Cyber Center of Excellence

Unclassified Threat Read Book

01-15 April 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

6. Unlocking the true potential of IoT with low cost satellite communications - 05 APR
7. If you hate Starlink, you’re not going to like that China is working on its own mega constellation - 01 APR

Items of Interest

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. US intelligence was aware of four extra Chinese spy balloons, leaked Pentagon data reveals - 15 APR,
4. U.S. arrests 21-year-old National Guardsman for online intelligence leaks - 14 APR
5. US, Ukraine say many war secrets safe from intel leaks - 13 APR
6. Russian T-90 Tank From Ukraine Mysteriously Appears At U.S. Truck Stop - 13 APR
7. Foreign Reflections on U.S. Exercises and Operations, 13 April 2023 - 13 APR
8. Damage Assessment From Major War Plans Leak Underway In U.S. - 07 APR
9. Foreign Reflections on U.S. Exercises and Operations, 06 April 2023 - 06 APR)

Cyber

1. **‘Unsophisticated Iranian Cyberattack’ Temporally Downs Israeli Bank Sites, Post Office (Haaretz, 14 APR, Ofir Dor)**

   Coinciding with Iran's Quds Day in support of the Palestinian people, the websites of several Israeli banks and the Israel Postal Service were bombarded with heavy hackers' traffic and hit by a denial of service (DDos) attack that took them offline. Check Point Software Technologies said the attacks were relatively unsophisticated and not very powerful, dealing limited damage.

   While the attacks stopped the website services intermittently, many have returned to operation. The Israel Post website was shut down, returned to service and once again crashed. The Bank of Jerusalem website announced that they were updating the site before it returned to service.

2. **Russian APT Hackers Actively Targeting European NATO Allies (Gov Infosecuirty, 13 APR, Akshaya Asokan)**

   An ongoing cyberespionage campaign tied to a Russian nation-state group is targeting European government agencies and diplomats to steal Western government intelligence on the war in Ukraine, says the Polish CERT and Military Counterintelligence Service.

3. **AI tools like ChatGPT likely to empower hacks, NSA cyber boss warns (C4ISRNet, 12 APR, Colin Demarest)**

   Generative artificial intelligence that fuels products like ChatGPT will embolden hackers and make email inboxes all the more tricky to navigate, according to the U.S. National Security Agency cybersecurity director.

   While much-debated AI tools will not automate or elevate every digital assault, phishing scheme or hunt for software exploits, NSA’s Rob Joyce said April 11, what it will do is “optimize” workflows and deception in an already fast-paced environment.

4. **Zero trust, AI and the cloud: The new frontiers in cybersecurity (Silicon Angle, 12 APR, Ryan Stevens)**

   In today’s technology-driven world, cybersecurity has grown more important than ever. Global cyberattacks increased by 38% in 2022 compared to 2021, and the world is facing global cyberthreats that have serious implications.

   These increasing cyberthreats have also led to an increase of companies seeking solutions, which has also led to fragmentation within the industry. That has made it difficult for organizations to pursue standardization and integration.

5. **Hackers have been spreading malware via fake Chrome updates (Tech Radar, 12 APR, Craig Hale)**

   According to security researcher Rintaro Koike(opens in new tab), hackers have been overwriting legitimate web pages with fake Chrome update messages designed to install malware that can evade antivirus detection - and worse.

   Initially observed from November 2022, Koike explains that the attack campaign became active in February 2023, targeting predominantly Japanese websites as well as some geared towards Korean and Spanish language ones.

6. **Russian attacks on Ukrainian infrastructure cause internet outages, cutting off a valuable wartime tool (Cyber Scoop, 12 APR, Elias Groll)**

   With its war effort faltering, the Kremlin is stepping up its attacks on Ukrainian power plants, resulting in cascading internet failures.

When Russian forces crossed into Ukraine early last year, one of their first targets was a key piece of internet infrastructure. By hitting the satellite internet provider Viasat on Feb. 24, 2022, with a wiper malware attack that infected its networking hardware, Russian forces appear to have disrupted communications at a key moment.

7. **Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries (Microsoft, 11 APR, Amy Hogan-Burney)**

The explosive growth of private “cyber mercenary” companies poses a threat to democracy and human rights around the world. Cyber mercenaries – private companies dedicated to developing, selling, and supporting offensive cyber capabilities that enable their clients to spy on the networks, computers, phones, or internet-connected devices of their targets – are a real cause for concern. These tools have been used to target elections, journalists, and human rights defenders and are increasingly accessible on the open market, enabling malicious actors to undermine our key democratic institutions.

8. **FBI warns against using public charging stations due to malware and 'juice jacking' risk (The national news, 11 APR, Alvin R. Cabral)**

The FBI has warned against the use of public charging points for electronic devices, saying they can be a gateway for cyber criminals.

Public charging stations heightens the risk of bad actors installing malware and gaining access to devices, the top US law enforcement agency's Denver department said on Twitter.

“Avoid using free charging stations in airports, hotels or shopping centres. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software on to devices,” the FBI said.

“Carry your own charger and USB cord and use an electrical outlet instead.”

9. **Cybercriminals use simple trick to obtain personal data (Help Net Security, 10 APR)**

People reveal more personal information when you ask them the same questions a second time – according to new research from the University of East Anglia.

A new study reveals how simple repetition can make people over-disclose, and potentially put themselves at risk of identity theft and cybercrime.

The research team say that understanding why people disclose personal data could help inform measures to address the problem.

10. **IoT Hack Enables Cybercriminals to Steal Cars (Ubergimo, 8 APR, Paulo Montenegro)**

In a new fashion for stealing cars, automotive security experts have discovered that cybercriminals can hack into a vehicle’s control system through the headlight. The control system is managed by the controller area network (CAN) bus, an Internet of Things (IoT) protocol that allows devices and microcontrollers to communicate with each other within the car.

By manipulating the electronic control unit (ECU) in a Toyota RAV4’s headlight, attackers could access the CAN bus and gain control of the car. This approach, as described in a blog post by Canis Automotive Labs CTO Ken Tindell, is a unique way of car hacking that had not been seen before. Once connected through the headlight, the attackers could gain access to the CAN bus, responsible for functions like the parking brakes, headlights, and smart key, and then into the powertrain panel where the engine control is located.

11. **Stopping cybercriminals from abusing security tools (Microsoft, 06 APR, Amy Hogan-Burney)**

    Microsoft's Digital Crimes Unit (DCU), cybersecurity software company Fortra™ and Health Information Sharing and Analysis Center (Health-ISAC) are taking technical and legal action to disrupt cracked, legacy copies of Cobalt Strike and abused Microsoft software, which have been used by cybercriminals to distribute malware, including ransomware. This is a change in the way DCU has worked in the past – the scope is greater, and the operation is more complex. Instead of disrupting the command and control of a malware family, this time, we are working with Fortra to remove illegal, legacy copies of Cobalt Strike so they can no longer be used by cybercriminals.

12. **How AI is transforming cybersecurity for better and worse (Help Net Security, 05 APR, Matt Aldridge)**

    Many sectors view AI and machine learning with mixed emotions, but for the cybersecurity industry, they present a double-edged sword. On the one hand, AI provides powerful tools for cybersecurity professionals, such as automated security processing and threat detection. On the other hand, cybercriminals have access to the same technology, making it a constant cat-and-mouse game between attackers and defenders.

Electronic Warfare

1. **South Korea to develop electronic warfare aircraft, buy helicopters (C4ISRNet, 14 APR, Mike Yeo)**

   South Korea's defense procurement agency has approved two major acquisition programs, paving the way for the country to develop a new electronic warfare aircraft and buy new heavy-lift helicopters.

   The Defense Acquisition Program Administration announced Thursday its approval of a $1.41 billion program to develop a new airborne electronic warfare platform. The project is expected to run from 2024 to 2032, and the new aircraft will seek to improve joint operational capabilities and the survivability of the country's air assets by jamming and disrupting adversarial air defenses as well as command and communications systems.

2. **Jam The Weapons And Comms: The Future Of Conflict Is Electronic Warfare (EW) (1945. 10 APR, Kris Osborn)**

   Jamming weapons guidance systems, "blinding" an enemies' targeting sensors, disabling communications systems and interfering with radar systems are all critical future warfare missions potentially performed by electronic warfare systems, or EW.

   Dominating the electromagnetic spectrum is fast becoming a heavily prioritized area of future warfare focus given the growing extent to which networks and weapons systems rely upon electronics. A precision-guided weapon, for example, cannot hit its target if its RF guidance is interfered with or jammed by an EW.

3. **China's Massive Fleet Of Radar Planes And The Strategy Behind It (The Drive, 05 APR, Andreas Rupprecht & Thomas Newdick)**

   China's path to fielding airborne early warning aircraft wasn't straightforward, but has yielded big results that speak to a wider strategy.

   While the rapid pace of developments across China's military aerospace domain has been widely reported, the focus has typically been weighted toward fighter jets and, to a lesser extent, bombers. But with China having increasingly embraced the tenets of modern airpower, airborne early warning and control (AEW&C) platforms now play a critical and remarkably expansive role within its air force and navy. A sometimes-complex development path has led to a range of different in-service solutions for this mission. The fact that China's AEW&C fleet dwarfs that of the U.S. and is far younger in age is also a major factor to consider and underlines China's unique strategic mindset. With all that in mind, an in-depth survey of the Chinese military's AEW&C capabilities is long-overdue.

4. **Chinese spy balloon gathered intelligence from sensitive U.S. military sites, despite U.S. efforts to block it (NBC News, 03 APR, Courtney Kube & Carol E. Lee)**

   The Chinese spy balloon that flew across the U.S. was able to gather intelligence from several sensitive American military sites, despite the Biden administration's efforts to block it from doing so, according to two current senior U.S. officials and one former senior administration official.

   China was able to control the balloon so it could make multiple passes over some of the sites (at times flying figure-eight formations) and transmit the information it collected back to Beijing in real time, the three officials said. The intelligence China collected was mostly from electronic signals, which can be picked up from weapons systems or include communications from base personnel, rather than images, the officials said.

5. **Soldiers innovating technology, refining tactical concepts, and strengthening partnerships (DVIDS, 03 APR, Steven Stover)**

Soldiers from the 11th Cyber Battalion, 780th Military Intelligence (MI) Brigade (Cyber), U.S. Army Cyber Command (ARCYBER) refined tactical Cyber-Electromagnetic Activities (CEMA) concepts for the Army during an Operational Readiness Assessment here in late March 2023.

For the event the 11th Expeditionary CEMA Teams (ECTs) employed innovative technology with assistance from experts from the Army Cyber Institute (ACI) at the U.S. Military Academy at West Point, the Army Program Executive Office – Intelligence, Electronic Warfare and Sensors (PEO IEW&S) and industry partners, along with training with the Combat Mission Team, Detachment-Hawaii, 782nd MI Battalion (Cyber).

Information Advantage

1. **Using Big Data Analytics to Enhance Cybersecurity Measures (Data Floq, 15 APR, Ali Ahmad)**

   Big data refers to the vast amount of structured and unstructured data that is generated by individuals, businesses, and organizations every day. It includes text, images, videos, social media interactions, transaction histories, and other digital footprints. However, big data is not just about the volume of data but also its velocity, variety, veracity and value.

   In recent years there has been an exponential growth in big data analytics as businesses seek to harness its potential for insights into customer behavior patterns, market trends and business optimization. One area where big data analytics has shown great promise is cybersecurity. With cyberattacks becoming increasingly sophisticated and frequent in nature- leveraging AI to detect anomalies in network traffic or implementing predictive analysis on user behaviour can help prevent attacks before they occur.

2. **Russia calls US intel leaks and Jack Teixeira arrest a 'planned disinformation campaign' (iNews, 14 APR, Kieron Monks)**

   Russian media and security sources suggest the leaks could be serving a purpose for Ukraine's benefit

   Russian commentators reacted with a mix of suspicion, scepticism and, in some cases, alarm to the leak of classified US intelligence files and the arrest of a 21-year-old national guardsman.

3. **Israel military builds up AI battlefield tech to hunt Hamas terrorists, protect against Iran threat (Fox News, 14 APR, Peter Aitken & Yonat Friling)**

   IDF understands AI presents 'leap forward' for its forces

   The Israel Defense Forces (IDF) believes that integrating artificial intelligence (AI) into military operations presents "a leap forward," but researchers have raised concerns about the potential escalation AI would create on the battlefield.

4. **China's military kicks off debate on use of ChatGPT with article in official PLA newspaper (SCMP, 14 APR, Zhang Tong)**

   The analysis looking at how the armed forces could use the AI software highlights its potential for information gathering and cognitive warfare

   The article also looks at AI's general weaknesses, saying human innovation could provide a key edge over the technology

5. **Cybercriminals Now Using Psychology To Target Remote Burned-Out Workers (Freelance Informer, 12 APR, Staff Reporter)**

   4 in 5 ransomware attacks include threats beyond data encryption and are now focusing on emotional manipulation, according to CyberEdge Group's Cyberthreat Defense Report (CDR). A cybersecurity awareness expert with a background in psychology offers his tips on what to do if you believe you are being targeted by a cyberattack

6. **Tackling misinformation and disinformation (LGiU, 12 APR, Malcolm Powers)**

   Ours is an age of misinformation and disinformation. From spin and marketing to 'gaslighting' and deliberate mistruths, delivered via a range of media from radio and tv, to social media and messaging apps. While misinformation and disinformation have long been used as a tool in politics to promote or challenge a particular point of view there is increasing evidence that democracy and democratic institutions at a global, national and local level are under increasing threat as a result of the scale and pace at which misinformation can spread as a result of these technologies.

7. **Leak or hack? Information or disinformation? Russian or US ploy? A quick guide to leaked top secrets (The Age, 11 APR, Eric Nagourney)**

   Leak or hack? Information or disinformation? A coup for Russia or a ploy by the United States?

   Days after US intelligence documents, some marked "top secret", were found circulating on social media, questions remain about how dozens of pages from Pentagon briefings became public and how much stock to put in them.

8. **A QUICK GUIDE TO THE HISTORY OF BIG DATA (Baseline Mag, 11 APR, Sunil Yadav)**

   In the history of big data, no one knows exactly how the term Big Data originated. It has been used since the 1990s. John R. Mashey, a Silicon Graphics professional, is credited with popularizing the term. It may surprise many that Big Data is not a term coined in recent years. Data analysis and techniques related to analysis were used by people over the course of centuries to help them make better decisions. The speed and volume of data generation have increased incredibly over the last two decades. It is now reached a level where it has sprung beyond measures of human comprehension.

9. **China releases new AI rules as tech giant Alibaba unveils ChatGPT rival (Independent, 11 APR, Vishwam Sankaran)**

   Alibaba working on ChatGPT rival Tongyi Qianwen, which it plans to integrate across its services

   Regulators in China have unveiled new draft rules to manage how companies develop artificial intelligence tools like ChatGPT.

   The draft rules by the Cyberspace Administration of China seek to manage fast-developing Generative AI tools after tech giants like Alibaba and Baidu announced their plans to roll out their own version of the AI chatbot.

10. **Making Unilateral Norms for Military AI Multilateral (Lawfare, 06 APR, Michael Depp)**

    The speed and pitfalls of artificial intelligence (AI) development are on public display thanks to the race for dominance among leading AI firms following the public release of ChatGPT. One area where this "arms race" mentality could have grave consequences is in military use of AI, where even simple mistakes could cause escalation, instability, and destruction. In an attempt to mitigate these risks, the State Department released the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. The declaration is a good step toward improving the global conversation around AI in military systems. The United States can work with its closest allies to turn this unilateral statement into a multilateral commitment to promote norms for military AI use around the globe.

Signal

1. **Space Force to propose plan to acquire high-capacity satellite communications (SpaceNews, 11 APR, Sandra Erwin)**

   In an effort to keep up with the ever-increasing demands of U.S. military services, the Space Force will propose a new plan to acquire high-capacity satellite communications.

   Senior members of the Joint Chiefs of Staff are set to be briefed on this plan in the coming weeks, said Lt. Gen. Philip Garrant, deputy chief of space operations for strategy, plans, programs and requirements

2. **The Top Five Challenges Of Zero-Trust Security (Forbes, APR 11, Lior Yaari)**

   Zero-trust security is a model that has gained popularity as an effective solution to ensure that only authorized users can access critical information. With the rise of remote work and SaaS services, the traditional perimeter security models to protect endpoints and devices are no longer sufficient. Zero-trust security is important as it provides a more comprehensive approach to security, ensuring that only authorized users can access the data or applications they need.

3. **Report: U.S. military satellite antennas overdue for upgrades (SpaceNews, 10 APR, Sandra Erwin)**

   The ground terminals used to operate U.S. military and intelligence satellites are running out of capacity and in dire need of upgrades, warns a new report from the Government Accountability Office.

   GAO auditors spent more than a year investigating the state of the Satellite Control Network, operated by the U.S. Space Force. The network of 19 parabolic antennas, first established in 1959, is distributed across seven locations around the world.

   The SCN is facing “obsolescence challenges and potential capacity gaps as DoD and other agencies launch more satellite systems that will rely on the network,” says GAO in the report released April 10.

4. **Potential Starlink use for Taiwan discussed by US lawmakers, TW President: Report (Teslarati, 09 APR, Maria Merano)**

   During a recent visit to Taipei, Taiwan, US House Foreign Affairs Committee Chairman Michael McCaul and Arkansas Representative French Hill reportedly held talks with Taiwan President Tsai Ing-wen about the potential use of Elon Musk’s Starlink to help Taiwan.

   McCaul and Hill had described the discussion as one of the “constructive takeaways” from their meeting with Tsai. During their talks, the group reportedly discussed the possibility of using Starlink to bolster Taiwan’s deterrence capabilities against China, Bloomberg News reported.

5. **China’s military aims to launch 13,000 satellites to rival Elon Musk’s Starlink (The Washington Post, 06 APR, Cate Cadell)**

   In the race for low-earth orbit dominance, Beijing is years behind SpaceX and worried about the threat to its national security

   Chinese military researchers are calling for the rapid deployment of a national satellite network project to compete with SpaceX’s Starlink, over concerns that Elon Musk’s internet-beaming satellites pose a major national security threat to Beijing following their successful use in the Ukraine war.

6. **Unlocking the true potential of IoT with low cost satellite communications (African Wireless Communications, 05 APR, Eric Ménard)**

   With an expected 5.2 billion connected devices by 2025, IoT is now a fundamental component of both government policy and corporate strategy. The ability to track, monitor, record and analyse through an extraordinary array of hugely innovative sensors has already transformed many businesses and industries. But, to date, the true power of IoT has been constrained by the limits of fixed and wireless connectivity: just 15% of the planet is currently covered by affordable, accessible IoT connection.

   If organisations are to truly harness the power and sophistication of IoT, connectivity must extend around the globe. It needs to be both affordable and accessible – yet the only alternative to wireless networks has been satellite IoT at a price point that cannot be justified by most businesses or use cases. Until now.

7. **If you hate Starlink, you're not going to like that China is working on its own mega constellation (Space Explored, 01 APR, Seth Kurkowski)**

   In 2019, SpaceX launched its first batch of 60 Starlink satellites. Since then, there have been two sides of the mega constellation debate: those that support and fear them. While I wish I could answer which of those sides is correct, I can only provide the latter more to worry about because China is entering stage right.

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, 14 April 2023

Russia-Ukraine Situation Report, 13 April 2023

Russia-Ukraine Situation Report, 12 April 2023

Russia-Ukraine Situation Report, 11 April 2023

Russia-Ukraine Situation Report, 10 April 2023

Russia-Ukraine Situation Report, 07 April 2023

Russia-Ukraine Situation Report, 06 April 2023

Russia-Ukraine Situation Report, 05 April 2023

Russia-Ukraine Situation Report, 04 April 2023

Russia-Ukraine Situation Report, 03 April 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Ukraine Situation Report: Official hints At New Weapons To Be Unleashed On Crimea - 14 APR
Ukraine Situation Report: Norwegians Laud Kyiv’s Tank Crews – 13 APR
Ukraine Situation Report: Russia Building Up Zaporizhzhia Fortifications - 12 APR
Ukraine Situation Report: Denmark To Decide By Summer On F-16s For Kyiv - 11 APR
Ukraine Situation Report: Russia Adding ‘Cope Cages’ To TOS-1A - 10 APR
Ukraine Situation Report: Both Sides Rationing Shells Ahead Of Kyiv’s Counteroffensive - 08 APR
Ukraine Situation Report: Russian Border Towns Hit With Onslaught Of Attacks - 06 APR
Ukraine Situation Report: Latest U.S. Aid Package Includes New Drone Defenses – 04 APR
Ukraine Situation Report: Polish MiG-29s Delivered – 03 APR

3. US intelligence was aware of four extra Chinese spy balloons, leaked Pentagon data reveals (Independent, 15 APR, Maroosha Muzaffar)

The leaked documents also detail a lack of ‘strong senior’ oversight of the balloon surveillance program

US intelligence agencies were reportedly aware of four extra Chinese spy balloons, according to leaked top-secret data from Pentagon.

The data leaked to a Discord chatroom by Jack Teixeira, a member of the Massachusetts Air National Guard, reveals that the US intelligence knew of at least four Chinese spy balloons that traversed the US airspace.

4. U.S. arrests 21-year-old National Guardsman for online intelligence leaks (Reuters, 14 APR, Ross Kerber & Sarah N. Lynch)

The FBI on Thursday arrested Jack Douglas Teixeira, a 21-year-old member of the U.S. Air National Guard, over the leaks online of classified documents that embarrassed Washington with allies around the world.

Federal agents in an armored car and military gear swooped in on Teixeira, dressed in gym shorts, a T-shirt and trainers, at his home in Dighton, Massachusetts, a mostly wooded town of 8,000 about 50 miles (80 km) south of Boston.

5. US, Ukraine say many war secrets safe from intel leaks (C4ISRNet, 13 APR, Ellen Knickmeyer & Hanna Arhirova)

Ukraine's leaders say they don't see a major U.S. intelligence leak as gravely damaging future offensives. A key reason: They have long held back on sharing their most sensitive operational information, doubting Washington's ability to keep their secrets safe.

Ukrainian and U.S. officials said this week that only Ukrainians know some battle plans and other operational information, not the Americans, their most important ally. That means the leak of secret military documents, including some assessing Ukraine's battlefield strengths and weaknesses against Russia, may not have been enough — so far — to change the course of the war.

6. Russian T-90 Tank From Ukraine Mysteriously Appears At U.S. Truck Stop (The Drive, 13 APR, Howard Altman)

The tank was apparently captured by Ukraine last fall, but it is unclear how or why it ended up in Louisiana.

The folks at Peto's Travel Center and Casino in Roanoke, Louisiana see all kinds of vehicles pull up, but Tuesday night was different. What ended up in their parking lot is certainly something of a mystery, to say the least.

Someone left a Russian T-90A tank, which open source intelligence (OSINT) trackers say was captured by Ukraine last fall, on a trailer after the truck hauling it broke down and pulled into this truck stop off U.S. Interstate 10. An employee at Peto's, and the individual who first posted the images on Reddit, shared them with The War Zone.

7. Foreign Reflections on U.S. Exercises and Operations, 13 April 2023 (U.S. Army Asian Studies Detachment, 13 APR)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 6 to 12 April 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, India, North Korea, and the Philippines

8. Damage Assessment From Major War Plans Leak Underway In U.S., Ukraine (The Drive, 07 APR, Howard Altman)

The classified documents could become a problem for the sharing of sensitive information between Ukraine and the U.S., as well as others.

Ukrainian intelligence and military officials are analyzing whether documents leaked about U.S. and NATO plans to support Kyiv ahead of the looming spring counteroffensive are real and what damage was caused to future efforts if they are.

“Right now we are checking and comparing these materials” in the documents, Maj. Gen. Kyrylo Budanov, head of Ukraine’s Defense Intelligence Directorate, told The War Zone Friday.

9. Foreign Reflections on U.S. Exercises and Operations, 06 April 2023 (U.S. Army Asian Studies Detachment, 06 APR)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 30 March to 5 April. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, India, Japan, Nepal, the Philippines, and South Korea.