



Cyber Center of Excellence

Unclassified Threat Read Book

01 - 15 JUL 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

1. [Cyberespionage and used car salesmen. Email extortion through embarrassment, not encryption. The personal is the professional. And a look back at Patch Tuesday](#) - 12 JUL
2. [Inside the Mind of the Hacker: Report Shows Speed and Efficiency of Hackers in Adopting New Technologies](#) – 12 JUL
3. [Microsoft Warns of Office Zero-Day Attacks, No Patch Available](#) – 11 JUL
4. [Zero-Day Exploits: A Cheat Sheet for Professionals](#) – 11 JUL
5. [Russian-Linked RomCom Hackers Targeting NATO Summit Guests](#) – 11 JUL
6. [Storm-0978 attacks reveal financial and espionage motives](#) – 11 JUL
7. [How To Address Cyber Threats Facing Uncrewed Military Vehicles](#) – 11 JUL
8. [South Korea, NATO to boost partnership on security, cyber threats](#) – 11 JUL
9. [Staying Ahead of Cyber Threats: Innovations in Cybersecurity and Phishing Mitigation](#) – 10 JUL
10. [8 Most Common Ways Hackers Exploit Computers](#) – 09 JUL
11. [You need to check your phone for these popular apps sending pictures and other info to China](#) – 08 JUL
12. [The five-day job: A BlackByte ransomware intrusion case study](#) – 6 JUL
13. [China releases its first open-source computer operating system](#) – 06 JUL
14. [Recent Chinese cyber intrusions signal a strategic shift](#) – 05 JUL
15. ['Cyber battlefield' map shows attacks being played out live across the globe](#) – 03 JUL
16. [Ransomware criminals are dumping kids' private files online after school hacks](#) – 05 JUL

Electronic Warfare

1. [Senators eye electronic warfare capability demonstration in western US](#) – 14 JUL
2. [US military losing electronic warfare 'muscle memory,' CQ Brown warns](#) – 12 JUL
3. [July Spectrum SitRep](#) – 06 JUL
4. [Ukraine confirms: Russian EWs jam US GPS munition, HIMARS, JDAMs](#) – 06 JUL
5. [US Precision-Guided Missiles "FLOP" In Ukraine; Kyiv Admits Russia's Electronic Warfare Systems Taking A](#) –
6. [North Korean satellite wasn't advanced enough to conduct reconnaissance from space, Seoul says](#) – 04 JUL
7. [Russia's electronic warriors are intercepting Ukrainian troops' communications and jamming their GPS-guided bombs, experts say](#) – 03 JUL

Information Advantage

1. [Prigozhin's troll factories in Russia: what's next?](#) – 13 JUL
2. [US Tech Firms 'Win Big' From Ukraine War, Turn The Region Into A Testing Ground For AI Warfare – Chinese Media](#) – 11 JUL
3. [Cuba says US responsible for 2021 protests, biggest in decades](#) – 10 JUL
4. [Foreign Reflections on U.S. Exercises and Operations, 7 July](#) – 7 JUL
5. [Russia 'Hell-Bent' On Destroying Western-Supplied Weapons & Win Info War – Ukrainian General Hints](#) – 07 JUL
6. [China aims to sap Taiwan morale with 'escape plan' misinformation, sources say](#) – 06 JUL
7. [Russia spreads disinformation in Spanish-speaking world](#) – 06 JUL
8. [China buzzes Taiwan Strait again, minister decries 'disinformation' about safety](#) – 04 JUL

9.

Signal

1. [Inside the subsea cable firm secretly helping America take on China](#) – 06 JUL
2. [Pentagon review finds no 'single point of failure' in Discord leaks, proposes new office to monitor users](#) – 05 JUL
3. [11 best practices for securing data in cloud services](#) – 5 JUL

Items of Interest

1. [Russia-Ukraine Situation Report](#)
2. [The WARZONE Ukraine Situation Report](#)
3. [Deutsche Welle \(DW\) Ukraine updates](#)
4. [What Biden's Troop Call-Up Order To Europe Really Means](#) – 14 JUL
5. [Ukraine Has Already Received American Cluster Munitions](#) – 13 JUL
6. [NATO Recognizes China As 'BIG THREAT'; Russia-Centric Military Alliance Goes Beyond Europe Into Indo-Pacific](#) – 13 JUL
7. [Wagner Turns Over 2,000 Heavy Weapons Including Tanks, SAM Systems](#) – 12 JUL,
8. [NATO summit: G7 Leaders announce Ukraine security framework](#) – 12 JUL
9. ['Barbie' Map Of China's Nine-Dash Line Erupts Into Controversy; Comes After Philippines Vessel Incident](#) – 10 JUL
10. [North Korea repeatedly complains of US 'spy planes'](#) –10 JUL
11. [North Korea Threatens To Down US Spy Planes Violating Its Airspace](#) – 10 JUL
12. [Is Ukraine Using Old S-200 SAMs In The Land-Attack Role?](#) – 10 JUL
13. [Watch Six AK-74s Strapped Together As A Ukrainian Anti-Drone Gun In Action](#) – 07 JUL
14. [What DPICM Cluster Munitions Are And Why Ukraine Wants Them So Bad](#) – 06 JUL,
15. [China Fires 'Warning Salvo' In A Direct Threat To US; Can Choke The World By Blocking Lithium, Rare Earth & API Supply](#) – 06 JUL
16. [China has had a spy base in Cuba for decades, former intelligence officer](#) – 05 JUL
17. [Chinese Responses to Wagner Mutiny Attempt](#) – 05 JUL

Cyber

17. [**Cyberespionage and used car salesmen. Email extortion through embarrassment, not encryption. The personal is the professional. And a look back at Patch Tuesday.**](#) (The Cyber Wire, 12 JUL, Dave Bittner)

A Chinese threat actor hits US organizations with a Microsoft cloud exploit. Open source tools allow threat actors to exploit a loophole in Microsoft's kernel driver authentication procedures. A RomCom update. Beamer phishing, email extortion attacks and digital blackmail. A new report concludes companies allowing personal employee devices onto their network are opening themselves to attack. Tim Starks from the Washington Post looks at Microsoft's recent woes. Our guest is Eyal (aye-AL) Benishti from IRONSCALES with insights on business email compromise. And a July Patch Tuesday retrospective.

18. [**Inside the Mind of the Hacker: Report Shows Speed and Efficiency of Hackers in Adopting New Technologies**](#) (Security Week, 12 JUL, Kevin Townsend)

Bugcrowd's Inside the Mind of the Hacker report shows the speed and efficiency of hackers adopting new technologies to assist their hunting

The application of artificial intelligence is still in its infancy, but we are already seeing one major effect: the democratization of hacking.

The annual Bugcrowd report, Inside the Mind of a Hacker 2023, examines the attitudes held and methods used by the Bugcrowd pool of bug hunters. This year, the report focuses on the effect and use of artificial intelligence (AI) by hackers.

It also provides valuable insight into how malicious hackers will employ AI. For now, this is centered around the use of LLM GPTs, such as ChatGPT. There are numerous 'specialist' GPTs appearing, but for the most part they are wrappers around the GPT4 engine. ChatGPT remains the primary tool of hackers.

19. [**Microsoft Warns of Office Zero-Day Attacks, No Patch Available**](#) (Security Week, 11 JUL, Ryan Naraine)

Patch Tuesday: Microsoft calls attention to a series of zero-day remote code execution attacks hitting its Office productivity suite.

Russian spies and cybercriminals are actively exploiting still-unpatched security flaws in Microsoft Windows and Office products, according to an urgent warning from the world's largest software maker.

In an unusual move, Microsoft documented "a series of remote code execution vulnerabilities" impacting Windows and Office users and confirmed it was investigating multiple reports of targeted code execution attacks using Microsoft Office documents.

20. [**Zero-Day Exploits: A Cheat Sheet for Professionals**](#) (Tech Republic, 11 JUL, Lance Whitney)

This guide covers everything you need to know about zero-day security exploits, which are secret vulnerabilities used by hackers to infiltrate PCs, networks, mobile phones and IoT devices.

21. [**Russian-Linked RomCom Hackers Targeting NATO Summit Guests**](#) (Security Week, 11 JUL, Ionut Arghire)

As part of a recently identified cyber operation, a Russia-linked threat actor known as RomCom has been targeting entities supporting Ukraine, including guests at the 2023 NATO Summit taking place July 11-12, the cybersecurity unit at BlackBerry reports.

Taking place in Vilnius, Lithuania, the NATO Summit has on the agenda talks focusing on the war in Ukraine, as well as new memberships in the organization, including Sweden and Ukraine itself.

22. [Storm-0978 attacks reveal financial and espionage motives \(Microsoft, 11 JUL, Microsoft Threat Intelligence\)](#)

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, which included a remote code execution vulnerability exploited before disclosure to Microsoft via Word documents, using lures related to the Ukrainian World Congress.

23. [How To Address Cyber Threats Facing Uncrewed Military Vehicles \(Forbes, 11 JUL, Tim Reed\)](#)

To maintain a defensive edge over its adversaries, the military is always looking for ways to modernize and innovate. One area that has seen significant progress in recent years is the development and use of uncrewed vehicles on land, sea and air. These crafts operate without humans onboard, making them suitable for traversing hazardous or unpleasant environments for humans and for jobs that meet “the three Ds”—difficult, dull and dangerous.

Uncrewed military vehicles have become essential assets to most militaries in the 21st century and have been used for decades to conduct surveillance and reconnaissance, attack remote targets, perform search and rescue and more. With today’s advanced AI, these vehicles are leveraging machine learning technologies that can be used to detect objects, recognize and track targets and classify or segment images and video footage.

24. [South Korea, NATO to boost partnership on security, cyber threats \(Reuters, 11 JUL, Hyonhee Shin\)](#)

South Korea and NATO will expand cooperation on global security issues including Ukraine and North Korea their leaders said on Tuesday on the sidelines of NATO’s annual meeting in Lithuania, the South Korean presidential office said.

President Yoon Suk Yeol arrived in Vilnius on Monday for the summit of NATO leaders, aiming to step up security ties in the face of evolving nuclear threats from North Korea and tension over China.

25. [Staying Ahead of Cyber Threats: Innovations in Cybersecurity and Phishing Mitigation \(Hacker Noon, 10 JUL, Ascend Agency\)](#)

In our digital world, cyber threats continually menace the safety of individuals and corporations alike. Phishing, an insidious tactic whereby cybercriminals manipulate unsuspecting users into divulging sensitive information, is especially prevalent. This deceptive practice continually evolves, growing more sophisticated with each passing day. To counter this escalating threat, the field of cybersecurity has witnessed remarkable technological progress, the aim of which is to keep pace with these malicious advances and offer effective mitigation strategies.

26. [8 Most Common Ways Hackers Exploit Computers \(Make Use Of, 09 JUL, Katie Rees\)](#)

How do cybercriminals actually take your money and data? Here are a few common methods hackers and scammers target you.

Hackers are always looking for new ways to get their hands on your money and data, but there are a few common avenues they tend to most commonly pursue. So what are the top methods hackers use to exploit computers?

27. [**You need to check your phone for these popular apps sending pictures and other info to China**](#) (Phone Arena, 08 JUL, Anam Hamid)

Although Play Store is generally a trusted place for downloading apps on Android phones, every now and then malicious apps manage to sneak into the app marketplace. The latest fishy apps that were found hiding on Play Store are File Recovery & Data Recovery and File Manager.

Cyber security company Pradeo says that these apps came from the same developer and were downloaded by 1.5 million users. They look like file management apps but are actually spyware and silently send user information to servers based in China.

28. [**The five-day job: A BlackByte ransomware intrusion case study**](#) (Microsoft, 6 JUL, Microsoft Incident Response)

As ransomware attacks continue to grow in number and sophistication, threat actors can quickly impact business operations if organizations are not well prepared. In a recent investigation by Microsoft Incident Response (previously known as Microsoft Detection and Response Team – DART) of an intrusion, we found that the threat actor progressed through the full attack chain, from initial access to impact, in less than five days, causing significant business disruption for the victim organization.

29. [**China releases its first open-source computer operating system**](#) (Reuters, 06 JUL, Josh Ye)

China has released its first homegrown open-source desktop operating system, named OpenKylin, state media said, as the country steps up efforts to cut reliance on U.S. technology.

Released on Wednesday, and based on the existing open-source Linux operating system, China's version was built by a community of about 4,000 developers, and is used in its space programme and industries such as finance and energy, they added.

30. [**Recent Chinese cyber intrusions signal a strategic shift**](#) (Australian Strategic Policy Institute The Strategist, 05 JUL, Pukhraj Singh)

On 25 May, Australia and its partners in the Five Eyes intelligence-sharing network—Canada, New Zealand, the UK and the US—made a coordinated disclosure on a state-sponsored cyber hacking group dubbed 'Volt Typhoon'. The group has been detected intruding on critical infrastructure since 2021, but the nature of recent intelligence on its behaviour hints at worrying developments in the Chinese cyber establishment. While the Five Eyes' disclosure is direct in its attribution of Volt Typhoon to the Chinese government, there are many layers that need to be peeled away to reveal the true nature, and implications, of the threat.

31. [**'Cyber battlefield' map shows attacks being played out live across the globe**](#) (Metro, 03 JUL, Josh Layton)

A live map is monitoring cyber attacks across the globe at a time when the war in Ukraine is fuelling a 'significant increase' in hostile activity.

UNCLASSIFIED

The dashboard gives a startling picture of the digital frontline, where more than 850 assaults are launched against UK targets every week on average.

Updating in real-time, the technology uses intelligence collected from a sophisticated artificial intelligence-powered system called ThreatCloud AI.

The most commonly targeted countries and industries are shown, with the map covering malware, phishing and 'exploit' attacks.

32. **[Ransomware criminals are dumping kids' private files online after school hacks](#)** (APNews, 05 JUL, Frank Bajak, Heather Hollingsworth & Larry Fenn)

The confidential documents stolen from schools and dumped online by ransomware gangs are raw, intimate and graphic. They describe student sexual assaults, psychiatric hospitalizations, abusive parents, truancy — even suicide attempts.

"Please do something," begged a student in one leaked file, recalling the trauma of continually bumping into an ex-abuser at a school in Minneapolis. Other victims talked about wetting the bed or crying themselves to sleep.

Complete sexual assault case folios containing these details were among more than 300,000 files dumped online in March after the 36,000-student Minneapolis Public Schools refused to pay a \$1 million ransom. Other exposed data included medical records, discrimination complaints, Social Security numbers and contact information of district employees.

Electronic Warfare

1. [Senators eye electronic warfare capability demonstration in western US](#) (Defense News, 14 JUL, Colin Demarest)

The U.S. military would be required to test its electronic warfare and information influence prowess in a future, interstate experiment, if lawmakers get their way.

Included in a Senate version of fiscal 2024 defense legislation is a provision for a “Western regional range complex demonstration,” in which multiple services would together evaluate capacities to communicate, gather intelligence, conduct offensive and defensive cyber operations, and jam and spoof.

2. [US military losing electronic warfare ‘muscle memory,’ CQ Brown warns](#) (Defense News, 12 JUL, Colin Demarest)

The U.S. Department of Defense’s ability to fend off attacks on the electromagnetic spectrum has atrophied over decades, leaving troops vulnerable on the high-tech battlefields of tomorrow, according to President Joe Biden’s pick to be the nation’s highest-ranking military officer.

Air Force Chief of Staff Gen. CQ Brown, nominated in May to be the next chairman of the Joint Chiefs of Staff, told senators this week at his confirmation hearing that the military “has lost some muscle memory” when it comes to electronic warfare after spending years fighting lesser-equipped forces, namely in the Middle East.

3. [July Spectrum SitRep](#) (Armada International, 06 JUL, Dr. Thomas Withington)

Armada’s monthly round-up of all the latest electronic warfare news in the product, programme and operational domains.

4. [Ukraine confirms: Russian EWs jam US GPS munition, HIMARS, JDAMs](#) (Bulgarian Military, 06 JUL, Boyko Nikolov)

As the Ukraine conflict unfolds, there’s a growing concern among military analysts and experts. The US-made guided weapons supplied to Kyiv are reportedly losing their effectiveness due to Russian electronic jamming, causing a significant shift in battlefield dynamics.

5. [US Precision-Guided Missiles “FLOP” In Ukraine; Kyiv Admits Russia’s Electronic Warfare Systems Taking A Toll](#) (The EurAsian Times)

Military analysts and experts ardently following the ongoing Ukraine war have warned for quite some time that US-made guided weapons sent to Kyiv have lost their sheen and can no longer hit targets accurately due to Russia’s electronic jamming.

6. [North Korean satellite wasn’t advanced enough to conduct reconnaissance from space, Seoul says](#) (APNews, 04 JUL, Hyung-Jin KIM)

SEOUL, South Korea (AP) — The satellite North Korea failed to put into orbit wasn’t advanced enough to conduct military reconnaissance from space as it claimed, South Korea’s military said Wednesday after retrieving and studying the wreckage.

UNCLASSIFIED

North Korea had tried to launch its first spy satellite in late May, but the long-range rocket carrying it plunged into the waters off the Korean Peninsula's west coast soon after liftoff. The satellite was to be part of a space-based reconnaissance system North Korea says it needs to counter escalating security threats from South Korea and the United States.

South Korea mobilized navy ships, aircraft and divers to recover debris from the rocket and satellite in a 36-day operation that ended Wednesday, the South's Joint Chiefs of Staff said in a statement.

7. [Russia's electronic warriors are intercepting Ukrainian troops' communications and jamming their GPS-guided bombs, experts say](#) (Business Insider, 03 JUL, Michael Peck)

Russian jamming has become so effective that Ukraine — as well as the US and NATO — can no longer assume that Joint Direct Attack Munition glide bombs and other smart weapons will hit their targets.

That's the conclusion of an analysis by Britain's Royal United Services Institute. "Jamming is not causing the JDAMs to stop working, but it is risking their accuracy," according to RUSI researcher Thomas Withington.

Information Advantage

1. [Prigozhin's troll factories in Russia: what's next?](#) (DW, 13 JUL, Ilya Koval)

After a failed mutiny, Yevgeny Prigozhin, head of the Wagner Group, has reportedly shut down his media group. But experts and observers warn this won't be the end of fake news and online trolls from Russia.

2. [US Tech Firms 'Win Big' From Ukraine War, Turn The Region Into A Testing Ground For AI Warfare – Chinese Media](#) (The EurAsian Times, 11 JUL, Ashish Dangwal)

China has leveled allegations that US military and technology companies are reaping financial gains from the Russia-Ukraine conflict by exploiting it as a testing ground for "AI warfare."

On July 6, the Global Times (GT), a state-backed media outlet in China, published a report that suggests that the US military and some Western technology companies view the Russia-Ukraine conflict as an opportunity for a "shortcut to profit" and as a suitable testing environment for their new AI technologies and products.

Citing a recent Bloomberg story, the Chinese media report shed light on the financial trajectory of Blake Resnick, a 23-year-old US entrepreneur. The article details how Resnick amassed a net worth surpassing \$100 million through a combination of donations and the sale of his drones to Ukraine.

3. [Cuba says US responsible for 2021 protests, biggest in decades](#) (Reuters, 10 JUL, Nelson Acosta)

Cuba on Monday accused the U.S. government of bearing "direct responsibility" for the protests that rocked the Caribbean island two years ago, marking the largest demonstrations since Fidel Castro's 1959 revolution.

"The United States has a direct responsibility for the disturbances of July 11 and 12, 2021," the Communist Party-run Granma newspaper said in a front-page editorial ahead of the anniversary of the protests. It provided no evidence to back the accusations.

4. [Foreign Reflections on U.S. Exercises and Operations, 7 July 2023](#) (U.S. Army Asian Studies Detachment, 7 JUL)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 30 June to 6 July 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, and the Philippines.

5. [Russia 'Hell-Bent' On Destroying Western-Supplied Weapons & Win Info War – Ukrainian General Hints](#) (The EurAsian Times, 07 JUL, Ashish Dangwal)

Russian troops are intentionally directing their efforts toward causing maximum damage and destruction to the Western-supplied military equipment of Ukraine, according to General Oleksandr Tarnavskiy, who is leading the counter-offensive in

the south.

Ukrainian troops launched a counter-offensive on the southern frontline in Zaporizhia a month ago. Using Western-supplied vehicles, they are attacking multiple fronts to regain control and push back the Russian forces.

However, while carrying out their counter-offensive, the Ukrainian Armed Forces have faced intense opposition. Russian forces have reportedly employed various tactics, including minefields and conducting extensive aerial operations involving aviation and missile strikes.

6. [China aims to sap Taiwan morale with 'escape plan' misinformation, sources say](#) (Reuters, 06 JUL, Yimou Lee)

China has launched a misinformation campaign that includes news reports Taiwan's president has an "escape plan" in the event of a Chinese invasion, aiming to sap morale as Beijing presses the island to accept its sovereignty, Taiwan officials said.

Taiwan is on high alert for what it sees as China's attempts to sway public opinion on the democratically governed island, including through illicitly funding Beijing-friendly candidates in the run-up to a presidential election next year, according to security reports reviewed by Reuters in June.

7. [Russia spreads disinformation in Spanish-speaking world](#) (DW, 06 JUL)

Russia has been bringing propaganda to its war effort in Ukraine well beyond its borders. With over 500 million speakers, Spanish is a key language for Russian propaganda, and now Russia's narrative is getting exposure in sympathetic Spanish voices.

8. [China buzzes Taiwan Strait again, minister decries 'disinformation' about safety](#) (Reuters, 04 JUL, Yimou Lee & Ben Blanchard)

Chinese fighter jets again crossed the median line of the Taiwan Strait on Tuesday, as a senior Taiwanese official decried "annoying disinformation" about how safe the island is given the mounting tensions with Beijing.

Taiwan, which China claims as its own territory despite the island's strong objections, has over the past three years reported almost daily missions by Chinese military aircraft nearby, and since last August, regular crossings of the median line that used to serve as an unofficial boundary.

Signal

1. [Inside the subsea cable firm secretly helping America take on China](#) (Reuters, 06 JUL, Joe Brock)

SubCom, a New Jersey company born out of a Cold War spy project, has become a key player in the U.S.-China tech war. It's laying internet cables on the ocean floor to boost Washington's economic and military might, including a clandestine mission to a remote island naval base, Reuters can reveal.

2. [Pentagon review finds no 'single point of failure' in Discord leaks, proposes new office to monitor users](#) (Breaking Defense, 05 JUL, Jaspreet Gill)

The review was launched in April after a 21-year-old member of the Massachusetts Air National Guard was hit with two federal charges alleging that he shared classified information about the Russia-Ukraine war on the social media platform Discord.

3. [11 best practices for securing data in cloud services](#) (Microsoft, 5 JUL, Pramiti Bhatnagar, Abbas Kudrati)

In today's digital age, cloud computing has become an essential part of businesses, enabling them to store and access their data from anywhere. However, with convenience comes the risk of data breaches and cyberattacks. Therefore, it is crucial to implement best practices to secure data in cloud services.

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 July 2023

[Russia-Ukraine Situation Report](#), 13 July 2023

[Russia-Ukraine Situation Report](#), 12 July 2023

[Russia-Ukraine Situation Report](#), 11 July 2023

[Russia-Ukraine Situation Report](#), 10 July 2023

[Russia-Ukraine Situation Report](#), 07 July 2023

[Russia-Ukraine Situation Report](#), 06 July 2023

[Russia-Ukraine Situation Report](#), 05 July 2023

2. **The WARZONE Ukraine Situation Report (Howard Altman)**

[Ukraine Situation Report: Kyiv's Growing Counter-Battery Advantage](#) – 15 JUL

[Ukraine Situation Report: Wagner Begins Training Belarusian Military](#) – 14 JUL

[Ukraine Situation Report: Russian General Fired After Lambasting Shoigu](#) – 13 JUL

[Ukraine Situation Report: Antonovsky Bridgehead Holds](#) – 12 JUL

[Ukraine Situation Report: France Officially Sending SCALP Cruise Missiles](#) – 11 JUL

[Ukraine Situation Report: Kyiv's Forces Push Deeper South Near Robotyne](#) – 10 - JUL

[Ukraine Situation Report: Zelensky Blasts Bulgarian President Over Opposition To Arming Kyiv](#) – 06 JUL

[Ukraine Situation Report: A Peek Into Prigozhin's Bizarre Pad](#) – 05 JUL

[Ukraine Situation Report: Patriot Kill Marks Hint That It Downed Aircraft Inside Russia](#) – 03 JUL

[Ukraine Situation Report: Russian SAMs Can't Stop This Storm Shadow](#) – 01 JUL

3. **Deutsche Welle (DW) Ukraine updates**

[Ukraine updates: Russia fires general who criticized bosses](#) – 13 JUL

[Ukraine Situation Report: Kyiv's Forces Push Deeper South Near Robotyne](#) – 10 JUL

[Ukraine Situation Report: Zelensky Marks 500 Days Of War At Snake Island](#) – 08 JUL

[US expected to approve cluster bombs for Ukraine](#) – 07 JUL

[Mystery surrounds whereabouts of Wagner boss Prigozhin](#) – 06 JUL

[Ukraine: What's the worst-case scenario for Zaporizhzhia?](#) – 05 JUL

[Russia, Ukraine continue blame game over Zaporizhzhia](#) - 05 JUL

[Dozens injured in Russian missile strike](#) – 04 JUL

[The fate of Ukraine's abducted children](#) – 04 JUL

[What happens if Russia blocks the Ukraine grain deal?](#) – 1 JUL

4. **[What Biden's Troop Call-Up Order To Europe Really Means \(The Drive, 14 JUL, Howard Altman\)](#)**

With a strained force in Europe, the order could recall hundreds of people who left the military to take the place of deployed troops.

When President Joe Biden announced his executive order about U.S. forces in Europe on Thursday, concern ran rampant that America was beefing up for an immanent direct armed conflict with Russia.

But the reality is that the move was designed to replace some currently deployed troops and bolster some critical requirements. It was not meant to add to the 100,000 troops already stationed there — about a fifth of whom were deployed in the wake of Russia's all-out invasion. Still, it sets a new precedent and could open the door to further call-ups.

Biden's executive order called for mobilizing up to 3,000 reserve troops, of which no more than 450 could be what are known as Individual Ready Reserve (IRR) troops. Those are people who previously served but still have a contingency commitment to the military.

5. **[Ukraine Has Already Received American Cluster Munitions \(Updated\) \(The Drive, 13 JUL, Howard Altman\)](#)**

A Ukrainian general has stated that the cluster munitions will be a powerful weapon, but that they have not yet been used.

Kyiv's forces have already received controversial cluster munitions promised by the U.S. last week, a top Ukrainian general told CNN Thursday.

"We just got them, we haven't used them yet, but they can radically change [the battlefield]," Brig. Gen. Oleksandr Tarnavskiy, commander of the Tavria Joint Forces Operation, said in an interview Thursday with CNN's Alex Marquardt.

6. **[NATO Recognizes China As 'BIG THREAT'; Russia-Centric Military Alliance Goes Beyond Europe Into Indo-Pacific \(The EurAsian Times, 13 JUL, Prakash Nanda\)](#)**

The just concluded NATO summit in the Lithuanian capital of Vilnius has been dominated by the news related to the war in Ukraine and its quest for membership in what is considered the world's most formidable military alliance.

7. **[Wagner Turns Over 2,000 Heavy Weapons Including Tanks, SAM Systems \(The Drive, 12 JUL, Howard Altman\)](#)**

The Russian MoD claims Prigozhin turned over high-end weapons like T-90 tanks, howitzers and multiple launch rocket systems.

8. **[NATO summit: G7 Leaders announce Ukraine security framework \(DW, 12 JUL\)](#)**

The leaders of the G7 nations have announced a framework to protect Ukraine against any future Russian aggression. The assurances come after Ukraine missed out on a timeline for its NATO accession. DW has the latest.

9. **['Barbie' Map Of China's Nine-Dash Line Erupts Into Controversy;](#)**

[Comes After Philippines Vessel Incident](#) (The EurAsian Times, 10 JUL, Jeffrey Maitem)

The Philippine Coast Guard (PCG) accused its Chinese counterpart of dangerous maneuvers that could have caused a collision during a resupply mission in the contested South China Sea, the second incident this year.

The incident happened on June 30 near Ayungin Shoal (Second Thomas Shoal) in the West Philippine Sea. The West Philippine Sea is the name usually used by the Philippines for the part of the South China Sea within the nation's Exclusive Economic Zone (EEZ), where it holds exclusive rights to natural resources.

Speaking with reporters, Commodore Jay Tarriela, Philippines Coast Guard spokesperson for the West Philippines Sea, said they deployed BRP Malabrigo and BRP Pascua to assist the resupply mission of the Armed Forces of the Philippines.

10. [North Korea repeatedly complains of US 'spy planes'](#) (DW, 10 JUL)

Pyongyang has accused the US of violating its airspace in a series of critical comments about alleged air espionage, threatening reprisals. Seoul, meanwhile, spoke Kim Jong Un's powerful military sister, Kim Yo Jong, alleged on Tuesday that a United States spy plane entered North Korea's exclusive economic zone eight times.

11. [North Korea Threatens To Down US Spy Planes Violating Its Airspace](#) (Army Open Source Portal, 10 JUL)

North Korea on Monday threatened to shoot down any US spy planes violating its airspace and condemned Washington's plans to deploy a nuclear missile submarine near the Korean peninsula.

A spokesperson for the North's Ministry of National Defence said the United States has "intensified espionage activities beyond the wartime level", with "provocative" flights made by US spy aircraft over eight straight days this month, and one reconnaissance plane intruding into its airspace over the East Sea "several times".

12. [Is Ukraine Using Old S-200 SAMs In The Land-Attack Role?](#) (The Drive, 10 JUL, Thomas Newdick)

Russia claims Ukrainian S-200 SAMs were launched against ground targets as video emerged. Russia has claimed that Ukraine is now using Cold War-era S-200 long-range surface-to-air missiles — known to NATO as SA-5 Gammon — to attack land targets in its rear areas and in Russia itself. A video from one particular claimed strike appears to show a missile that looks very similar to an S-200 diving almost vertically onto a target, supposedly in Bryansk Oblast, in western Russia, a region that borders Ukraine.

While Russia has been using the advanced S-300 SAM — which possesses a little-known surface-to-surface capability, which can read all about here — to strike large static ground target areas in Ukraine, the use of the vintage S-200s, in this way, is a new development in this conflict. Indeed, until now there was seemingly no evidence of S-200s being used in any capacity, by Ukraine or Russia, and the incident raises many questions.

The S-200s could give Ukraine a quasi-short-range ballistic missile-like capability, and if the missiles were deeply modified, it's possible they could be far more accurate in doing so than if used in their original configuration. ged supposedly showing one of the strikes.

13. [Watch Six AK-74s Strapped Together As A Ukrainian Anti-Drone Gun In Action](#) (The Drive, 07 JUL, Oliver Parken)

It looks like something out of a post-apocalyptic Hollywood action movie and its usefulness is questionable, but it sure looks intimidating.

In the latest example of 'unconventional' improvised Ukrainian weapons, we now have video of the contraption made of half a dozen AK-74 assault rifles in action. This follows footage released two days ago which showed the same weapon, but did not depict it firing. It is now one of a variety of improvised small arms solutions — some more relevant than others — that have been pressed into service as counter-drone weapons by Ukrainian forces.

In the footage, which can be seen below, the weapon with its crosshair iron sight sits by the edge of a field as two targets fly overhead. An individual operating it proceeds to open fire at the targets with seemingly predictable results. It's unclear what type of drones the targets were specifically.

14. [What DPICM Cluster Munitions Are And Why Ukraine Wants Them So Bad](#) (The Drive, 06 JUL, Joseph Trevithick)

Cluster munitions are highly controversial, but Ukraine has its reasons why they can be crucial to unseating deeply entrenched Russian forces.

The U.S. military has confirmed that there are ongoing deliberations about the possibility of sending certain types of so-called Dual-Purpose Improved Conventional Munitions (DPICM), a family of cluster munitions, to Ukraine. A decision to provide these weapons could come at any time. Though they are highly controversial, the Ukrainians have been increasingly seeking these kinds of weapons, which could be especially useful in uprooting dug-in Russian units that inhabit created vast trench networks and for tackling large enemy formations, including some armored forces, in open terrain.

15. [China Fires 'Warning Salvo' In A Direct Threat To US; Can Choke The World By Blocking Lithium, Rare Earth & API Supply](#) (The EurAsian Times, 06 JUL, Ritu Sharma)

The tech war between China and the US just got heated as Beijing fired a warning salvo at the major world economies by restricting the export of critical minerals Germanium and Gallium, useful in mobile phones, electric vehicles, nuclear energy, and other devices, including weapons.

The supply chain disruption of these two critical raw materials has already made the world economies scramble to amass as much of these minerals as possible before the restrictions kick in.

For a world frightened by China's rise and its dominance of many industries critical for global infrastructure and security, it has done little to build manufacturing capability and resilient supply chains.

The US government identified four fields in 2021: Semiconductor manufacturing and advanced packaging, large capacity batteries, critical minerals and materials, and pharmaceuticals and active pharmaceutical ingredients (APIs).

16. [China has had a spy base in Cuba for decades, former intelligence officer says](#) (Miami Herald, 05 JUL, NORA GÁMEZ TORRES)

China's espionage efforts in Cuba targeting the United States are not recent and date back at least three decades, a retired army counterintelligence agent has told the

Miami Herald.

It took U.S. intelligence agencies nine years to figure out who was behind the repair and enhancements spotted during the 1990s at a “signals intelligence facility” — a reference to the interception of electronic communications — in the town of Bejucal, a 45-minute drive from Havana.

17. [Chinese Responses to Wagner Mutiny Attempt](#) (U.S. Army Asian Studies Detachment, 05 JUL)

This article summarizes Chinese language media responses with the Wagner company’s attempted mutiny in Russia.