Cyber Center of Excellence

Unclassified Threat Read Book

1-15 March 2023

Prepared by: Threat Management Office
CCoE
Fort Gordon, GA 30905

POC: Threat Management Office, jeffrey.t.hardimon.civ@army.mil or
kevin.m.bird.civ@army.mil 706-849-9259

Table of Content

Cyber

Electronic Warfare

Information Advantage

Signal

1. Fine-Tuning the Work Needed to Adapt Commercial 5G to Military Communications – 14 MAR
2. Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military – 09 FEB
3. A Chinese spacecraft has been checking out US satellites high above Earth – 03 MAR
4. DoD interested in smartphone-to-satellite communications services – 01 MAR
5. European firms line up behind push for secure SATCOM standard – 01 MAR

Items of Interest

1. Russia-Ukraine Situation Report
2. Video Purports To Show Russian Su-27's Close Encounter With An MQ-9 – 15 MAR
3. What We Know—and Don't Know—About the U.S. Drone-Russian Fighter Jet Encounter – 15 MAR
4. Russian Su-27 Collided With U.S. MQ-9 Over Black Sea (Updated) – 14 MAR
5. Foreign Reflections on U.S. Exercises and Operations - 10 March 2023
6. Posture Statement of General Paul M. Nakasone – 07 MAR
7. Ukraine Situation Report: Belarus Admits Russian A-50 Radar Jet Damaged In Drone Attack – 07 MAR
8. Russia Using Western Satellites to Hone Attacks in Ukraine – 02 MAR
9. There's Now a Video of the 'Most Successful' Sabotage Operation Against Russia During the Full-Scale Invasion – 02 Mar
10. Former PLA Senior Colonel: Putin Cannot Win War, But Cannot Afford to Lose It – 02 MAR
11. Ukrainian Drone Gets Within 70 Miles Of Moscow – 28 FEB

Cyber

1. **Russian hackers have been exploiting unknown flaw in Outlook for nearly a year now (Tech Radar, 15 MAR, Craig Hale)**

   Microsoft has just issued an update to its Outlook desktop client to protect users from hackers reportedly associated with the Russian military intelligence service GRU.

   Official bodies and government agencies appear to have been the key focus of the attack, which took place from as early as April 2022.

   The elevation of privilege vulnerability, according to Microsoft(opens in new tab), only affected Outlook for Windows. macOS, iOS, Android, and web versions of the email provider were unaffected during this time.

2. **ChatGPT can write term papers and speak like people. Cyber criminals now use it. Here's how (The Charlotte Observer, 14 MAR, Chyna Blackmon)**

   A new artificial intelligence tool that has been used in classrooms, online forums and social media posts is now being used to steal your private information and money.

   ChatGPT has gained a lot of attention for its ability to generate realistic human responses to text-based input, particularly in academia.

   So far, it's been used for multiple legitimate purposes. Some major companies have turned to the tool to conduct business.

3. **Get Ready to Meet the ChatGPT Clones (Wired, 10 MAR, Will Knight)**

   The technology behind OpenAI's viral chatbot is set to become widely replicated, unleashing a tidal wave of bots.

   CHATGPT might well be the most famous, and potentially valuable, algorithm of the moment, but the artificial intelligence techniques used by OpenAI to provide its smarts are neither unique nor secret. Competing projects and open-source clones may soon make ChatGPT-style bots available for anyone to copy and reuse.

4. **Russian Cyberwar Against Ukraine Stumbles, Just Like Conventional One (Insurance Journal, 09 MAR, William Turton)**

   Even before Russia invaded Ukraine, its hacking offensive was well under way.

   Suspected Russian hackers targeted Ukrainian government and financial websites with so-called distributed denial-of-service attacks aimed at creating chaos; they bombarded government, nonprofit and IT organizations with malicious software designed to render computers inoperable; and, in a broadside widely blamed on Russia, they zeroed in on Viasat Inc.'s commercial satellite network, causing major disruptions in Ukrainian communications, including for military units, at a crucial early stage in the war

5. **North Korea-linked Lazarus APT group exploits a zero-day vulnerability in attacks aimed at a South Korean financial entity. (Security Affairs, 08 MAR, Pierluigi Paganini)**

   ASEC (AhnLab Security Emergency Response Center) observed North Korea-linked Lazarus APT group exploiting a zero-day vulnerability in an undisclosed software to breach a financial business entity in South Korea. The nation-state actors breached twice the company in one year.

6. **Russia will have to rely on nukes, cyberattacks, and China since its military is being thrashed in Ukraine, US intel director says (Business Insider, 08 MAR, Chris Panella & John Haltiwanger)**

   Russia's high losses and wasted resources in Ukraine have made it less of a traditional military threat and will leave it reliant on "asymmetric" options such as nuclear weapons, cyberattacks, and space technology, and other countries like China, the US intelligence director said Wednesday.

   At a Senate Intelligence Committee hearing, Director of National Intelligence Avril Haines said Russia "has suffered losses that will require years of rebuilding and leave it less capable of posing a conventional military threat."

   As a result, Haines said, "Russia will become even more reliant on asymmetric options such as nuclear, cyber, space capabilities, and on China."

7. **Cyber-Threat Detections Surge 55% in 2022 (Info Security, 08 MAR, Phil Muncaster)**

   Trend Micro has said it stopped 146 billion cyber-threats in 2022, a 55% increase on the previous year and evidence of cyber-criminals widening their efforts to companies of all sizes and sectors.

   The global security vendor compiled its annual roundup report, Rethinking Tactics, from threat intelligence generated across mobile, IoT, PC and server endpoints, email, web and network layers, OT networks, cloud, home networks, vulnerabilities, consumers, businesses and governments worldwide.

   It revealed a 242% increase in the number of blocked malicious files and an 86% increase in backdoor malware detections – the latter indicative of threat actors successfully gaining initial access into targeted networks in greater numbers, the report claimed.

8. **'Password' Still the Most Common Term Used by Hackers to Successfully Breach Enterprise Networks According to Specops 2023 Weak Password Report (Business Wire, 08 MAR, Paula Brici)**

   Specops Software, a leading provider of password management and user authentication solutions, has today announced the release of its annual Weak Password Report which analyzed over 800 million breached passwords, and proves passwords are still the weakest link in an organization's network.

9. **Russia remains a 'very capable' cyber adversary, Nakasone says (C4ISR Net, 07 MAR, Colin Demarest)**

   U.S. Cyber Command is keeping a close watch on digital activity in the Russia-Ukraine war that may coincide with a springtime renewal of military operations, according to the organization's leader, Gen. Paul Nakasone.

   Nakasone, who oversees both CYBERCOM and the National Security Agency, told the Senate Armed Services Committee March 7 that his teams are monitoring the situation in Ukraine "very carefully," noting that Russia remains a "very capable adversary."

10. **6 New-age cybersecurity threats to look out for in 2023: Automotive hacking, automated cyberattacks, threat of ChatGPT & more (Times of India, 06 MAR, Neelesh Kripalani)**

    As the world of technology continues to evolve, so do the security threats that come with it. Cybersecurity is an ever-growing field that is constantly changing and adapting to the latest threats. As we look ahead to 2023, here are 6 predictions that can be made about the future of cybersecurity and how it will shape the digital world that we live in…

11. **Threat Intelligence: Do We Need A 'Rosetta Stone' of Cyber Attribution? (Infosecurity-Magazine, 06 MAR, Kevin Poireault)**

    What do FoxBalde, HermeticWiper and DriveSlayer have in common? They are all same wiper malware deployed against Ukrainian organizations on February 23, 2022, several hours before Russian troops set foot on Ukraine's soil.

    The only difference, they were named by three different vendors, Microsoft, SentinelOne and CrowdStrike respectively.

    This is not an uncommon complication. WhisperGate and Paywipe for instance are names used to talk about a separate wiper attack launched a month earlier, the former has been coined by Microsoft, and the latter by Google's Mandiant.

12. **Palo Alto Networks Takes On Identity Attacks, Extends its Cortex XSIAM Platform with AI-driven Identity Threat Detection and Response (PR Newswire, Palo alto Networks, INC, 06 MAR)**

    SANTA CLARA, Calif., March 6, 2023 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, announced today the availability of its new Identity Threat Detection and Response (ITDR) module for Cortex® XSIAM™. ITDR enables customers to ingest user identity and behavior data and deploy state of the art AI technology to detect identity-driven attacks within seconds. The module further strengthens XSIAM's ability to consolidate multiple security operations capabilities into a unified, AI-driven security operations center (SOC) platform.

    Identity-driven attacks, which target user credentials to access confidential data and systems, are one of the most common methods cyber criminals use to breach organizations' networks. For example, in recent years Lapsus$ Group has used privileged user credentials to attack multiple government agencies, as well as multiple large technology companies.

13. **Japan can learn from Israel about how to win cyberwars (Nikkei Asia, 05 MAR, Hiroyuki Akita)**

    Cyberattacks have drastically jumped around the world, and Japan may have become easy prey.

    Between September and November last year, Japan was targeted with the second-highest number of cyberattacks in the world after the U.S., according to a recent report by Canadian cybersecurity company BlackBerry, which said 8% of the 1.76 million attacks it had detected in the period were directed at Japan.

    It is no surprise that the U.S., the world's top information and technology destination, was the No.1 target. But why did Japan come under such a heavy attack? "Hacker groups around the world may have realized how feeble the country's cyberdefense is," said a Japanese government official in charge of national security.

14. **Stay Ahead of the Game: How AI Can Help You Avoid Cybersecurity Traps (ghacks.net, 05 MAR, Zakhi Mgu Tshini)**

I have never been a victim of cyber threats, but from what I've heard, the effects are devastating. Cybersecurity officers and consultants work tirelessly to implement security strategies to fight hackers. Artificial Intelligence (AI) is a new powerful tool that helps organizations and individuals stay ahead of cybersecurity threats.

15. **AI Image Generators: An Emerging Cybersecurity Threat (Make Use Of, 04 MAR, Damir Muezinovic)**

Pictures made by artificial intelligence seem like good fun, but they can be a serious security danger too. Here's how.

Artificial intelligence (AI) has the potential to change the very nature of our society. And if the AI tools we currently have at our disposal are any indication of what's to come, we have a lot to look forward to.

We also have a lot to be wary of. Namely, the weaponization of AI by cybercriminals and other threat actors. This isn't a theoretical concern, and not even AI image generators are immune to abuse.

16. **ChatGPT being used by cybercriminals to generate scams, Norton warns (NZ Herald, 02 MAR)**

Cybercriminals are using artificial intelligence chatbot ChatGPT to quickly create emails or social media posts to lure the public into scams, an anti-virus software provider is warning.
ChatGPT is set to be expanded across Microsoft's products including Word, Powerpoint and Outlook after the tech giant invested billions of dollars into parent company OpenAI in January.
But despite the chatbot causing a raft of excitement over its ability to allow users to write poems, stories and answer questions, it seems it could also have a darker side.

17. **Hackers Can Turn Bing's AI Chatbot Into a Convincing Scammer, Researchers Say (Vice, 02 MAR, Chloe Xiang)**

The Resarchers Found that a text prompt hiding in an open browser tab can cause the chatbot to take on whatever persona the attacker desires.

Hackers can make Bing's AI chatbot ask for personal information from ta user interacting with it, turning it into a convincing scammer without the user's knowledge, researcher say

In a new study, researchers determined that AI chatbots are currently easily influenced by text prompts embedded in web pages. A hacker can thus plant a prompt on a web page in 0-point font, and when someone is asking the chatbot a question that causes it to ingest that page, it will unknowingly activate that prompt. The researchers call this attack "indirect prompt injection," and give the example of compromising the Wikipedia page for Albert Einstein. When a user asks the chatbot about Albert Einstein, it could ingest that page and then fall prey to the hackers' prompt, bending it to their whims—for example, to convince the user to hand over personal information.

18. **The next big threat to AI might already be lurking on the web (ZDNet, 02 MAR, Danny Palmer)**

Artificial intelligence experts warn attacks against datasets used to train machine-learning tools are worryingly cheap and could have major consequences.

Artificial Intelligence (AI) and machine-learning experts are warning against the risk of

data-poisoning attacks that can work against the large-scale datasets commonly used to train the deep-learning models in many AI services.

Data poisoning occurs when attackers tamper with the training data used to create deep-learning models. This action means it's possible to affect the decisions that the AI makes in a way that is hard to track.

19. **ChatGPT is dark web's 'hottest topic' as criminals look to weaponise AI (Independent, 02 MAR, Anthony Cuthbertson)**

Hackers want to take 'complete control' of artificial intelligence tool, warns cyber expert

Discussions about ChatGPT have begun to flood forums on the dark web as hackers seek ways to exploit the AI chatbot, according to cyber security researchers.

The number of new posts about ChatGPT on the dark web – a section of the internet unreachable through conventional web browsers – grew seven-fold between January and February, while threads rose in popularity by 145 per cent.

Electronic Warfare

1. **Boeing says ground-based system keeps satellites free from jamming (C4ISR Net, 07 MAR, Courtney Albon)**

   A demonstration at Aberdeen Proving Grounds in Maryland validated Boeing's design for a ground-based system that can protect communication satellites from signal jamming, according to the company.

   Boeing is developing the U.S. Space Force's Protected Tactical Enterprise Services ground system, which can defend against electronic warfare threats to military and commercial satellites.

2. **Electronic warfare key to keeping PRC at bay (Taipei Times, 05 MAR, Chang Yan-ting)**

   An Australian military aircraft last week entered Taiwan's northeastern air defense identification zone (ADIZ) four times within a day. Last month, Australian aircraft flew similar maneuvers twice, approaching from more than 5,000km away and flying at an unusually low altitude.

   The flights might be part of the Cope North 23 exercise involving Australia, Japan and the US. The area of the Guam-based drill included the airspace near Taiwan.

   In the past few years, Australian E-7A airborne early-warning and control aircraft and AP-3C electronic warfare and early-warning aircraft were part of the annual drills. The E-7A has a radar detection range of about 400km, and uses Ka and Ku-band technology that enables it to detect general communication signals.

3. **Aussie Space Command looks to electronic warfare, other tech to deter attacks on satellites (Breaking Defense, 02 MAR, Colin Clark)**

   The head of Australia's Defense Space Command says her country seeks technologies to deter countries that might try to laze, jam, bump or move Aussie satellites.

   "We are working on making sure that we've got a level of capability so that we can deter attacks on our satellites, essentially through non-kinetic means so that we can have some impact," Air Vice Marshall Cath Roberts, told a small group of reporters here, one year after her command was established. Electronic warfare is a key tool, she said.

   "I think it's a really important part of where we go to is just looking at how we can have that sort of electronic warfare-type of capability to allow us to deter attacks or certainly interfere," she said. Asked when she would have EW capabilities to deter other nations, she said simply, "As soon as I can."

4. **China Sees Balloon-Launched Drone Swarms In Its Future (The Drive, 02 MAR, Joseph Trevithick)**

   Researchers in China and elsewhere have demonstrated that high-altitude balloons can launch drones and the military applications are glaring.

   Astring of shootdowns of high-flying aerial objects over the United States and Canada last month has called new attention to the value of balloons for intelligence-gathering and other military purposes. This also includes acting as launch platforms for drones, potentially in large numbers, that could then be operated as networked swarms. The ability to deploy uncrewed aircraft from high-altitude balloons is real and is something that researchers around the world, including in China, have been publicly experimenting with for years now.

Information Advantage

1. **EU expansion key to counter Russia, China's influence, says Swedish premier (Yenisafak, 15 MAR, Carsamba)**

   The EU's enlargement to include Ukraine and Western Balkan countries is important to counter Russia and China's influence, The Swedish prime minister said on Wednesday.

   In a keynote speech at Berlin's Hertie School of Governance, Ulf Kristersson, said the Ukraine war has been a critical geopolitical turning point for the EU.

   "Russia's war against Ukraine has also brought enlargement back on the agenda, although integrating additional countries info the EU will be difficult," he said.

2. **Russian Special Ops Group to Conduct False Flag in Belarus (U.S. Army Europe Open Source Intelligence Center, 13 MAR)**

   A social media user posted that Russia has a special operations group in Belarus who will conduct a false flag attack and blame it on Ukraine. The groups is trained to speak Ukrainian and will wear Ukrainian military uniforms.

3. **China's Influence in West Through AI Could Trigger Catastrophic Responses: Arthur Herman (NTD, 08 MAR, Evelyn LI)**

   According to Graphika, China is using AI anchors to spread pro-China disinformation on social media. Now, national security and Pentagon officials say they are investigating concerns that made-in-China cargo cranes in American ports are being used for spying. NTD speaks to Arthur Herman, a senior fellow and director of the Quantum Alliance Initiative at the Hudson Institute, who explains how China is making its predictions to guide people's decisions increasingly accurate.

4. **US intel: Chinese influence operations are growing more aggressive, more similar to Russia's (Cyber Scoop, 08 MAR, Elias Groll)**

   China is stepping up efforts to influence U.S. public opinion, which increasingly resemble Russian operations.

   U.S. intelligence officials warned on Wednesday that China is stepping up its efforts to carry out influence operations against the United States and that its efforts to influence American public opinion increasingly resemble Russian operations.

5. **US sees China propaganda efforts becoming more like Russia's (C4ISR Net, 07 MAR, Nomaan Merchant & Matthew Lee)**

   China has long been seen by the U.S. as a prolific source of anti-American propaganda but less aggressive in its influence operations than Russia, which has used cyberattacks and covert operations to disrupt U.S. elections and denigrate rivals.

   But many in Washington now think China is increasingly adopting tactics associated with Russia — and there's growing concern the U.S. isn't doing enough to respond.

6. **China's AI-powered influence operations at India's doorstep (Hindustan Times, 06 MAR)**

   In the 21st century, battle lines become more complex as they now also use technology, as well as civilians as combatants in various types of cyber warfare. A recent report revealed a pro-Chinese political spam operation promoting a new and distinctive form of

video content.

7. **Industry's Influence on AI Is Shaping the Technology's Future—for Better and for Worse (Singularity Hub, Edd Gent, 05 MAR)**

   The enormous potential of AI to reshape the future has seen massive investment from industry in recent years. But the growing influence of private companies in the basic research that is powering this emerging technology could have serious implications for how it develops, say researchers.

   The question of whether machines could replicate the kind of intelligence seen in animals and humans is almost as old as the field of computer science itself. Industry's engagement with this line of research has fluctuated over the decades, leading to a series of AI winters as investment has flowed in and then back out again as the technology has failed to live up to expectations.

8. **Alleged Russian Mass Information Attack on Serbo-Russian Relations (USAEUR Open Source Intelligence Center, 03 MAR)**

   March 3. Social media report originating from Russia blogosphere alleging that Serbia through third party has acted as a weapons supplier to Ukraine. Russia has officially asked for investigation of this matter, while Serbia Defense Office has vehemently denied such arrangement.

9. **North Korea's Nuclear Missile Attack AI Is Aiding And Robot-Human Composite Boundary (Yonhap Online, Ha Chae-rim, 03 MAR)**

   With the help of an artificial intelligence (AI) command and control system, a military operational concept that can respond in real time to North Korea's nuclear weapons and missiles will be established.

   An unmanned combat system, such as robots with AI technology, will be deployed at the forefront to establish a system that entrusts guard operations in the Demilitarized Zone (GP) and general outpost (GOP).

   The Ministry of National Defense announced on the 3rd that it had received approval from President Yoon Seok-yeol of the 'Defense Innovation 4.0 Basic Plan' with these details.

10. **Electronic Warfare (Providence, 01 MAR, Steven Tucker)**

    Amongst the more trivial consequences of Russia's invasion of Ukraine in February 2022 was the postponement of the turn-based military tactics title Advance Wars 1+2: Re-Boot Camp, originally scheduled to appear on Nintendo's Switch console last April. "In light of recent world events," said Nintendo, it was now temporarily considered too insensitive to release.

Signal

1. **Fine-Tuning the Work Needed to Adapt Commercial 5G to Military Communications (Satellite Today, 14 MAR, David Hodes)**

   Space-based 5G is a growing development with the promise of a big impact in military communications because of its high reliability, and its accuracy for communication and information exchange in remote areas where low latency instant warfighting data is critical.

   A key issue addressed by the four panelists at the presentation, "The Role of Space-Based 5G in Military Communications," is the work needed to address the challenges in adapting 5G for military use from the commercial product that exists today, and how quickly that innovation-driven adaptation can come together.

2. **Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military (Space News, 09 MAR, Sandra Erwin)**

   SpaceX's decision to limit Ukrainian troops' use of the company's satellite internet is a cautionary tale for the U.S. military as it grows its reliance on commercial services, the head of U.S. Space Command Gen. James Dickinson told lawmakers March 9.

   The issue was raised by Sen. Mark Kelly (D-Ariz.) during a hearing of the Senate Armed Services Committee. He questioned SpaceX's actions to prevent Ukraine's military from using the company's Starlink service to control drones in the war against Russia.

3. **A Chinese spacecraft has been checking out US satellites high above Earth (Space.com, Andrew Jones, 03 MAR)**

   The Chinese satellite TJS-3 has been inspecting other countries' assets in geostationary orbit.

   A Chinese satellite launched in 2018 has been inspecting other nations' spacecraft high above Earth in geostationary orbit.

   Tongxin Jishu Shiyan Weixing-3 (TJS-3), named vaguely as a communications experiment satellite, was sent up into geostationary orbit in late 2018. It then released a small subsatellite, possibly to help test TJS-3's capabilities.

4. **DoD interested in smartphone-to-satellite communications services (Space News, 01 MAR, Sandra Erwin)**

   The Commercial Services Communications Office is working on a solicitation for direct-to-device satellite communications services to be released later this year.

   The technology race to connect cellphones to satellite networks has not gone unnoticed by the Defense Department.

   "That capability is exciting to us," Clare Grason, head of the Pentagon's commercial satellite communications office, said Feb. 28.

   Emerging communications services that connect phones directly to satellites are attractive to military users that operate in locations where there is no cellular network connectivity, Grason said during a FedInsider webinar.

5. European firms line up behind push for secure SATCOM standard (C4ISR Net, 01 MAR, Colin Demarest)

European satellite communications industry and academia have kicked off a government-supported effort to develop a new protected waveform for the continent's militaries.

The European Protected Waveform is one of the 61 projects to receive inaugural European Defense Fund (EDF) support, the European Union announced in summer 2022. The goal of the program is to design a new secure and resilient waveform standard that will help EU armed forces tackle increased throughput demand over satellite while supporting dispersed operations, mobility, and novel security threats, according to an EDF fact sheet.

Items of Interest

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

These reports are a compilation of articles from Russia, Ukraine, and other nations regarding the current tensions between Russia and Ukraine. Topics covered in this report include the following:

- Foreign Observations and Reactions
- Social Media Highlights
- Russian Eastern Military District Movements
- Other Topics

Russia-Ukraine Situation Report, 15 March 2023

Russia-Ukraine Situation Report, 14 March 2023

Russia-Ukraine Situation Report, 13 March 2023

Russia-Ukraine Situation Report, 10 March 2023

Russia-Ukraine Situation Report, 09 March 2023

Russia-Ukraine Situation Report, 07 March 2023

Russia-Ukraine Situation Report, 06 March 2023

Russia-Ukraine Situation Report, 03 March 2023

Russia-Ukraine Situation Report, 02 March 2023

Russia-Ukraine Situation Report, 01 March 2023

2. Video Purports To Show Russian Su-27's Close Encounter With An MQ-9 (The Drive, 15 MAR, Thomas Newdick)

A day after a collision between a U.S. MQ-9 and a Russian Su-27, new footage appears to show a close-in pass between the two types.

A video has surfaced that allegedly shows a close pass involving a U.S. Air Force MQ-9 Reaper and a Russian Su-27 Flanker fighter jet, the two types that were involved in a collision over the Black Sea yesterday. Readers of The War Zone can get fully up to speed on what is known about this incident in our initial reporting here. Since then, U.S. Defense Secretary Lloyd Austin has added his comments on the incident, describing it as a "hazardous episode [that] is part of a pattern of aggressive, risky, and unsafe actions by Russian pilots in international airspace."

3. What We Know—and Don't Know—About the U.S. Drone-Russian Fighter Jet Encounter (Time, 15 MAR, Lolita C. Baldor & Tara Copp)

When a Russian fighter jet collided with a large U.S. surveillance drone over the Black Sea on Tuesday, it was a rare but serious incident that triggered a U.S. diplomatic protest and raised concerns about the possibility Russia could recover sensitive technology.

U.S. and Russian officials had conflicting accounts of the collision between the MQ-9 Reaper drone and the Russian Su-27 fighter jet — each blaming the other. But a

Pentagon spokesman raised the possibility that the Defense Department could eventually declassify and release video it has of the collision.

4. **Russian Su-27 Collided With U.S. MQ-9 Over Black Sea (Updated) (The Drive, 14 MAR, Howard Altman & Joseph Trevithick)**

   Prior to the collision, two Russian Su-27s intercepted the MQ-9 and were dumping fuel on it, before one clipped the drone's propeller.

   The U.S. Air Force says that one of its MQ-9 Reaper drones crashed into the Black Sea today after a collision with a Russian Su-27 Flanker fighter jet. The incident was the end result of a "reckless" and "unprofessional" intercept of the uncrewed aircraft by a pair of Russian Su-27s in international airspace, according to the service.

5. **Foreign Reflections on U.S. Exercises and Operations, 10 March 2023 (U.S. Army Asian Studies Detachment, 10 MAR)**

   This week's report contains reporting of foreign observations on U.S. and bilateral exercises from 3 to 9 March 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, North Korea, the Philippines, and South Korea.

6. **Posture Statement of General Paul M. Nakasone (U.S. Cyber Command, 07 MAR)**

   Chairman Reed, Ranking Member Wicker and distinguished members of the committee, thank you for your enduring support and the opportunity to represent the men and women of U.S. Cyber Command (USCYBERCOM). I am honored to be here beside Assistant Secretary of Defense Christopher Maier and General Bryan Fenton. I look forward to describing how USCYBERCOM continues to deliver return on investment by using the authorities and resources provided by Congress and highlighting the work ahead for 2023.

   Guided by the National Defense Strategy, USCYBERCOM focuses on building enduring advantages through campaigning to support Integrated Deterrence. USCYBERCOM acts against foreign adversaries that threaten our nation and expands capability through cooperation with federal, private and allied partners. We seek to outmaneuver our adversaries as they look for opportunities to exploit the United States' dependence on data and networks in critical infrastructure, the Defense Industrial Base and private industry.

7. **Ukraine Situation Report: Belarus Admits Russian A-50 Radar Jet Damaged In Drone Attack (The Drive, 07 MAR, Thomas Newdick)**

   The Belarusian president has now admitted that a drone attack by partisans caused some damage to a Russian A-50 radar plane last month.

   Belarusian leader Alexander Lukashenko has claimed that more than 20 people have been arrested following a drone attack on a Russian A-50 Mainstay airborne early warning and control (AEW&C) aircraft at Machulishchy Air Base, Belarus, late last month. Lukashenko confirmed that an attack using a "small drone" did indeed take place but said the radar plane suffered only superficial damage.

8. **Russia Using Western Satellites to Hone Attacks in Ukraine (Kyiv Post, 02 MAR, Jason Jay Smart)**

   Ukrainian officials tell the Kyiv Post that certain European and US companies may be involved in providing satellite images to Russia which are then used to target Ukraine's critical infrastructure.

As many as ten companies are suspected of selling satellite images to Russia which are then used to attack critical infrastructure sites in Ukraine, sources with knowledge of the issue confirmed to Kyiv Post.

Such sales would be in violation of current United States and European Union sanctions against Russia.

Included among those suspected of trading with Russia and its proxies are companies from the USA, South Korea, the European Union, Israel and China.

9. **There's Now a Video of the 'Most Successful' Sabotage Operation Against Russia During the Full-Scale Invasion (Kyiv Post, 02 MAR, Stefan Korshak)**

Belalrus opposition releases video of hobby drone making brazen landing on Russian air force AWACS jet.

A Belarusian opposition group, BYPOL, on Thursday released a video of a partisan-operated hobby drone making a brazen landing on top of the radar emitter of a $350 million dollar AWACS jet operated by the Russian air force.

10. **Former PLA Senior Colonel: Putin Cannot Win War, But Cannot Afford to Lose It (US Army Asian Studies Detachment, 02 MAR)**

On 1 March 2023 Shanghai-based Observer Online published a summary of a Deutsche Welle (DW) interview of a member of the Chinese delegation to the February 2023 Munich Security Conference. The delegate interviewed was former PLA Senior Colonel Zhou Bo. The Chinese language summary accurately gisted Zhou Bo's English statements on the Russia-Ukraine conflict and the role that China could play to avert further escalation. Key points emphasized in the Chinese summary of the English language interview have been summarized below.

11. **Ukrainian Drone Gets Within 70 Miles Of Moscow (The Drive, 28 FEB, Joseph Trevithick)**

The appearance of a Ukrainian-made UJ-22 near the Russian capital comes amid a spate of reported drone attacks in the country.

AUkrainian-made UJ-22 drone has come down in Russia within 70 miles of Moscow. This appears to be the closest a Ukrainian uncrewed aerial system has gotten to the Russian capital and follows the unexpected deployment of additional air defense assets there last month. This incident is also just one of a recent flurry of apparent Ukrainian drone attacks, or at least attempted attacks, on Russian targets in the past 24 hours or so.