Cyber Center of Excellence

Unclassified Threat Read Book

01-29 February 2024

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

Table of Contents

Cyber

Electronic Warfare

Information Advantage

Signal

Back to Table of Contents

Items of Interest

13. China-Taiwan Weekly Update, February 2, 2023 - 02 FEB
14. Iran begins building 4 more nuclear power plants - 01 FEB

US/IRAN

1. Hamas and Iran in Nigeria; Turkey Capitalizes on Horn of Africa Tensions – 23 FEB
2. Iranian-Backed Militia Claims New Attack On U.S. Base In Syria - 05 FEB
3. U.S. Plans Further Action Against Iran's Militia Allies - 04 FEB
4. U.S. Airstrikes Obliterated Munitions Storage Compound In Syria - 03 FEB
5. Everything We Know About The Aftermath Of Last Night's Airstrikes - 03 FEB
6. Over 85 Targets Hit In U.S. Retaliation Strikes Against Iranian Proxies, IRGC (Updated) - 02 FEB
7. Iranian Proxies Scatter Ahead Of Looming U.S. Retaliation Strikes - 01 FEB

Israel-Hamas Conflict

1. Institute for The Study of War Iran Update
2. A deal between Isreal and Hamas appears to be taking shape. What would it look like? – 28 FEB
3. Palestinians in Rafah ask where they should go - 14 FEB
4. Israeli Forces Discover Hamas Leader Yahya Sinwar's Hidden Tunnel - 13 FEB
5. Israel prepares full-scale ground offensive in Gaza's Rafah - 13 Feb
6. Live updates | Israel's evacuation orders cover ⅔ of Gaza, leaving Palestinians crammed in Rafah - 06 FEB

Back to Table of Contents

Houthis Conflict

1. IRAN: Enabling Houthi Attacks Across the Middle East - Feb
2. Rocket fire reported off Yemen in Red Sea in a new suspected attack by Houthi rebels – 28 FEB
3. Houthi Missile Strike Results In Crew Abandoning Damaged Cargo Ship – 19 FEB
4. Houthi Rebels Target Commercial Ship Carrying Corn to Iran: A Dangerous Escalation in the Red Sea - 14 FEB
5. 'America Is the Mothe of Terrorism'. Why the Houthis' New Slogan Is Important to Understanding the Middle East – 13 FEB
6. Suspected drones sed by Yemen's Houthi rebels attack 2 more ships in Mideast waters – 06 FEB
7. Military experts evaluate the U.S. response in the MidEast – 05 FEB

Russia-Ukraine Conflict

1. The Warzone Russia-Ukraine Situation Report
2. Institute for the Study of War
3. Putin Warns that sending Western troops to Ukraine risks a global nuclear conflict – 29 FEB
4. Ukraine's First M1 Abrams Tank Loss Appears To Have Occurred – 26 FEB
5. Another One Of Russia's Prized A-50 Radar Planes Shot Down, Ukraine Claims – 26 FEB
6. Ukraine decodes Russian 'carrots' and 'tea bags' chatter to save lives - 14 FEB
7. Ukraine's 6000+ EW 'Acoustic Sensors' To Counter Russia's Kamikaze UAVs Get US Military Interested – 13 FEB
8. Ukraine: Is Europe starting to change its strategy? – 13 FEB

Back to Table of Contents

Cyber

1. **FBI: Russian hackers are using these routers as part of their covert cyber attacks (IT Pro, 28 FEB, Steve Ranger)**

   Russia's state-backed hackers are using compromised routers to carry out their covert cyber attacks against governments and organizations worldwide.

   This warning, issued by the FBI, NSA and US Cyber Command, said that the group linked with Russia military intelligence, known to security companies as APT28 or Fancy Bear, has used compromised EdgeRouters to steal, and host spear-phishing landing pages and custom tools.

2. **CISA warns that malicious actors are targeting cloud infrastructure (Security Magazine, 28 FEB, Security Staff)**

   The Cybersecurity & Infrastructure Security Agency (CISA) recently announced that cyberattackers are evolving techniques to gain initial cloud access. The advisory discusses the recent adjustments made by the group APT29, also known as the Dukes, Cozy Bear or Midnight Blizzard.

3. **With 41% Cyber Attacks Linked To China – Hacking Buck Passes From Washington To Beijing To New Delhi (The EurAsian Times, 26 FEB, KN Pandita)**

   China has often blamed India for cyber attacks. The latest blame game by China is a ruse to deflect the accusations leveled against it by the U.S., which has gone on record to point out that China was getting ready to create havoc by taking down the power grid, oil pipelines, and water systems in the event of a war over Taiwan.

Back to Table of Contents

4. **An Online Dump of Chinese Hacking Documents Offers a Rare Window Into Pervasive State Surveillance (Associated Press, 22 FEB, Frank Bajak & Dake Kang)**

   Chinese police are investigating an unauthorized and highly unusual online dump of documents from a private security contractor linked to the nation's top policing agency and other parts of its government — a trove that catalogs apparent hacking activity and tools to spy on both Chinese and foreigners.

5. **Ransomware Declines as InfoStealers and AI Threats Gain Ground: IBM X-Force (Security Week, 21 FEB, Kevin Townsend)**

   The ransomware threat is declining as actors pivot to infostealing, according to a new report from IBM X-Force, which also says that attacks on cloud services and critical infrastructures are growing – and the AI threat is looming.

6. **Russian Cyberspies Exploit Roundcube Flaws Against European Governments**

   A Russian cyberespionage group has been observed exploiting vulnerable Roundcube webmail servers in attacks against European government, military, and critical infrastructure entities, cybersecurity firm Recorded Future reports.

7. **Microsoft says US rivals are beginning to use generative AI in offensive cyber operations (AP News, 14 FEB, Frank Bajak)**

Microsoft said Wednesday that U.S. adversaries — chiefly Iran and North Korea and to a lesser extent Russia and China — are beginning to use its generative artificial intelligence to mount or organize offensive cyber operations.

The technology giant and business partner OpenAI said they had jointly detected and disrupted the malicious cyber actors' use of their AI technologies — shutting down their accounts.

8. **Staying ahead of threat actors in the age of AI (Microsoft, 14 FEB, Microsoft Threat Intelligence)**

Over the last year, the speed, scale, and sophistication of attacks has increased alongside the rapid development and adoption of AI. Defenders are only beginning to recognize and apply the power of generative AI to shift the cybersecurity balance in their favor and keep ahead of adversaries. At the same time, it is also important for us to understand how AI can be potentially misused in the hands of threat actors. In collaboration with OpenAI, today we are publishing research on emerging threats in the age of AI, focusing on identified activity associated with known threat actors, including prompt-injections, attempted misuse of large language models (LLM), and fraud. Our analysis of the current use of LLM technology by threat actors revealed behaviors consistent with attackers using AI as another productivity tool on the offensive landscape. You can read OpenAI's blog on the research here. Microsoft and OpenAI have not yet observed particularly novel or unique AI-enabled attack or abuse techniques resulting from threat actors' usage of AI. However, Microsoft and our partners continue to study this landscape closely.

Back to Table of Contents

9. **Cyber Signals: Navigating cyberthreats and strengthening defenses in the era of AI (Microsoft, 14 FEB, Vasu Jakkal)**

The world of cybersecurity is undergoing a massive transformation. AI is at the forefront of this change, and has the potential to empower organizations to defeat cyberattacks at machine speed, address the cyber talent shortage, and drive innovation and efficiency in cybersecurity. However, adversaries can use AI as part of their exploits, and it's never been more critical for us to both secure our world using AI and secure AI for our world.

10. **The Cyberlaw Podcast: Serious Threats, Unserious Responses (Lawfare, 06 FEB, Stewart Baker)**

It was a week of serious cybersecurity incidents paired with unimpressive responses. As Melanie Teplinsky reminds us, the U.S. government has been agitated for months about China's apparent strategic decision to hold U.S. infrastructure hostage to cyberattack in a crisis. Now the government has struck back at Volt Typhoon, the Chinese threat actor pursuing that strategy. It claimed recently to have disrupted a Volt Typhoon botnet by taking over a batch of compromised routers. Andrew Adams explains how the takeover was managed through the court system. It was a lot of work, and there is reason to doubt the effectiveness of the effort. The compromised routers can be re-compromised if they are turned off and on again. And the only ones that were fixed by the U.S. seizure are within U.S. jurisdiction, leaving open the possibility of DDOS attacks from abroad. And, really, how vulnerable is our critical infrastructure to DDOS attack? I argue that there's a serious disconnect between the government's hair-on-fire talk about Volt Typhoon and its business-as-usual response.

11. **Iran accelerates cyber ops against Israel from chaotic start (Mirosoft, 06 FEB, Clint Watts)**

    Since Hamas attacked Israel in October 2023, Iranian government-aligned actors have launched a series of cyberattacks and influence operations (IO) intended to help the Hamas cause and weaken Israel and its political allies and business partners. Many of Iran's immediate operations after October 7 were hasty and chaotic – indicating it had little or no coordination with Hamas – but it nevertheless has achieved growing success.

12. **Chinese spies hacked Dutch defense network last year - intelligence agencies (Reuters, 06 FEB, James Pearson & Anthony Deutsch)**

    Chinese state-backed cyber spies gained access to a Dutch military network last year, Dutch intelligence agencies said on Tuesday, calling it part of a trend of Chinese political espionage against the Netherlands and its allies.

13. **China says it opposes and cracks down on all forms of cyberattacks (Reuters, 05 FEB, Neil Jerome Morales)**

    The Chinese government does not tolerate any form of cyberattacks and will not allow any country or individual to engage in such illegal activities using Chinese infrastructure, its embassy in the Philippines said.

14. **China's "Ugly Gorilla" Haunts US; FBI Director Calls World's Largest Hacking Program 'Defining Threat' Of Our Generation (The EurAsian Times, 05 FEB, Vaishali Basu Sharma)**

    In a hearing conducted by the United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party on Jan 31, 2024, Federal Bureau of Investigation (FBI) director Christopher Wray testified on the growing threat of Chinese cyberattacks against the USA. The hearing deliberated on the risks presented by Chinese cyber warfare units.

Back to Table of Contents

15. **Lessons From Israel's Rise as a Cyber Power (Lawfare, 02 FEB, Emily O. Goldman)**

    Review of "Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power" by Charles D. Freilich, Matthew S. Cohen, and Gabi Sabonoi.

16. **Exclusive: US disabled Chinese hacking network targeting critical infrastructure (Reuters, 01 FEB, Chritopher Bing & Karen Freifeld)**

    The U.S. government in recent months launched an operation to fight a pervasive Chinese hacking operation that compromised thousands of internet-connected devices, two Western security officials and a person familiar with the matter said.

    The Justice Department and Federal Bureau of Investigation sought and received legal authorization to remotely disable aspects of the Chinese hacking campaign, the sources told Reuters.

17. **What is Volt Typhoon, the Chinese hacking group targeting US infrastructure? (Reuters, 01 FEB, Raphael Satter & James Pearson)**

    The U.S. Department of Justice and the FBI said on Wednesday they disrupted a sweeping Chinese cyber-spying operation that targeted critical American infrastructure entities and could be used against the United States in a future geopolitical crisis.

    The operation weeded out malicious Chinese software from a network or "botnet" of hundreds of compromised U.S. routers, both agencies said in a statement.

Electronic Warfare

1. **Philippines Accuses China Of EW Attack On It Ships & Using Disruptive Tactics To Jam Vessel’s Signals (The EurAsian Times, 26 FEB, Sakshi Tiwari)**

   Even as the stand-off between the Philippines and China refuses to de-escalate in the South China Sea, there is news that the Philippines Coast Guard has accused its Chinese counterpart of employing disruptive tactics along the disputed territory, which included jamming the tracking system of Filipino vessels.

2. **Russian Army Tests Electronic Weapons In Kaliningrad Oblast (Memri, 21 FEB)**

   On January 16 – 17, 2024, Global Positioning System (GPS) disturbances were recorded over the eastern territory of Poland, in particular covering the Suwałki Gap. Previously, aircraft flying over the Baltic region reported issues in GPS function. Several media outlets attributed the issues to the Russian Army testing electronic weapons. Local media in Russia's Kaliningrad region confirmed the involvement of the Russian Army and mocked the panic caused by the GPS disruptions in Poland.

3. **China claims AI-powered electronic warfare breakthrough (Asia Times, 20 FEB, Gabriel Honrada)**

   Chinese scientists claim to have developed an advanced military surveillance device that could significantly enhance China’s electronic warfare capabilities, a high-tech realm where future conflicts will increasingly be fought and potentially decided, South China Morning Post (SCMP) reported.

Back to Table of Contents

4. **Ukrainian Commercial Sector To Develop Electronic Warfare Systems (Forbes, 16 FEB, Vikram Mittal)**

   On February 10, an address by Ukrainian President Zelenskyy discussed the crucial role that electronic warfare (EW) systems have played in the defense of Ukraine. The use of EW systems is expected to increase as the war continues, resulting in a need for newer, more advanced technology. Consequently, a recent statement from the Ukrainian Digital Transformation Minister, Mykhailo Federov, outlined a new goal to increase Ukrainian production of advanced EW technology by shifting the production of EW systems to the commercial sector.

5. **GPS Spoofing Emerges ‘Biggest Threat’ To Global Civil Aviation; 50+ Cases Reported In Middle East (The EurAsian Times, 14 FEB, Gp Cpt TP Srivastava (Retd))**

   Signal Intelligence (SIGINT) was one of the most potent weapons instrumental in Germany’s defeat during the 2nd World War. British successfully decoded the communication code used for directing U-boats.

6. **Secretive nature of spectrum ops could complicate deterrence (Defense Scoop, 14 FEB, Mark Pomerleau)**

   SAN DIEGO, Calif. — Deterrence against adversaries’ use of capabilities within the electromagnetic spectrum could be difficult to assess given the secretive nature of the environment and the desire to mask high-end jamming tools and waveforms from the enemy, according to a recently retired flag officer.

7. **Detecting Russian 'carrots' and 'tea bags': Ukraine decodes enemy chatter to save lives (AP News, 14 FEB, Samya Kullab)**

As the radio crackles with enemy communications that are hard to decipher, one Russian command rings out clear: "Brew five Chinese tea bags on 38 orange."

A Ukrainian soldier known on the battlefield as Mikhass, who has spent months listening to and analyzing such chatter, is able to quickly decode the gibberish. It means: Prepare five Beijing-made artillery shells and fire them on a specific Ukrainian position in the Serebryansky Forest, which forms the front line in the country's restive northeast.

8. **China Claims Starlink Satellites Now Easy Prey Thanks To 'Tech Breakthrough' In Electronic Warfare (The EurAsian Times, 06 FEB, Ashish Dangwal)**

Chinese researchers, for the very first time, have reportedly managed to monitor & analyze the complete electromagnetic spectrum in real time. This is another set of extraordinary claims emerging from Beijing regarding its electronic warfare (EW) capabilities.

9. **Ukraine's 'Backpack Jammers' Are Taking The Fight To Russian FPV Drones Battering Its Military & Infra (The EurAsian Times, 04 FEB, Sakshi Tiwari)**

A Ukrainian company called 'Kvertus,' which manufactures military equipment, has created a portable signal-jamming tool that is small enough to fit in a backpack and can take down Russian drones.

Back to Table of Contents

10. **Unable To 'Destroy' Even A Single HIMARS, Russia Is Jamming Its Missiles With 'Pole Attacks' (The EurAsian Times, 01 FEB, Ritu Sharma)**

The Ukrainian armed forces could face a monumental challenge as it can no longer rely on the US-supplied High Mobility Artillery Rocket System (HIMARS) missiles and Excalibur artillery shells as the Russian electronic warfare (EW) systems are now reportedly leading them astray.

Information Advantage

1. **Captured Ukrainian M2 Bradley Paraded On Russian Propaganda Train (The Warzone, 26 FEB, Joseph Trevithick & Oliver Parken)**

   Crowds of onlookers greeted a captured U.S.-supplied Ukrainian M2A2-ODS-SA Bradley Fighting Vehicle that is now on a rail-bound propaganda tour of Russia. It is an unprecedented and somewhat jarring thing to behold, but one that should come as no surprise.

2. **China 'Attacks' Taiwan With Massive Disinformation Campaign But Anti-China Sentiments Rule The Roost (The EurAsian Times, 26 FEB, NC Bipindra)**

   With the advancement of the internet and social media, there has been phenomenal growth in information sharing. At the same time, it has become easy for the state and non-state actors to fuel disinformation and propaganda as a tool to exert their influence.

3. **Meeting the moment: combating AI deepfakes in elections through today's new tech accord (Microsoft, 16 FEB, Brad Smith)**

   As the months of 2024 unfold, we are all part of an extraordinary year for the history of both democracy and technology. More countries and people will vote for their elected leaders than in any year in human history. At the same time, the development of AI is racing ever faster ahead, offering extraordinary benefits but also enabling bad actors to deceive voters by creating realistic "deepfakes" of candidates and other individuals. The contrast between the promise and peril of new technology has seldom been more striking.

Back to Table of Contents

4. **Combating abusive AI-generated content: a comprehensive approach (Microsoft, 13 FEB, Brad Smith)**

   Each day, millions of people use powerful generative AI tools to supercharge their creative expression. In so many ways, AI will create exciting opportunities for all of us to bring new ideas to life. But, as these new tools come to market from Microsoft and across the tech sector, we must take new steps to ensure these new technologies are resistant to abuse.

5. **Staying ahead of threat actors in the age of AI (Microsoft, 14 FEB, Microsoft Threat Intelligence)**

   Over the last year, the speed, scale, and sophistication of attacks has increased alongside the rapid development and adoption of AI. Defenders are only beginning to recognize and apply the power of generative AI to shift the cybersecurity balance in their favor and keep ahead of adversaries. At the same time, it is also important for us to understand how AI can be potentially misused in the hands of threat actors. In collaboration with OpenAI, today we are publishing research on emerging threats in the age of AI, focusing on identified activity associated with known threat actors, including prompt-injections, attempted misuse of large language models (LLM), and fraud. Our analysis of the current use of LLM technology by threat actors revealed behaviors consistent with attackers using AI as another productivity tool on the offensive landscape. You can read OpenAI's blog on the research here. Microsoft and OpenAI have not yet observed particularly novel or unique AI-enabled attack or abuse techniques resulting from threat actors' usage of AI. However, Microsoft and our partners continue to study this landscape closely.

6. **ChatGPT will digitally tag images generated by DALL-E 3 to help battle misinformation (Engadget, 07 FEB, Richard Lai)**

   In an age where fraudsters are using generative AI to scam money or tarnish one's reputation, tech firms are coming up with methods to help users verify content — at least still images, to begin with. As teased in its 2024 misinformation strategy, OpenAI is now including provenance metadata in images generated with ChatGPT on the web and DALL-E 3 API, with their mobile counterparts receiving the same upgrade by February 12.

7. **Drone Warfare's Terrifying AI-Enabled Next Step Is Imminent (The Warzone, 05 FEB, Tyler Rogoway)**

   The next major advance in the realm of drone warfare is being rapidly incubated and could flood into war zones, and become a huge security problem in non-combat environments too, in the near future.

8. **Intel community tools can speed AI adoption (C4ISR Net, 02 FEB, Stephen J. Townsend)**

   Hamas' heinous attack against Israel. Houthi missile, drone and maritime attacks on Red Sea shipping. Militant drones striking US troops in Jordan, Iraq, and Syria. CCP brinkmanship in the South China Sea.

9. **CCP Adviser Says Beijing Wants Global 'Respect' as Critics Point to State-Backed Influence Operations (NTD, 02 FEB, NTD Newsroom)**

   A new book published by top Chinese economist and state advisor Li Daokui claims that Beijing just wants global respect. He frames the regime's policy-making as anxiety-driven and a kind of defense mode. But critics point to a number of state-backed influence operations, from meddling in Taiwan's recent elections to spreading communist ideology across borders.

10. **Manipulating reality: the intersection of deepfakes and the law (Reuters, 01 FEB, Sara H. Jodka)**

    The use of artificial intelligence ("AI") continues to expand, meaning the use of deepfake technology to create digital fabrications will necessarily follow. Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness using AI techniques. Deepfakes are incredibly realistic, making it difficult to distinguish between real versus manipulated media. This can and has led to impersonation, fraud, blackmail and the spread of misinformation and propaganda.

Back to Table of Contents

.

Signal

1. Cyber Insights 2024: Quantum and the Cryptopocalypse **(Security Week, 27 FEB, Kevin Townsend)**

   Quantum computers are coming and will defeat current PKE encryption. But this cryptopocalypse is not dependent upon quantum computers — it could happen through other means, at any time.

2. US 'Denies' Link-22 Military Datalink To Taiwan To Challenge China's PLA; Sells 'Hackable' Link-16 Instead **(The EurAsian Times, 22 FEB, Parth Satam)**

   Nearly ten months after showing interest in acquiring the US Link 22 advanced battlefield data link system, Taiwan is set to receive its slightly less sophisticated version, the Link 16. The island's foreign ministry said it received official communication from Washington about the possible sale of the technology for a cost of around $75 million.

3. US Air Force, British RAF Enhance 'HF Communication' To Be Able To Reach China's Doorstep At Short Notice **(The Eurasian Times, 20 FEB, Ashish Dangwal)**

   British Royal Air Force Tactical Communicators have recently teamed up with their counterparts from the US Air Force in Germany to sharpen their expertise in high-frequency communications.

Back to Table of Contents

4. US 'Blocks' Chinese Access To Quantum Technology But Report Claims Beijing Ahead In Race? **(The Eurasian Times, 17 FEB, Ashish Dangwal)**

   In recent years, the United States has taken multiple steps to restrict China's access to American quantum technology, an emerging field with potential military applications. However, there are concerns that the US might already be lagging Beijing in the quantum technology race, Chinese media claims.

5. Russian forces buying Starlink satellite units from 'Arab countries' **(Daily Mail, 14 FEB, Paul Farrell)**

   Russian forces are buying Starlink satellite internet terminals in 'Arab countries' for use on the battlefield for a little over $2,000 each, Ukraine's military spy agency said. The Elon Musk-owned service has been vital to Kyiv 's battlefield communications, but Ukrainian officials have said Russian forces are also increasingly relying on it during their nearly two-year-old invasion.

6. Russian Military Now Using Musk's Starlink on Battlefield: Ukraine Intel **(The Defense Post, 12 FEB, Joe Saballa)**

   The Russian military has begun using Elon Musk's satellite internet service Starlink more extensively in some occupied Ukrainian cities, according to a recent report by Kyiv's intelligence agency.

7. **Space Force may launch GPS demonstration satellites to test new tech (C4ISR Net, 09 FEB, Courtney Albon)**

The Space Force is exploring options for expanding the capabilities of its GPS satellites and is asking companies to propose ideas for delivering low-cost demonstration spacecraft to help test new technologies.

Space Systems Command, the service's primary acquisition organization, said in a Feb. 5 notice it is conducting market research to refine its concept for a constellation of GPS demonstration satellites.

8. **Hand-held navigation tool for US Army deemed effective against jamming (C4ISR Net, 07 FEB, Colin Demarest)**

The latest edition of hand-held equipment U.S. Army soldiers can use to navigate and sync maneuvers performed well in the presence of simulated enemy electronic warfare attack, according to the Pentagon's independent weapons tester.

The second-generation Dismounted Assured Positioning, Navigation and Timing System, or DAPS GEN II, is more effective than the legacy Defense Advanced GPS Receiver, or DAGR, amid jamming and spoofing, the Office of the Director of Operational Test and Evaluation said in a report published last month.

9. **The Difficulties of Defining "Secure-by-Design" (Lawfare, 06 FEB, Scott J. Shackelford, Craig Jackson, Scott Russell, Emily K. Adams, Anne Boustead & Christos Makridis)**

Back to Table of Contents

New survey findings and efforts to identify the most impactful security controls underscore the need for an empirical approach to defining—and promoting—security-by-design.

Security-by-design is not a new idea. By some reckoning, it dates back to the 1970s. Various companies, including Microsoft through its Security Development Lifecycle, have tried to implement security-by-design with varying degrees of success during the preceding decades.

Items of Interest

1. **‘Outspending’ US By $200 Billion, China Not Russia Emerges The Biggest Threat To Pentagon In Space (The EurAsian Times, 25 FEB, Prakash Navda)**

   Americans may express their worries over the possibility of Russia using nuclear weapons in space to destabilize their assets, but it is China that seems to pose the real challenge to the U.S. by emerging as the world’s most dominant global space power economically, diplomatically, and militarily by 2045, if not earlier.

2. **China-Taiwan Weekly Update, February 23, 2024 (ISW, 23 FEB, Nils Peterson, Matthew Sperzel, & Daniel Shats)**

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

3. **China-Taiwan Weekly Update, February 15, 2024 (ISW, 15 FEB, Nils Peterson, Matthew Sperzel, & Daniel Shats)**

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

4. **Russia’s “Highly Concerning” Anti-Satellite Super Weapon: What Are The Possibilities? (The Warzone, 15 FEB, Joseph Trevithick)**

   The White House has now formally confirmed that a recently disclosed "serious national security threat" is indeed related to a new anti-satellite capability that Russia is developing. But what could this capability be and why would Russia be perusing it? Let's talk about some possibilities.

Back to Table of Contents

5. **North Korea fires multiple cruise missiles: Seoul (DW, 14 FEB)**

   This is the fifth test of such weapons by Pyongyang since January, according to Seoul’s military, and comes with increasingly aggressive rhetoric by Kim Jong Un.

6. **Threats In Space “Extremely Concerning”: Space Force Boss (The Warzone, 14 FEB, Joseph Trevithick)**

   The U.S. Space Force's top officer says the scale and scope of Russian and Chinese threats to American assets in orbit, including demonstrated abilities to conduct very close proximity operations, is "of paramount concern."

7. **China Eyes Military Base In US’ Front Yard! Experts Call PLA’s Atlantic Outpost Greatest Security Risk (The EurAsian Times, 12 FEB, Ritu Sharma)**

   China’s interest in Africa has got a new hue as the rising Asian giant looks for a naval base in the Atlantic Ocean to increase the reach of its rapidly growing People’s Liberation Army-Navy (PLA Navy).

   The U.S. sees the Chinese presence in the Atlantic, its strategic front yard, as inimical to its security interests.

8. **Israel's AI-Enabled Counter-UAV System: A Game-Changer in Drone Defense (BNN Breaking, 12 FEB, Hedeel Hashem)**

In the conflict-ridden Gaza strip, the Israeli military has deployed an innovative AI-enabled counter-UAV system. This advanced technology, developed by Smart Shooter, can be affixed to various weapons and is accompanied by a friendly drone with a net. The system has already demonstrated remarkable success in neutralizing enemy drones, highlighting the growing importance of AI in modern warfare.

9. **Air Force To Totally Revamp Its Structure To Compete With China (Updated) (The Warzone, 09 FEB, Howard Altman)**

To counter the growing threat especially from China, the Air Force is undergoing major changes in how it operates and is organized. Dubbed "Re-optimization for Great Power Competition," details of the initiative will be unveiled Monday at the Air and Space Forces Warfare Symposium in Denver by Air Force Secretary Frank Kendall and other senior leaders, an Air Force official told The War Zone.

10. **Poland's Plan To Deploy Early Warning Radar Aerostats Moves Forward (The Warzone, 08 FEB, Thomas Newdick)**

Poland has received U.S. government approval to purchase elements of a new airborne early warning system based on an aerostat — a type of uncrewed tethered airship. While many details about the system are still to come, Poland's interest in such a capability is notable in itself, coming after the 2016 cancellation of a similar project — known as JLENS — that would have served the U.S. military.

Back to Table of Contents

11. **China-Taiwan Weekly Update, February 8, 2024 (ISW, 08 FEB, Nils Peterson, Matthew Sperzel, & Daniel Shats)**

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

12. **First-Person-View Drone: Ukraine's Top Commander Calls FVP Kamikaze UAVs 'Massive Threat' To Its Military (The EurAsian Times, 04 FEB, Sakshi Tiwari)**

Valerii Zaluzhnyi, the beleaguered head of Ukraine's army, says that if his country is to prevail in its conflict with Russia, it will have to adjust to the plateauing military support from its allies and put an even greater emphasis on technology to counter Russia.

13. China-Taiwan Weekly Update, February 2, 2023 (ISW, 02 FEB, Nils **Peterson, Matthew Sperzel & Daniel Shats)**

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

14. **Iran begins building 4 more nuclear power plants (AP News, 01 FEB)**

Iran began construction on four more nuclear power plants in the country's south, with expected total capacity of 5,000 megawatts, the official IRNA news agency reported Thursday.

Iran seeks to produce 20,000 megawatts of nuclear energy by 2041.

US/Iran

1. **Hamas and Iran in Nigeria; Turkey Capitalizes on Horn of Africa Tensions (ISW, 23 FEB, Liam Karr)**

   The Africa File will provide weekly analysis and assessments of state and non-state actors' activities in Africa that threaten US personnel and the numerous US national security interests on the continent. US national security interests in Africa include preventing adversaries from using Africa as a base to launch attacks or evade sanctions, ensuring access to strategic minerals and economic markets that are crucial to US supply chains, working with partners to manage potentially destabilizing migration flows to Europe and the US, disrupting transnational crime networks that support illicit markets worldwide, and promoting democracy to prevent the spread of anti-Western authoritarianism. Prominent actors on the African continent that threaten these interests include state powers such as China, Iran, and Russia, as well as non-state groups like the Islamic State and al Qaeda. The Africa File distills open-source information to assess these actors' campaigns and related security and political issues in Africa that could affect their efforts. Irregular editions may be published based on current events.

2. **Iranian-Backed Militia Claims New Attack On U.S. Base In Syria (The Warzone, 05 FEB, Howard Altman)**

   Iranian-backed militias launched a drone attack on a U.S. outpost in eastern Syria Sunday, killing at least six Syrian Democratic Forces (SDF) troops and wounding many others stationed there, a spokesman for the U.S.-backed group said. The drone strike came days after the U.S. dropped 125 munitions on at least 85 targets in Iraq and Syria in the first wave of what is was expected to be a sustained campaign designed to reduce the ability of these militias to carry out such attacks. Regardless, those strikes were in response to the Jan. 28 drone strike on a U.S. base in Jordan that killed three American soldiers and wounded more than 40 others.

Back to Table of Contents

3. **U.S. Plans Further Action Against Iran's Militia Allies (WSJ, 04 FEB, Benoit Faucon & Sune Engel Rasmussen)**

   The U.S. and U.K. launched a fresh wave of strikes against Iran-backed Houthi rebels in Yemen in response to their attacks on international shipping in the Red Sea, as Secretary of State Antony Blinken prepared to head to the Middle East in hopes of brokering a pause in Israel's war in Gaza.

4. **U.S. Airstrikes Obliterated Munitions Storage Compound In Syria (The Warzone, 03 FEB, Tyler Rogoway)**

   The morning after the aerial strikes on Iranian-backed militias and IRGC-related targets in Syria and Iraq there are questions about what the effort achieved, especially as it was telegraphed five days in advance. What was clearly one of the operation's primary targets - located near Dier al-Zour, a hotspot of Iranian-backed militant activity in eastern Syria that sits along the Euphrates River - no longer exists.

5. **Everything We Know About The Aftermath Of Last Night's Airstrikes (The Warzone, 03 FEB, Howard Altman)**

   Iran threatened Wednesday to "decisively respond" to any U.S. attack on the Islamic Republic following President Joe Biden's linking of Tehran to the killing of three U.S. soldiers at a military base in Jordan.

6. **Over 85 Targets Hit In U.S. Retaliation Strikes Against Iranian Proxies, IRGC (Updated) (The Warzone, 02 FEB, Howard Altman, Joseph Trevithick)**

The U.S. has launched its much-anticipated strikes in retaliation for the drone attack that killed three U.S. soldiers in Jordan on Jan. 28, a U.S. official confirmed to The War Zone.

The attacks are the first of many expected to take place.

The strikes were carried out in part by U.S. Air Force B-1B bombers, Politico reported.

7. **Iranian Proxies Scatter Ahead Of Looming U.S. Retaliation Strikes (The Warzone, 01 FEB, Howard Altman)**

Four days after a deadly drone attack on U.S. troops in Jordan, plans are leaking out about the expected American response, sending many of the intended targets scrambling for cover.

Back to Table of Contents

Israel-Hamas Conflict

1. 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, February 29, 2024
Iran Update, February 28, 2024
Iran Update, February 27, 2024
Iran Update, February 26, 2024
Iran Update, February 25, 2024
Iran Update, February 24, 2024
Iran Update, February 23, 2024
Iran Update, February 22, 2024
Iran Update, February 21, 2024
Iran Update, February 20, 2024
Iran Update, February 19, 2024
Iran Update, February 18, 2024
Iran Update, February 17, 2024
Iran Update, February 16, 2024
Iran Update, February 15, 2024
Iran Update, February 14, 2024
Iran Update, February 13, 2024
Iran Update, February 12, 2024
Iran Update, February 11, 2024
Iran Update, February 10, 2024
Iran Update, February 09, 2024
Iran Update, February 08, 2024
Iran Update, February 07, 2024
Iran Update, February 06, 2024
Iran Update, February 05, 2024
Iran Update, February 04, 2024
Iran Update, February 03, 2024
Iran Update, February 02, 2024
Iran Update, February 01, 2024

Back to Table of Contents

2. A deal between Israel and Hamas appears to be taking shape. What would it look like? (AP News, 28 FEB, Samy Magdy & Tia Goldenberg)

Israel and Hamas are inching toward a new deal that would free some of the roughly 130 hostages held in the Gaza Strip in exchange for a weekslong pause in the war, now in its fifth month.

U.S. President Joe Biden says a deal could go into effect as early as Monday, ahead of what is seen as an unofficial deadline — the start of the Muslim holy month of Ramadan, around March 10.

3. **Palestinians in Rafah ask where they should go (DW, 14 FEB, Mohammed Al-Kahlout)**

   About 1.5 million Palestinians are now crammed into Rafah in Gaza's south. As Israel threatens an offensive in the city, they ask where they should go instead.

4. **Israeli Forces Discover Hamas Leader Yahya Sinwar's Hidden Tunnel (BNN Breaking, 13 FEB, Hadeel Hashem)**

   The Israeli military discovered a hidden tunnel used by Yahya Sinwar, the elusive Hamas leader in the Gaza Strip, fueling ongoing tensions in the region. Sinwar is accused of masterminding an attack on October 7 and is currently in hiding. The tunnel is equipped with essential amenities, showcasing the resources at Hamas's disposal.

5. **Israel prepares full-scale ground offensive in Gaza's Rafah (DW, 13 Feb, Benjamin Restle)**

   Four months into its war on Hamas in the Gaza Strip, Israel is about to send troops into Rafah. The enclave's southern city is thought to be home to 1.5 million Palestinians, most of them internally displaced refugees.

6. **Live updates | Israel’s evacuation orders cover ⅔ of Gaza, leaving Palestinians crammed in Rafah (AP News, 06 FEB)**

   Israel’s evacuation orders in the Gaza Strip now cover two-thirds of the territory, or 246 square kilometers (95 square miles), U.N. humanitarian monitors said Tuesday.

   More than half of Gaza’s population of 2.3 million people is now crammed into the town of Rafah on the border with Egypt and surrounding areas, the U.N. Office for the Coordination of Humanitarian Affairs said.

Back to Table of Contents

Houthis Conflict

1. **IRAN: Enabling Houthi Attacks Across the Middle East (DIA, Feb)**

   This product provides a visual comparison of Iranian missiles and weaponized unmanned aerial vehicles (UAVs) and those displayed and employed by Houthis forces in Yemen to attack civilian infrastructure across the region.

2. **Rocket fire reported off Yemen in Red Sea in a new suspected attack by Houthi rebels (AP News, 28 FEB, Jon Gambrell)**

   A rocket exploded late Tuesday night off the side of a ship traveling through the Red Sea off the coast of Yemen, authorities said, the latest suspected attack to be carried out by Yemen's Houthi rebels.

   The attack comes as the Houthis continue a series of assaults at sea over Israel's war on Hamas in the Gaza Strip and as the U.S. and its allies launch airstrikes trying to stop them.

3. **Houthi Missile Strike Results In Crew Abandoning Damaged Cargo Ship (The Warzone, 19 FEB, Joseph Tevithick)**

   ABelize-flagged cargo ship, the Rubymar, is now sitting at anchor without a crew in the vicinity of the Bab al Mandeb Strait after being hit by missiles fired by Iranian-backed Houthi militants in Yemen. The Houthis claim the ship is now at risk of sinking, but the full extent of the damage remains unconfirmed. The Yemeni group also reportedly damaged another ship in a subsequent attack and shot down a U.S. MQ-9 Reaper drone in a series of new incidents in and around the Red Sea.

Back to Table of Contents

4. **Houthi Rebels Target Commercial Ship Carrying Corn to Iran: A Dangerous Escalation in the Red Sea (BNN Breaking, 14 FEB, Aqsa Younas Rana)**

   The Star Iris, a commercial ship carrying corn to Iran, was targeted by Yemen's Houthi rebels in the Red Sea. The attack highlights the growing risks to international shipping in the region. The ongoing conflict in Yemen threatens global trade and stability.

5. **'America Is the Mother of Terrorism': Why the Houthis' New Slogan Is Important for Understanding the Middle East (Z Network, 13 FEB, Sarah G. Phillips)**

   Yemen's Houthi militants continue to disrupt shipping in the Red Sea, undeterred by the intensifying Western airstrikes or the group's re-designation as a "global terrorist" organization. As their attacks have intensified, the group's slogan (or sarkha, meaning "scream") has also gained notoriety.

6. **Suspected drones used by Yemen's Houthi rebels attack 2 more ships in Mideast waters (AP News, 06 FEB, Jon Gambrell)**

   Two ships traveling in Middle East waters were attacked by suspected Yemen Houthi rebel drones early on Tuesday, authorities said, the latest assaults in the Iranian-backed fighters' campaign of targeting vessels over Israel's war on Hamas in the Gaza Strip.

7. **Military experts evaluate the U.S. response in the MidEast (AP News, 05 FEB)**

   Tension has been rising since the latest Israel-Hamas war began in early October, with Iran-backed fighters intensifying attacks on U.S. military and international commercial interests in the region.

Russia-Ukraine Conflict

1. The Warzone Ukraine Situation Report:

Ukraine Situation Report: Scholz Says Germans Would Need To Deploy With Taurus Missiles – 28 FEB

Ukraine Situation Report: U.S. Warns Of Looming “Catastrophic” Arms Shortage – 23 FEB

Ukraine Situation Report: Kyiv Claims Six Russian Jets Downed In Three Days – 19 FEB

Ukraine Situation Report: NATO Wants To Give Kyiv A Million Drones In 2024 – 15 FEB

Ukraine Situation Report: Battle-Damaged HIMARS Return To United States – 12 FEB

Ukraine Situation Report: Zelensky Picks New Top Commander – 08 FEB

Ukraine Situation Report: Kyiv’s Grip On Avdiivka Is Slipping – 06 FEB

Ukraine Situation Report: Czechs Call For Sourcing Shells For Ukraine From Outside Europe – 02 FEB

2. Institute for The Study of War

Russian Offensive Campaign Assessment, February 29, 2024
Russian Offensive Campaign Assessment, February 28, 2024
Russian Offensive Campaign Assessment, February 27, 2024
Russian Offensive Campaign Assessment, February 26, 2024
Russian Offensive Campaign Assessment, February 25, 2024
Russian Offensive Campaign Assessment, February 24, 2024
Russian Offensive Campaign Assessment, February 23, 2024
Russian Offensive Campaign Assessment, February 22, 2024
Russian Offensive Campaign Assessment, February 21, 2024
Russian Offensive Campaign Assessment, February 20, 2024
Russian Offensive Campaign Assessment, February 19, 2024
Russian Offensive Campaign Assessment, February 18, 2024
Russian Offensive Campaign Assessment, February 17, 2024
Russian Offensive Campaign Assessment, February 16, 2024
Russian Offensive Campaign Assessment, February 15, 2024
Russian Offensive Campaign Assessment, February 14, 2024
Russian Offensive Campaign Assessment, February 13, 2024
Russian Offensive Campaign Assessment, February 12, 2024
Russian Offensive Campaign Assessment, February 11, 2024
Russian Offensive Campaign Assessment, February 10, 2024
Russian Offensive Campaign Assessment, February 09, 2024
Russian Offensive Campaign Assessment, February 08, 2024
Russian Offensive Campaign Assessment, February 07, 2024
Russian Offensive Campaign Assessment, February 06, 2024
Russian Offensive Campaign Assessment, February 05, 2024
Russian Offensive Campaign Assessment, February 04, 2024
Russian Offensive Campaign Assessment, February 03, 2024
Russian Offensive Campaign Assessment, February 02, 2024
Russian Offensive Campaign Assessment, February 01, 2024

Back to Table of Contents

3. **Putin warns that sending Western troops to Ukraine risks a global nuclear conflict (AP News, 29 FEB, Vladimir Isachenkov)**

Russian President Vladimir Putin vowed Thursday to fulfill Moscow's goals in Ukraine and sternly warned the West against deeper involvement in the fighting, saying that such a move is fraught with the risk of a global nuclear conflict.

Putin's warning came in a state-of-the-nation address ahead of next month's election he's all but certain to win, underlining his readiness to protect Russian gains in Ukraine.

4. **Ukraine's First M1 Abrams Tank Loss Appears To Have Occurred (The Warzone, 26 FEB, Joseph Trevithick)**

One of Ukraine's U.S.-supplied M1 Abrams tanks looks to have sustained significant damage and appears to be the first loss of one of these prized tanks in combat in the country. Evidence that Ukrainian Abrams tanks had finally entered the fight only recently began to emerge. This also comes amid concerns about the ability of Ukraine's armed forces to sustain these tanks in the long term.

5. **Another One Of Russia's Prized A-50 Radar Planes Shot Down, Ukraine Claims (The Warzone, 23 FEB, Thomas Newdick)**

Ukraine claimed today that Russia lost another A-50 Mainstay airborne early warning and control (AEW&C) aircraft — which would be the second such loss of the conflict so far. Among the first rumors of the incident to circulate came from Russian military bloggers, saying that the Mainstay was a victim of friendly fire over the Sea of Azov. Meanwhile, Ukrainian accounts suggested that the aircraft was shot down in a joint operation by the Ukrainian Armed Forces and Ukrainian intelligence services.

Back to Table of Contents

6. **This May Be The First Video Of A Ukrainian M1 Abrams In Combat (The Warzone, 23 FEB, Thomas Newdick)**

Avideo has emerged showing, apparently for the first time, a U.S.-supplied M1 Abrams tank in action on the front lines of Ukraine. While it's been known that these tanks have been in the country since at least last September, the appearance of a Ukrainian Abrams reportedly close to Avdiivka in the eastern Donetsk region — as well as possible evidence of one having been put out of action — confirms that these capable combat vehicles are indeed in the fight.

7. **How Ukraine's defense companies have adapted to two years of war (Defense News, 22 FEB, Elisabeth Gosselin-Malo)**

With the third winter of war well underway in Ukraine, the country's military-industrial complex is in a race against the technological clock to out-innovate Russian invaders.

The uncertainty looming over the future of foreign military aid to Ukraine and the slow deliveries of pledged equipment from allies have affected how Kyiv designs and develops weapons.

8. **WARNING: Transnistria May Organize a Referendum on Annexation to Russia to Support Russian Hybrid Operation Against Moldova (ISW, 22 FEB, George Barros, Fredrick w. Kagan, Christina Harward, and Angelica Evans)**

Warning: The pro-Russian breakaway region of Transnistria may call for or organize a referendum on Transnistria's annexation to Russia at a recently announced Transnistrian Congress of Deputies planned for February 28. The pretext for such a call would be the purported need to protect Russian citizens and "compatriots" in Transnistria from threats from Moldova or NATO or both. Russian President Vladimir Putin could, in the most dangerous course of action, declare Russia's annexation of Transnistria during his planned address to the Russian Federal Assembly on February 29, although that appears unlikely. Putin will more likely welcome whatever action the Transnistrian Congress of Deputies takes and offer observations on the situation. ISW offers this assessment as a warning for a high-impact event of indetermined probability. Moldovan government officials state that the situation in Moldova is unlikely to worsen as of February 22.

9. **Iran Just Delivered Hundreds Of Iranian Ballistic Missiles To Russia: Report (The Warzone, 21 FEB, Joseph Trevithick)**

Russia has finally begun receiving hundreds of Iranian ballistic missiles, according to a new report. If true, these deliveries would bolster Russia's dwindling ballistic missile arsenal, which has already presented significant challenges for defenders in neighboring Ukraine, with additional combat-proven types. The War Zone highlighted these exact issues in detail before and after the first reports that Iran might send ballistic missiles to Russia first emerged in late 2022.

Back to Table of Contents

10. **North Korean Missile Used In Ukraine Was Packed Full Of U.S. Parts (The Warzone, 20 FEB, Thomas Newdick)**

Ashort-range ballistic missile (SRBM) produced by North Korea and recently used against Ukraine by Russia relied on more than 290 foreign-sourced components, many of them originating from U.S. manufacturers. This is the alarming result of a study by Conflict Armament Research (CAR), a U.K.-based investigative organization.

11. **Ukraine decodes Russian 'carrots' and 'tea bags' chatter to save lives (AP, 14 FEB, Samya Kullab)**

As the radio crackles with enemy communications that are hard to decipher, one Russian command rings out clear: "Brew five Chinese tea bags on 38 orange."

A Ukrainian soldier known on the battlefield as Mikhass, who has spent months listening to and analyzing such chatter, is able to quickly decode the gibberish. It means: Prepare five Beijing-made artillery shells and fire them on a specific Ukrainian position in the Serebryansky Forest, which forms the front line in the country's restive northeast.

12. **Ukraine's 6000+ EW 'Acoustic Sensors' To Counter Russia's Kamikaze UAVs Get US Military Interested (The EurAsian Times, 13 FEB, Ashish Dangwal)**

In response to massive threats posed by Russian kamikaze drones, Ukraine has implemented an innovative solution: a comprehensive acoustic sensor network spanning thousands of sensors across its territory.

The deployment of this network was revealed by General James Hecker, the head of the US Air Forces in Europe (USAFE), Air Forces Africa (AFAFRICA), and NATO's Allied Air Command, during a press roundtable held on the sidelines of the Air & Space Forces Association Warfare Symposium on February 12.

13. **Ukraine: Is Europe starting to change its strategy? (DW, 13 FEB, Frank Hofmann)**

NATO generals are bracing themselves for an increased risk of war with Russia and are calling for investment in deterrence. Ukraine may benefit from this as well.

14. **Ukraine Using Thousands Of Networked Microphones To Track Russian Drones (The Warzone, 12 FEB, Joseph Trevithick)**

Ukraine is using a network made up of thousands of acoustic sensors across the country to help detect and track incoming Russian kamikaze drones, alert traditional air defenses in advance, and also dispatch ad hoc drone hunting teams to shoot them down. This is according to the U.S. Air Force's top officer in Europe who also said the U.S. military is now looking to test this capability to see if it might help meet its own demands for additional ways to persistently monitor for, and engag,e drone threats.

15. **The Kremlin's Occupation Playbook: Coerced Russification and Ethnic Cleansing in Occupied Ukraine (ISW, 09 FEB, Karolina Hird)**

The war in Ukraine is primarily a war for control of people, not land. Russian President Vladimir Putin has invaded Ukraine twice not mainly because he desires Ukraine's land, but rather because he seeks to control its people. Putin's project, explicitly articulated in the 2021 article he published justifying the 2022 full-scale invasion, is the destruction of Ukraine's distinctive political, social, linguistic, and religious identity. Putin seeks to make real his false ideological conviction that Ukrainians are simply confused Russians with an invented identity, language, and history that a small, Western-backed minority is seeking to impose on the majority of inhabitants. He sees language as one of the primary determinants of ethnicity—Russian speakers, he claims, must be Russians regardless of the state they live in. The Russian Federation has claimed special rights to protect Russians in the former Soviet states since the 1990s, although the Kremlin did not act on those claims until Putin became president. Putin's aim to destroy Ukrainian identity, language, and culture is thus one of the primary objectives of his entire enterprise.

Back to Table of Contents

16. **Fact Sheet: US Assistance To Ukraine (ISW, 08 FEB)**

17. **'Double War' Weakens Ukraine; Unending Russia Conflict, Corruption Within Military Ranks Hurt Zelensky (The EurAsian Times, 06 FEB, Prakash Nanda)**

President Volodymyr Zelenskiy seems now to be fighting two wars simultaneously. One war is on the battlefield against Russia. The other, which, in a way, has gained more urgency, happens to be the war on corruption inside Ukraine.