for the post-quantum era.

4. **[Microsoft is overhauling its software security after major Azure cloud attacks](#) (The Verge, 02 NOV, Tom Warren)**

   Microsoft is getting ready to use AI and automation to identify security vulnerabilities and respond faster to software flaws.
   Microsoft has had a rough few years of cybersecurity incidents. It found itself at the center of the SolarWinds attack nearly three years ago, one of the most sophisticated cybersecurity attacks we’ve ever seen. Then, 30,000 organizations’ email servers were hacked in 2021 thanks to a Microsoft Exchange Server flaw. If that weren’t enough already, Chinese hackers

breached US government emails via a Microsoft cloud exploit earlier this year.

5. **Starting your journey to become quantum-safe (Microsoft, 01 NOV, Michal Braverman-Blumenstyk)**

There's no doubt we are living through a time of rapid technological change. Advances in ubiquitous computing and ambient intelligence transform nearly every aspect of work and life. As the world moves forward with new advancements and distributed technologies, so too does the need to understand the potential security risks. At Microsoft, our mission has always been focused on keeping our customers' and partners' information and data safe and secure, and this is why we're committed to advancing encryption solutions, in order to enable responsible use of new technologies such as AI and quantum computing. As one important example, while scaled quantum computing will help solve some of our toughest problems, like helping us discover new ways of addressing climate change and food scarcity, its development may also create a new set of security challenges and in turn require new encryption standards. As this future quickly approaches, how can we ensure that we reap the benefits of quantum computing while remaining safe in a post-quantum world?

Back to Table of Contents

Items of Interest

1. **Xi, Biden arrive in San Francisco for APEC talks (DW, 15 NOV)**

   US President Joe Biden and China's Xi Jinping have both arrived in San Francisco, California, where they will hold one-on-one talks later on Wednesday.

   The presidents of the world's strongest economies are set to meetat an undisclosed venue amid the annual Asia Pacific Economic Cooperation summit (APEC) in the city.

   It's Xi's first trip to the US in any capacity since 2017, and it will be the two leaders' first in-person, one-on-one talks since last November.

2. **Drone attacks on US troops in Middle East rise to 55 in under a month (C4ISR Net, 14 NOV, Meghann Myers)**

   The number of attacks on U.S. troops in Iraq and Syria has climbed to 55 as of Monday, a Pentagon spokeswoman told reporters during a briefing, resulting in 59 injuries counted so far.

   The attacks, 27 in Iraq and 28 in Syria, are part of an escalation in strikes by Iranian-backed militias in those countries that has steadily continued since Oct. 17.

3. **CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 10, 2023 (ISW, 10 NOV, Matthew Sperzel, Daniel Shats, and Ian Jones)**

Back to Table of Contents

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

   Key Takeaways

4. The negotiations between the Taiwan People's Party (TPP) and Kuomintang (KMT) about forming a joint presidential ticket have stalled.
5. The PRC instigated two aggressive encounters with US-allied militaries in the South China Sea between October 29 and November 6.
6. The PRC is using the Israel-Palestinian conflict to bolster its image as a fair, responsible broker in contrast to the "biased" United States.
7. The PRC extended a naval deployment in the Middle East during the Israel-Hamas war, possibly as a means of increasing its influence in the Middle East.

8. **FBI Highlights Emerging Initial Access Methods Used by Ransomware Groups (SecurityWeek, 08 NOV, Ionut Arghire)**

   The FBI has released a fresh warning on ransomware operators compromising third-party vendors and services to abuse them for initial access to victim environments.

   Threat actors have been observed exploiting vulnerabilities in vendor-controlled remote access to servers and abusing legitimate system management tools to elevate permissions in victim organizations' networks, the Bureau says.

   According to the FBI, between 2022 and 2023, multiple ransomware attacks abused third-party gaming vendors to compromise the servers of small and tribal casinos and encrypt personally identifiable information (PII).

   Furthermore, the agency warns of callback-phishing data theft and extortion attacks conducted by the Silent Ransom Group (SRG), which is also tracked as Luna Moth.

   The attackers initially send the victim a phishing message, typically claiming to be related to

pending charges on the victim's account, requesting them to call a specified number.

6. CHINA-TAIWAN WEEKLY UPDATE, NOVEMBER 2, 2023 (ISW, 02 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 Kuomintang (KMT) and Taiwan People's Party (TPP) agreed to cooperation in the legislative elections and will likely form a joint presidential ticket before the January 13 presidential election.
2) The Chinese Communist Party (CCP) is interfering in the Taiwanese election in order to harm the Democratic Progressive Party's (DPP) chances of victory in the January 13 presidential and legislative elections.
3) High-level meetings between PRC and United States officials are unlikely to mitigate People's Liberation Army (PLA) military coercion targeting Taiwan.
4) The PRC is shaping the information environment to blame the United States for potential future geopolitical incidents in the South China Sea.
5) The PRC is using the Israel-Hamas War to enhance its image as an international mediator in the Middle East.

Back to Table of Contents

Israel-Hamas Conflict

1. The Drive Israel-Gaza Update

Israel-Gaza Situation Report: No Decision Yet To Storm Gaza's Largest Hospital – 13 NOV
Israel-Gaza Situation Report: Calls For Ceasefire Grow – 10 NOV
Israel-Gaza Situation Report: Fighting In North To Pause Daily – 09 NOV
Israel-Gaza Situation Report: Hamas 'Lost Control In The North' IDF Says (Updated) – 08 NOV
Israel-Gaza Situation Report: Push Into Heart Of Gaza City Looms, Civilians Flee – 07 NOV
Israel-Gaza Situation Report: IDF Encircles Gaza City – 05 NOV
Israel-Gaza Situation Report: Hezbollah Not Ready For Full Fight Says Its Leader – 03 NOV
Israel-Gaza Situation Report: Northern Gaza 'Largely' Cut Off From South – 02 NOV
Israel-Gaza Situation Report: Sa'ar 5 Corvettes Moved To Red Sea – 01 NOV

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.

Back to Table of Contents

Iran Update, November 15, 2023
Iran Update, November 14, 2023
Iran Update, November 13, 2023
Iran Update, November 12, 2023
Iran Update, November 11, 2023
Iran Update, November 10, 2023
Iran Update, November 09, 2023
Iran Update, November 08, 2023
Iran Update, November 07, 2023
Iran Update, November 06, 2023
Iran Update, November 05, 2023
Iran Update, November 04, 2023
Iran Update, November 03, 2023
Iran Update, November 02, 2023
Iran Update, November 01, 2023

4. Israeli Raid On Gaza's Largest Hospital Underway (The Drive/The Warzone, 14 NOV, Howard Altman)

The IDF says a "precise and targeted" operation is taking place out of "operational necessity" at Al Shifa Hospital in Gaza City.

The Israeli Defense Forces (IDF) say they are carrying out a "precise and targeted" operation inside a "specified area" of Al-Shifa Hospital - Gaza's largest. The raid was ordered "based on intelligence information and operational necessity," the IDF said, adding that it is calling for Hamas forces inside the hospital to surrender. Israel has for weeks been hammering their claim that Hamas uses hospitals as key command centers, depots, and safe havens for its fighters. Tunnels under and around the hospitals are also key nodes for their military operations, according to the IDF, something Hamas denies.

5. **[What will happen to Gaza after the Israel-Hamas conflict?] (DW, 14 NOV, Ralph Martin)**

Gaza is fully embroiled in the latest Israel-Hamas conflict. What the future holds for the Palestinian territory once the fighting stops is uncertain. DW looks at three scenarios experts have discussed.

6. **[Hamas militants had prepared for a 'second phase' of terrorist attacks in Israel, report says] (Business Insider, 13 NOV, Tom Porter)**

Hamas militants had prepared for a "second phase" of terrorist attacks in Israel in the hope of provoking a wider conflict in the Middle East, The Washington Post reported.

The Post, citing more than a dozen current and former intelligence and security officials from four Western and Middle Eastern countries, said militants had carried enough provisions and ammunition to last them several days.

7. **[A Hamas leader pronounced dead in 2014 has been living in underground tunnels and masterminded the October 7 attacks, Israeli intel says] (Business Insider, 12 NOV, Alia Shoaib)**

A Hamas leader who was pronounced dead years ago is now believed to be alive and to have helped mastermind the October 7 attacks, Israeli intelligence says, The Telegraph reported.

Mohammed Sinwar, the younger brother of Hamas' leader in Gaza Yahya Sinwar, was pronounced dead by the militant group in 2014, with the group even releasing an image of him lying in a blood-soaked bed.

However, Israeli spies are now said to believe that his death was faked and that he had been living in Hamas' "spider's web" of tunnels under Gaza for years, sources close to Israeli intelligence said.

[Back to Table of Contents]

8. **[Beyond the Front Lines: How the Israel-Hamas War Impacts the Cybersecurity Industry] (Security Week, 10 NOV, Karolina Hird)**

The Russian Ministry of Defense (MoD) is pursuing three simultaneous and overlapping force generation efforts as it seeks to manage short- to medium-term requirements in Ukraine while also pursuing long-term restructuring to prepare for a potential future large-scale conventional war against NATO. Russian Defense Minister Sergei Shoigu and Chief of the General Staff Army General Valery Gerasimov have explicitly framed Russia's announced long-term force restructuring as increasing conventional capabilities against NATO.[1] The Russian MoD is also creating new formations intended as reinforcements for Russia's war in Ukraine separate from the peacetime Russian force structure, specifically the several new formations reportedly forming entirely in occupied areas of Ukraine and under the command and control of operationalized "groupings of forces" in Ukraine rather than under existing Russian military districts. The MoD appears to be undermining its long-term restructuring effort, however, by rushing some new formations - which were likely intended to form a strategic reserve or be the basis of long-term force restructuring – as rapid reinforcements to Russian forces in Ukraine. The Russian MoD's use of ongoing force structure changes to rush newly created and understrength formations to Ukraine will likely impede the accomplishment of the parallel objective of restructuring Russian ground forces to orient on conventional warfare with NATO as the main adversary.

6. **[The mastermind of Hamas' October 7 terrorist attacks is cornered in a bunker, says Israel] (Business Insider, 10 NOV, Rebecca Rommen)**

Israeli forces have Hamas' top leader surrounded in the ruins of Gaza City, Israel's defense

minister said.

Yahya Sinwar, 61, is considered to be the mastermind behind the October 7 terrorist attacks on southern Israel that left 1,400 people dead and more than 240 hostages abducted to Gaza.

The Hamas government and its offices are based in Gaza City, which is currently under siege by Israeli forces.

Back to Table of Contents

Russia-Ukraine Conflict

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

   Russia-Ukraine Situation Report, 15 November 2023
   Russia-Ukraine Situation Report, 14 November 2023
   Russia-Ukraine Situation Report, 13 November 2023
   Russia-Ukraine Situation Report, 09 November 2023
   Russia-Ukraine Situation Report, 07 November 2023
   Russia-Ukraine Situation Report, 02 November 2023

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

   Ukraine Situation Report: Advance Across Dnipro River Deepens – 14 NOV
   Ukraine Situation Report: U.S. Aid To Kyiv Slows – 10 NOV
   Ukraine Situation Report: Dutch F-16s For Ukrainian Training Arrive In Romania – 07 NOV
   Ukraine Situation Report: This May Be Our First Image Of An M1 Abrams In-Country – 06 NOV
   Ukraine Situation Report: M1 Abrams-Based Mine Clearing Vehicle Appears In-Country – 03 NOV
   Ukraine Situation Report: 1M North Korean Artillery Rounds Sent To Russia, Seoul Says – 01 NOV

3. **Institute for The Study of War**

Back to Table of Contents

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

4. **If The West Cuts Aid To Ukraine, Russia Will Win. If The West Leans In, Ukraine Can Win. (ISW, 15 NOV, Frederick W. Kagan)**

   The positional war in Ukraine is not a stable stalemate. It is not the result of fundamental realities in modern warfare that can only be changed with a technological or tactical revolution, as was the First World War's stalemate. Neither does it rest on a permanent parity in military capacity between Russia and Ukraine that will continue indefinitely regardless of Western support to Kyiv. It results, on the contrary, from self-imposed limitations on the technologies the West has been willing to provide Ukraine and constraints on the Russian defense industrial base largely stemming from Russian President Vladimir Putin's unwillingness so far to commit

Russia fully to this war. The current balance is thus, in fact, highly unstable, and could readily be tipped in either direction by decisions made in the West.

5. **Resistance fighters blew up a Russian military headquarters and killed 3 officers in occupied territory, Ukraine says (Business Insider, 13 NOV, Sinéad Baker)**

   Resistance fighters set off an explosion in a Russian headquarters building that killed at least three national guard officers, Ukrainian intelligence said.

   The explosion, in a building in the Russia-occupied city of Melitopol on Saturday, was set off by representatives of a local resistance movement, according to an update from the Main Directorate of Intelligence of Ukraine, or GUR, on Sunday.

   The attack took place during a meeting between the Rosgvardia, Russia's national guard, and the FSB, Russia's security service, the GUR said.

6. **Russia's Military Restructuring And Expansion Hindered By The Ukraine War (ISW, 12 NOV, Karolina Hird)**

   The Russian Ministry of Defense (MoD) is pursuing three simultaneous and overlapping force generation efforts as it seeks to manage short- to medium-term requirements in Ukraine while also pursuing long-term restructuring to prepare for a potential future large-scale conventional war against NATO. Russian Defense Minister Sergei Shoigu and Chief of the General Staff Army General Valery Gerasimov have explicitly framed Russia's announced long-term force restructuring as increasing conventional capabilities against NATO. The Russian MoD is also creating new formations intended as reinforcements for Russia's war in Ukraine separate from the peacetime Russian force structure, specifically the several new formations reportedly forming entirely in occupied areas of Ukraine and under the command and control of operationalized "groupings of forces" in Ukraine rather than under existing Russian military districts. The MoD appears to be undermining its long-term restructuring effort, however, by rushing some new formations - which were likely intended to form a strategic reserve or be the basis of long-term force restructuring – as rapid reinforcements to Russian forces in Ukraine. The Russian MoD's use of ongoing force structure changes to rush newly created and understrength formations to Ukraine will likely impede the accomplishment of the parallel objective of restructuring Russian ground forces to orient on conventional warfare with NATO as the main adversary.

Back to Table of Contents

7. **Russia and Ukraine are building up huge armies, but they both have the same problem with using them in battle (Business Insider, 12 NOV, Michael Peck)**

   The difference between an army and a well-armed mob often comes down to the presence of good junior officers. The same applies to staff work, which ensures combat operations are properly planned, synchronized, and supplied.

   Russia and Ukraine are both learning that lesson as they field newly formed armies with masses of inexperienced soldiers who need cadres of capable and experienced officers in order to be effective.