Cyber Center of Excellence

Unclassified Threat Read Book

16 - 30 JUN 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. Russian cyber expert arrested in Kazakhstan, triggering a showdown between US and Moscow - 28 JUN
2. Attackers Using Social Engineering to Capitalize on the ChatGPT Buzz - 28 JUN
3. Silobreaker unveils new geopolitical cyber threat intelligence capabilities - 26 JUN
4. Chinese Hackers Using Never-Before-Seen Tactics for Critical Infrastructure Attacks - 26 JUN
5. North Korean hackers prioritize cyber spying over digital attacks, analysis shows - 26 JUN
6. Randomly received a smartwatch? Don't turn it on, investigators warn. – 22 JUN
7. New US cyber unit to coordinate responses against nation states like North Kore - 22 JUN
8. iOS 16.5.1 fixes critical iMessage security flaw, you should update immediately! - 22 JUN
9. Supply Chain Hacks are Stealthy. Shore up Your Defenses - 21 JUN
10. A new cyberespionage campaign from China's APT15. - 21 JUN
11. This stealthy malware can steal your files without you knowing - 20 JUN
12. Six generative AI cyber security threats and how to mitigate them - 19 JUN
13. These are the most hacked passwords. Is yours on the list? - 19 JUN
14. Microsoft says early June disruptions to Outlook, cloud platform, were cyberattacks – 17 JUN
15. Russian cybercriminals attack US Government agencies - 16 JUN
16. Chinese spies breached hundreds of public, private networks, security firm says - 15 JUN

Electronic Warfare

1. Lockheed bests General Dynamics for Army long-range jammer contract – 27 JUN
2. Russian Su-34s Can "Disappear" From Enemy Radars As Moscow Arms It With New Anti-EW Suite – Media Claims - 23 JUN
3. Russian electronic warfare complicates Ukrainian attacks – 17 JUN

Information Advantage

1. Foreign Reflections on U.S. Exercises and Operations, 30 June 2023 – 30 JUN
2. BRI - Belt and Road Initiative - Highlights, 28 June 2023 - 29 JUN
3. First misinformation susceptibility test finds 'very online' Gen Z and millennials are most vulnerable to fake news - 28 JUN
4. Israel's Shin Bet spy service uses generative AI to thwart threats - 27 JUN
5. Ukraine war: Videos straight from the trenches to the phone - 21 JUN
6. Cooperation or competition? China's security industry sees the US, not AI, as the bigger threat - 21 JUN
7. AI: Chatbots replace journalists - 21 JUN
8. France targets Russian and Wagner disinformation in Africa - 21 JUN
9. Foreign Reflections on U.S. Exercises and Operations, 20 June 2023 - 20 JUN
10. Is misinformation the newest malware? - 20 JUN
11. How Ukraine uses artificial intelligence on the battlefield - 19 JUN
12. What is the EU doing to counter foreign disinformation? - 16 JUN
13. Social Engineering And The Disinformation Threat In Cybersecurity - 16 JUN
14. UN Report Highlights Dangers of Political Disinformation Caused by Rise of Artificial Intelligence - 15 JUN

Signal

1. China Threat Forces Japan To Test Starlink Satellite That Played A Critical Role To Keep Ukraine Connected - 27 JUN
2. US Global Positioning Systems Under Threat; The Emerging MagNav Could Take Over The GPS Soon - 25 JUN
3. Quantum computers to overtake regular computers 'within two years' after breakthrough - 22 JUN
4. Are federal agencies' post-quantum cryptography preparations on track? – 16 JUN
5. Photonic quantum computers can break encryption 700x faster – 16 JUN

Items of Interest

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. Deutsche Welle (DW) Ukraine updates
4. Did the Wagner Group have supporters within Russia's army? – 30 JUN
5. Will the Wagner mutiny help Ukraine's counteroffensive? – 29 JUN
6. How 'Vladimir Putin's chef' became a billionaire – 29 JUN
7. Russia Plotting To Assassinate Prigozhin, Ukraine's Spy Boss Tells Us – 29 JUN
8. Where are Russian generals Gerasimov and Surovikin after Wagner rebellion? - 29 JUN
9. Chinese Spy Balloon Was Chock Full Of Commercial US Tech, Investigation Finds: REPORT - 29 JUN
10. Wagner Group: What are private military companies? - 29 JUN
11. Purges Underway In Russian Security Apparatus After Prigozhin's Mutiny - 28 JUN
12. Wagner Group mutiny: The end for Russian defense minister? - 28 JUN
13. Belarus Wants Prigozhin's 'Wagnerites' To Train Its Army - 27 JUN
14. Russia's Putin under pressure after failed revolt - 27 JUN
15. Fact check: Do these videos show Wagner battles in Russia? - 27 JUN
16. Prigozhin Is Back On His Soapbox Two Days After Outright Mutiny - 26 JUN
17. How the Wagner Group mutiny became a Belarusian PR triumph - 26 JUN
18. Russia says it downed 3 drones outside Moscow, suspects it was attack by Ukraine – 22 JUN
19. Wagner Boss Declares War On Russian Defense Ministry (Updated) - 24 JUN
20. Russia's Wagner Group: Where is it active? - 25 JUN
21. Russia says it downed 3 drones outside Moscow, suspects it was attack by Ukraine - 22 JUN
22. Ukrainian T-72 Tank That Ran Over MRAP Seen In New Ground-Level Video – 21 JUN
23. China imposes limits on Russian banks – 21 JUN
24. North Korea Calls botched spy satellite launch 'most serious failure – 19 JUN

Cyber

1. **Russian cyber expert arrested in Kazakhstan, triggering a showdown between US and Moscow (The Record, 28 JUN, Daryna Antoniuk)**

   A notable Russian cybersecurity expert was detained in Kazakhstan last week at the request of the U.S., prompting authorities in Moscow on Wednesday to also seek his extradition.

   Although the details and reasoning for the arrest are unclear, Nikita Kislitsin was charged with selling usernames and passwords belonging to American customers of the social media company Formspring in 2012. Kislitsin worked as the head of network security at Group-IB, as well as its Russia-based spinoff company known as F.A.C.C.T. after Group-IB exited the country earlier this year.

2. **Attackers Using Social Engineering to Capitalize on the ChatGPT Buzz (Info Security, 28 JUN, Paolo Passeri)**

   According to the latest Netskope Cloud and Threat Report, during Q1 2023, social engineering continued to be a dominant malware infiltration technique, with attackers abusing search engines, email, collaboration apps and chat apps to trick their victims into downloading malware. These campaigns exploit popular topics in the zeitgeist or major events so that the attackers can better disguise malicious content as legitimate files or web pages so the victim would fail to recognize its nefarious intent.

   With all the buzz around ChatGPT, it was just a matter of time before threat actors started to capitalize on the hype around the artificial intelligence chatbot. For example, launching campaigns delivering malware in disguise of improbable ChatGPT clients or phishing pages promising rather improbable free access to the same service or other AI tools.

3. **Silobreaker unveils new geopolitical cyber threat intelligence capabilities (ARN, 26 JUN, Michael Hill)**

   Silobreaker integrates RANE geopolitical intelligence to warn security teams of world events that could heighten the risk of cyberattacks.

   Security and threat intelligence company Silobreaker has announced new geopolitical threat intelligence capabilities with RANE (Risk Assistance Network + Exchange).

   The tie-up will see Silobreaker integrate global risk intelligence company RANE's enterprise geopolitical intelligence into its own platform, providing cyber threat intelligence teams with real-time information about world events that could heighten the risk of cyberattacks.

4. **Chinese Hackers Using Never-Before-Seen Tactics for Critical Infrastructure Attacks (The Hacker News, 26 JUN, Ravie Lakshmanan)**

   The newly discovered Chinese nation-state actor known as Volt Typhoon has been observed to be active in the wild since at least mid-2020, with the hacking crew linked to never-before-seen tradecraft to retain remote access to targets of interest.

   The findings come from CrowdStrike, which is tracking the adversary under the name Vanguard Panda.

   "The adversary consistently employed ManageEngine Self-service Plus exploits to gain initial access, followed by custom web shells for persistent access, and living-off-the-land (LotL) techniques for lateral movement," the cybersecurity company said.

5. **North Korean hackers prioritize cyber spying over digital attacks, analysis shows (Washington Time, 26 JUN, Ryan Lovelace)**

North Korean hackers are overwhelmingly prioritizing cyber espionage over destructive digital attacks, according to a new analysis from cyber intelligence firm Recorded Future.

The firm found more than 70% of cyberattacks with a known purpose and attributed to North Korea since 2009 were likely conducted for information collection rather than to wipe out systems.

"North Korea's leadership appears to be much more interested in learning about what others think of them, gathering information that can help them develop nuclear and ballistic missile technology, and stealing money to fund their regime," Recorded Future said in a new report.

6. **Randomly received a smartwatch? Don't turn it on, investigators warn. (Defense News, 22 JUN, Colin Demarest)**

Smartwatches capable of automatically connecting to cellphones and Wi-Fi and gaining access to user data are being shipped to members of the U.S. military seemingly at random, raising cybersecurity concerns.

The Department of the Army Criminal Investigation Division, or CID, in an announcement last week warned the watches may contain malware, potentially granting whoever sent the peripherals "access to saved data to include banking information, contacts, and account information such as usernames and passwords."

7. **New US cyber unit to coordinate responses against nation states like North Kore (NK News, 22 JUN, Shreyas Reddy)**

Justice Department unit will break down 'wall' between criminal and national security investigations, expert says

The U.S. Justice Department has launched a new unit tasked with countering cyber threats, including from North Korean hackers, a move that one former U.S. intelligence official said was "a long time coming."

The new National Security Cyber Section under the National Security Division (NSD) is aimed at strengthening intragovernmental coordination against the growing dangers posed by adversaries' illicit cyber activities, the Justice Department stated in a press release on Tuesday.

8. **iOS 16.5.1 fixes critical iMessage security flaw, you should update immediately! (Android Authority, 22 JUN, Aamir Siddiqui)**

The flaw was exploited in iOS 15.7 and earlier, so Apple has also released iOS 15.7.7 with the same fixes.

Apple prides itself on the security and privacy provided by iPhones, and to a good extent, we do agree that it is better than Android. However, iPhones are relatively secure, and not absolutely secure. The proof for this assertion lies with the new iOS 16.5.1 update that is rolling out to iPhones, bringing an urgent fix for a critical iMessage security flaw. If you own an iPhone, we strongly recommend updating your phone right away.

9. **Supply Chain Hacks are Stealthy. Shore up Your Defenses (Dell Technologies Blog, 21 JUN, Tom Bentz)**

Support Zero Trust from manufacture to first boot with Secured Component Verification, now available on device and cloud.

As organizations harden their attack surfaces, it follows that cybercriminals move on to seek softer targets. However, there's one type of stealthy attack that doesn't get the attention it deserves: supply chain compromise. Why? Phishing and ransomware attacks are much more visible, occurring while devices are already in use. Anyone with an email account has experienced a phishing attempt. But the reality is that supply chain attacks happen, and the impact can be devastating.

Supply chain attacks were responsible for 62% of network breaches in 2021, and they will only increase in frequency and scope. The FBI has issued multiple alerts over the past few years on this topic. These malicious activities have been so concerning that it led to the February 2021 Executive Order on Supply Chain Security.

10. **A new cyberespionage campaign from China's APT15. (The Cyber Wire, 21 JUN, Jason Cole)**

The Threat Hunter Team at Symantec, part of Broadcom, released a new report detailing a recent campaign against various ministries of foreign affairs across the Americas by the China-backed advanced persistent threat (APT) group called the Flea (also known as APT15, Nickel, Nylon Typhoon, Backdoor Diplomacy, and Ke3chang).

11. **This stealthy malware can steal your files without you knowing (Tech Radar, 20 JUN, Lewis Maddison)**

Malware is getting more sophisticated, Bitdefender warns.

Bitdefender, one of the best antivirus software offerings around, has uncovered a worrying new malware that can extract sensitive information from an endpoint without the user ever finding out.

12. **Six generative AI cyber security threats and how to mitigate them (IT Pro, 19 JUN, Kate O'Flaherty)**

What are the risks posed by generative AI and how can businesses protect themselves?

ChatGPT and competitors such as the recently-launched Google Bard have shot generative artificial intelligence (AI) into the mainstream. Allowing users to create, combine and remix content, generative AI is hailed as a transformative technology for businesses.

13. **These are the most hacked passwords. Is yours on the list? (ZDNet, 19 JUN, Lance Whitney)**

Based on more than 6 million breached passwords, there are certain subjects and patterns you should avoid in your own passwords, says payment firm Dojo.

Cybercriminals use a variety of tactics to try to determine your passwords. And too many people make the effort easier by using weak and simple ones. A new study from Dojo on the most hacked passwords may be able to help you stay safer online by knowing which mistakes to avoid.

14. **Microsoft says early June disruptions to Outlook, cloud platform, were cyberattacks (AP News, 17 JUN, Frank Bajak)**

In early June, sporadic but serious service disruptions plagued Microsoft's flagship office suite — including the Outlook email and OneDrive file-sharing apps — and cloud computing platform. A shadowy hacktivist group claimed responsibility, saying it flooded the sites with junk traffic in distributed denial-of-service attacks.

Initially reticent to name the cause, Microsoft has now disclosed that DDoS attacks by the murky upstart were indeed to blame.

But the software giant has offered few details — and did not immediately comment on how many customers were affected and whether the impact was global. A spokeswoman confirmed that the group that calls itself Anonymous Sudan was behind the attacks. It claimed responsibility on its Telegram social media channel at the time. Some security researchers believe the group to be Russian.

15. **Russian cybercriminals attack US government agencies (Telecoms Tech News, 16 JUN, Ryan Daws)**

Several US federal government agencies have fallen victim to a global cyberattack by Russian cybercriminals.
The attack exploits a vulnerability in widely used software, leading to concerns about data breaches and potential disruptions. The US Cybersecurity and Infrastructure Security Agency (CISA) is working urgently to understand the impacts and facilitate timely remediation.

16. **Chinese spies breached hundreds of public, private networks, security firm says (Auburnpub, 15 JUN, Frank Bajak)**

Suspected state-backed Chinese hackers used a security hole in a popular email security appliance to break into the networks of hundreds of public and private sector organizations globally, nearly a third of them government agencies including foreign ministries, the cybersecurity firm Mandiant said Thursday.

“This is the broadest cyber espionage campaign known to be conducted by a China-nexus threat actor since the mass exploitation of Microsoft Exchange in early 2021,” Charles Carmakal, Mandiant's chief technical officer, said in a emailed statement. That hack compromised tens of thousands of computers globally.

Electronic Warfare

1. **Lockheed bests General Dynamics for Army long-range jammer contract (C4ISR Net, 27 JUN, Colin Demarest)**

   Lockheed Martin, the world's largest defense contractor by revenue, bested rival General Dynamics Mission Systems for a U.S. Army deal to develop a long-range electronic warfare, signals intelligence and cyber system the service sees as critical to its "deep sensing" playbook.

   Under the new arrangement, worth nearly $37 million over 21 months, Lockheed will build a prototype of the Terrestrial Layer System-Echelons Above Brigade, or TLS-EAB, at its facility in Syracuse, New York. Both Lockheed and General Dynamics Mission Systems were involved in preliminary designs and software demonstrations, according to contract announcements from August.

2. **Russian Su-34s Can "Disappear" From Enemy Radars As Moscow Arms It With New Anti-EW Suite – Media Claims (The EurAsian Times, 23 JUN, Ritu Sharma)**

   Fighting against technologically inferior adversaries, like Iraq and the Taliban, electronic warfare (EW) had become a forgotten discipline for the Western armed forces. However, the Ukraine War has bought EW back into the limelight.

   Russian news agency Ria Novosti recently claimed that the Russian twin-engine long-range strike aircraft Sukhoi Su-34, which goes with the nom de guerre 'Fullback' received new protection against enemy electronic warfare equipment, including protection against foreign-made electronic warfare systems, for use in the special military operation zone.

3. **Russian electronic warfare complicates Ukrainian attacks – ISW (Euromaidan, 17 JUN)**

   According to an Institute for the Study of War (ISW) daily update, Ukrainian forces' ongoing counteroffensive operations against Russia in Ukraine's western regions of Donetsk and Zaporizhzhia are encountering roadblocks due to Russia's sophisticated electronic warfare (EW) capabilities. These operations by Ukrainian forces are being viewed as the initial phase of an overall counteroffensive.

   On June 15, Ukrainian General Staff Spokesperson Oleksandr Shtupun confirmed successful Ukrainian offensive operations north and northwest of Bakhmut, with gains reported by Ukraine's Tavrisk Group of Forces Press Center in western Donetsk Oblast. Russian milbloggers, however, reported unsuccessful Ukrainian attacks in western Zaporizhzhia Oblast and attributed the resilience of Russian defenses to superior EW capabilities.

Information Advantage

1. **Foreign Reflections on U.S. Exercises and Operations, 30 June 2023 (U.S. Army Asian Studies Detachment, 30 JUN)**

   This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 24 to 29 June 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, the Philippines, Singapore, South Korea, Taiwan, and Vietnam.

2. **BRI - Belt and Road Initiative - Highlights, 28 June 2023 (U.S. Army Asian Studies Detachment, 29 JUN)**

   The Belt and Road Initiative (BRI) is an expansive economic and infrastructure program initiated by the People's Republic of China aimed at increasing its influence throughout the world. Targeted primarily at poorer nations, or nations the PRC has a strategic interest in, it aims to increase the infrastructure usable by the PRC as well as making those nations economically dependent upon the PRC.

   The following is a compilation of reports covering projects the PRC will initiate or have already started, as well as covering the evaluation or criticism of BRI in local countries and diplomatic efforts by China to promote BRI.

3. **First misinformation susceptibility test finds 'very online' Gen Z and millennials are most vulnerable to fake news (Phys.org, 28 JUN, Univeresity of Cambridge)**

   University of Cambridge psychologists have developed the first validated "misinformation susceptibility test": a quick two-minute quiz that gives a solid indication of how vulnerable a person is to being duped by the kind of fabricated news that floods online spaces.

   The test, proven to work through a series of experiments involving more than 8,000 participants taking place over two years, has been deployed by polling organization YouGov to determine how susceptible Americans are to fake headlines.

4. **Israel's Shin Bet spy service uses generative AI to thwart threats (Reuters, 27 JUN, Dab Williams)**

   Israel's Shin Bet security service has incorporated artificial intelligence into its tradecraft and used the technology to foil substantial threats, its director said on Tuesday, highlighting generative AI's potential for law-enforcement.

   Among measures taken by the Shin Bet - the Israeli counterpart of the U.S. Federal Bureau of Investigations or Britain's MI5 - has been the creation of its own generative AI platform, akin to ChatGPT or Bard, director Ronen Bar said.

5. **Ukraine war: Videos straight from the trenches to the phone (DW, 21 JUN, Frank Hofmann)**

   War reporting in the digital age: The flood of video footage from frontline trenches in Ukraine makes covering the war for journalists even more complex.

   Videos straight from the trenches: the killing shot, the fighting filmed with a helmet camera. Another shot, another dead person — and the viewers get those videos almost

instantly.

Unlike in any war before, the fighting in Ukraine can be seen on Twitter and other platforms, far away from where the fighting takes place.

Russia's war against Ukraine is so far "without a doubt the most extensively visually documented conflict in the history of images and war," said US photojournalist Ron Haviv on the podium at this year's Deutsche Welle Global Media Forum. The question many in the audience might ask themselves is what role journalism plays in this.

6. Cooperation or competition? China's security industry sees the US, not AI, as the bigger threat (AP News, 21 JUN, Dake Kang)

After years of breakneck growth, China's security and surveillance industry is now focused on shoring up its vulnerabilities to the United States and other outside actors, worried about risks posed by hackers, advances in artificial intelligence and pressure from rival governments.

The renewed emphasis on self-reliance, combating fraud and hardening systems against hacking was on display at the recent Security China exhibition in Beijing, illustrating just how difficult it will be to get Beijing and Washington to cooperate even as researchers warn that humankind faces common risks from AI. The show took place just days after China's ruling Communist Party warned officials of the risks posed by artificial intelligence.

Looming over the four-day meet: China's biggest geopolitical rival, the United States. American-developed AI chatbot ChatGPT was a frequent topic of conversation, as were U.S. efforts to choke off China's access to cutting-edge technology.

7. AI: Chatbots replace journalists (DW, 21 JUN, Peter Hille)

German tabloid Bild, Europe's top-selling newspaper, has told hundreds of editors they will be replaced by AI. Will chatbots sound the death knell for human-made media content?

Axel Springer SE, Europe's largest publishing house, has announced that it will replace a range of editorial jobs with artificial intelligence (AI). In an email sent to staff on Monday (June 19), Springer said that it would "unfortunately part with colleagues who have tasks that will be replaced by AI and/or processes in the digital world. The functions of editorial directors, page editors, proofreaders, secretaries, and photo editors will no longer exist as they do today."

The job cuts at Springer, home of news brands such as Bild and Die Welt, stoke fears that AI will throw the whole world's media industry in disarray. Chatbots such as ChatGPT could be used to write news stories, making human journalists obsolete.

8. France targets Russian and Wagner disinformation in Africa (Reuters, 21 JUN, John Irish, Elizabeth Pineau & Bate Felix)

After armed men killed nine Chinese nationals at a gold mine in Central African Republic in March, a video circulated on the internet saying France had secretly ordered the attack and planned to discredit Russian mercenary group Wagner in the country.

9. Foreign Reflections on U.S. Exercises and Operations, 20 June 2023 (U.S. Army Asian Studies Detachment, 20 JUN)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 9 to 16 June 2023. Each section also contains the respective ASD

report number for the original report (if available) and covers reporting from the PRC, Indonesia, Japan, the Philippines, and Taiwan.

10. Is misinformation the newest malware? (ARN Net, 20 JUN, Cynthia Brumfields)

Experts say that cybersecurity skills and a whole-of-organisation approach can go a long way to tackling misinformation threats.

Misinformation and cybersecurity incidents have become the top scourges of the modern digital era. Rarely does a day go by without significant news of a damaging misinformation threat, a ransomware attack, or another malicious cyber incident.

As both types of threats escalate and frequently appear simultaneously in threat actors' campaigns, the lines between the two are getting fuzzy. At this year's RSA Conference, information security experts appeared on a panel entitled "Misinformation Is the New Malware" to hammer out the distinctions.

11. How Ukraine uses artificial intelligence on the battlefield (DW, 19 JUN)

The war in Ukraine has seen brutal attritional fighting and trench warfare, but also the novel use of drones and robots. Is artificial intelligence revolutionizing modern warfare or just complementing old technology?

12. What is the EU doing to counter foreign disinformation? (DW, 16 JUN, Rosie Birchard)

Lutz Güllner, who's at the forefront the European Union's fight against foreign disinformation campaigns, describes foreign actors' efforts to undermine the bloc and outlines what can be done to counter their "corrosive effect."

13. Social Engineering And The Disinformation Threat In Cybersecurity (Forbes, 16 JUN, David Balaban)

Disinformation is one of the world's most debated topics. From Vote Leave's now infamous Brexit bus; to Donald Trump's hysterical "fake news" allegations; to Vladimir Putin's warmongering rhetoric, disinformation – whether real or imagined – is an inescapable reality of the modern world.

But disinformation campaigns aren't restricted to the political sphere – according to research from Weber Shandwick, 87% of executives say the spread of disinformation is one of the most significant reputational risks to businesses today.

14. UN Report Highlights Dangers of Political Disinformation Caused by Rise of Artificial Intelligence (Be In Crypto, 15 JUN, David Thomas & Geraint Price)

A UN Information Integrity report into AI highlights the potential for industry executives to collude with politicians to spread disinformation shortly after Sam Altman lobbied Congress.

The agency highlighted how governments could collude with companies to spread disinformation aligned with a political or financial agenda.

Signal

1. **[China Threat Forces Japan To Test Starlink Satellite That Played A Critical Role To Keep Ukraine Connected] (The EurAsian Times, 27 JUN, Sakshi Tiwari)**

   The Japanese Self-Defense Forces (SDF), which has embarked on a massive military modernization, is currently testing Elon Musk's Starlink satellite network, one year after Ukraine began using it amidst an unprecedented Russian invasion.

   The news was first published by the Japanese newspaper The Yomiuri Shimbun, which also stated that the deployment of the SpaceX Starlink technology would add a constellation of satellites in low Earth orbit, in addition to the communication satellites in geostationary orbit that are already available to the Japanese Ministry of Defense.

   Sources accessed by the publication reportedly revealed that the SDF has been conducting trials of SpaceX's Starlink satellite constellations since March this year.

2. **[US Global Positioning Systems Under Threat; The Emerging MagNav Could Take Over The GPS Soon] (The EurAsian Times, 25 JUN, GP CPT TP Srivastava (Retd))**

   One of the biggest challenges the aviators faced was navigating accurately to reach the target; the equipment available to assist pilots in navigation in the past was a magnetic compass. With time, gyro-magnetic compasses appeared in cockpits.

   The advent of the Global Positioning System (GPS) made navigating much simpler. All existing systems are satellite-based and are in use not only by pilots in the air but also by drivers on the ground.

3. **[Quantum computers to overtake regular computers 'within two years' after breakthrough] (Independent, 22 JUN, Anthony Cuthbertson)**

   The Microsoft's 'quantum supercomputer' aims to compress centuries of scientific discoveries into just a few years.

   Microsoft has announced plans to build a quantum supercomputer after researchers said the next-generation machines will be able to outperform standard computers within the next two years.

   Quantum computers have the potential to be orders of magnitude more powerful than today's leading supercomputers, but have so far failed to compete when it comes to practical tasks.

4. **[Are federal agencies' post-quantum cryptography preparations on track?] (FEDScoop, 16 JUN, Rebecca Heilweil)**

   Federal agencies are supposed to be preparing for quantum hacking. Their progress is unclear.

   Today, the government uses standard cryptographic algorithms to protect its data. But amid the rise of quantum computers, these algorithms may not offer the security they once did.

   Put simply, quantum computers — with the ability to factor extremely large prime numbers — could one day break into these algorithms, helping adversaries access all

sorts of critical information, including personal data about U.S. citizens and critical scientific and military secrets.

5. Photonic quantum computers can break encryption 700x faster (EE News, 16 JUN, Nick Flaherty)

PsiQuantum has shown its photonic fault tolerant quantum computer architecture can break Elliptic Curve Cryptography (ECC) 700 times faster than other quantum machines.

A paper describes a more efficient method to break ECC which is widely used for secure communications. This approach uses techniques especially applicable to photonic architectures and reduces the number of gate operations required to break an ECC key by up to 80% as well as a 700x reduction in computation time relative to the state-of-the-art quantum algorithms.

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, 30 June 2023
Russia-Ukraine Situation Report, 29 June 2023
Russia-Ukraine Situation Report, 28 June 2023
Russia-Ukraine Situation Report, 27 June 2023
Russia-Ukraine Situation Report, 26 June 2023
Russia-Ukraine Situation Report, 23 June 2023
Russia-Ukraine Situation Report, 22 June 2023
Russia-Ukraine Situation Report, 21 June 2023
Russia-Ukraine Situation Report, 20 June 2023
Russia-Ukraine Situation Report, 19 June 2023
Russia-Ukraine Situation Report, 16 June 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Ukraine Situation Report: Counteroffensive Criticism "Pisses Me Off" Says Top General – 30 JUN

Ukraine Situation Report: U.S. Warming To Sending ATACMS – 29 JUN

Ukraine Situation Report: Naval Strike Missiles May Be Headed To Ukraine – 28 JUN

Ukraine Situation Report: U.S. Replenishes Kyiv's Bradley Fighting Vehicle Force – 27 JUN

Ukraine Situation Report: Breakthrough Across The Dnipro At Antonvosky Bridge - 26 JUN

Ukraine Situation Report: Counteroffensive Slowed By 77,000 Square Miles Of Mines – 21 JUN

Ukraine Situation Report: Kyiv Tries To Lower Expectations For Its Counteroffensive – 20 JUN

Ukraine Situation Report: Russia Making Push In East – 19 JUN

Ukraine Situation Report: Waning Flood Waters Could Provide Opportunity For Kyiv's Forces – 17 JUN

Ukraine Situation Report: Putin Says Tactical Nukes Now In Belarus – 16 JUN

3. Deutsche Welle (DW) Ukraine updates

Ukraine: Deadly Russian missile strike hits Kramatorsk - 29 JUN

Ukraine updates: Kramatorsk attack death toll rises – 28 JUN

Ukraine updates: Zelenskyy says gains made in all sectors – 27 JUN
Ukraine updates: Kyiv claims Russia hiding dam breach dead – 23 JUN
Ukraine updates: Ukraine 'damages' key Crimea bridge – 22 JUN
Ukraine updates: EU takes aim at Russian sanction dodging – 21 JUN
Ukraine updates: Kyiv 'destroying the enemy,' Zelenskyy says – 21 JUN
Ukraine updates: No lost ground in counterattack, Kyiv says – 20 JUN
Ukraine updates: Russia blocking Kherson flood aid, UN says – 19 JUN

4. **Did the Wagner Group have supporters within Russia's army? (DW, 30 JUN, Mikhail Bushuev)**

   President Vladmir Putin has said Russian security forces were united in their response to the uprising by the Wagner Group. How was it, then, that fighters came within striking distance of Moscow?

5. **Will the Wagner mutiny help Ukraine's counteroffensive? (DW, 29 JUN, Frank Hofmann)**

   For the time being, Wagner Group mercenaries have stopped fighting alongside Russian forces. Will this help Ukraine's efforts on the battlefield?

6. **How 'Vladimir Putin's chef' became a billionaire (DW, 29 JUN, Kristina Becker)**

   Yevgeny Prigozhin, head of the paramilitary Wagner Group, has probably posed the biggest-ever challenge to Vladimir Putin's rule up until now. Who is he and how did he become so rich?

7. **Russia Plotting To Assassinate Prigozhin, Ukraine's Spy Boss Tells Us (The War Zone, 29 JUN, Howard Altman)**

   In a wide-ranging interview, Budanov says Wagner is no longer a threat in Ukraine and what would've happened if Prigozhin went all the way.

   Early this morning, just days after Wagner Private Military Company (PMC) leader launched, then aborted a mutiny against Moscow, The War Zone caught up with the head of the Ukrainian Defense Intelligence Directorate (GUR) for his assessment of the situation and more.

8. **Where are Russian generals Gerasimov and Surovikin after Wagner rebellion? (Reuters, 29 JUN, Andrew Osborn)**

   Russia's most senior generals have dropped out of public view after a failed mercenary mutiny aimed at toppling the top military brass, amid a drive by President Vladimir Putin to reassert his authority.

   Unconfirmed reports say that at least one person has been detained and is being questioned.

   Armed forces chief of staff General Valery Gerasimov has not appeared in public or on state TV since the aborted mutiny on Saturday when mercenary leader Yevgeny Prigozhin demanded Gerasimov be handed over. Nor has he been mentioned in a defence ministry press release since June 9.

9. **Chinese Spy Balloon Was Chock Full Of Commercial US Tech, Investigation Finds: REPORT (Daily Caller, 29 JUN, Micaela Burrow)**

Early findings in the analysis of debris from the Chinese spy balloon that floated over the U.S. earlier in January show that designers used a wide array of commercially available U.S.-made equipment that directly aided its surveillance capabilities, The Wall Street Journal reported, citing U.S. officials with knowledge of the investigation.

Several members of the intelligence community, including the FBI and the Department of Defense (DOD), have picked apart remains of the downed balloon from debris retrieved from the Atlantic, finding U.S.-made equipment for collecting photos, videos and other forms of information, according to the WSJ, citing the U.S. officials. It also contained specialized Chinese-made collection equipment, supporting the Biden administration's ultimate conclusion that China deployed the balloon to spy on Americans.

10. Wagner Group: What are private military companies? (DW, 29 JUN, Oliver Pieper)

So-called private military companies (PMCs) play an ever-greater role in military conflicts. But what are they? Here the most important questions and answers.

11. Purges Underway In Russian Security Apparatus After Prigozhin's Mutiny (The Drive, 28 JUN, Howard Altman)

Reports say Gen. Sergei Surovikin, head of the Russian Air Force and erstwhile Prigozhin ally, was arrested for his part in the mutiny.

Wagner mercenary group leader Yevgeny Prigozhin's abruptly halted mutiny attempt continues to roil Moscow and shake President Vladimir Putin's decades-long hold on power. Meanwhile, as a result of his putative exile to Belarus, its neighbor Poland is increasing its troop presence and beefing up fortifications out of concern for any trouble Prigozhin might cause. You can read more about what set this all off in our coverage here.

Both The Wall Street Journal and New York Times on Wednesday came out with stories raising issues about who knew what about Prigozhin's plans before they were launched. In reaction to the failed putsch, purges are taking place in Russia's military while claims have arisen about the arrest of top Russian general Sergei Surovikin for his role in the mutiny, Russian media and Russia's military-connected Telegram channels claim.

12. Wagner Group mutiny: The end for Russian defense minister? (DW, 28 JUN, Roman Goncharenko)

One of the Wagner Group boss' biggest complaints was about how Russian defense minister Sergei Shoigu was running the Ukraine war. But little has been said about Shoigu's future — as yet.

Sergei Shoigu is back — at least on Russian TV. The Russian defense minister was not seen in public during the Wagner Group's day-long mutiny, during which the paramilitary's leader railed against Shoigu's leadership in the Ukraine war. Even after the mutiny ended, Shoigu did not appear on television.

It was not until Monday that Russian media showed pictures of him — supposedly in the war zone in Ukraine in the morning and then at a meeting of the security services in the evening, together with Russian President Vladimir Putin. There has been no statement from Shoigu about the short-lived rebellion.

13. Belarus Wants Prigozhin's 'Wagnerites' To Train Its Army (The Drive, 27 JUN, Howard Altman)

Lukashenko said battle hardened Wagner troops can train his forces but won't have any role with Russian-provided nuclear weapons.

Three days after ending his attempted mutiny against Moscow, Yevgeny Prigozhin, the head of the Wagner Private Military Corporation, landed in his new home of Belarus, according to the leader of that nation. Though free from charges connected with the weekend's aborted 'march on Moscow,' he is facing an uncertain future. The troops and equipment he amassed are being prepared for turnover to the Russian Defense Ministry and his role remains murky.

"Yes, indeed, he is in Belarus today," Belarusian dictator Alexander Lukashenko said Tuesday during a speech after a military promotion ceremony, according to the official Belarusian BelTa news service. However, no images have yet emerged of him there. Allowing Prigozhin in Belarus raises questions about how he can be contained. What happens next with Wagner, meanwhile, particularly in Africa, is something the Pentagon said it is keeping an eye on.

14. Russia's Putin under pressure after failed revolt (DW, 27 JUN, Matthew Mannion)

The Wagner group's short-lived revolt has left Moscow seeking to restore calm and reassert President Putin's authority. Many questions remain about how the dramatic events will inform his next steps, and what they could mean for the war in Ukraine.

15. Fact check: Do these videos show Wagner battles in Russia? (DW, 27 JUN, Joscha Weber)

The world held its breath as Wagner forces advanced on Moscow and their leader, Yevgeny Prigozhin, seemed to challenge President Vladimir Putin. Many videos claim to show clashes between both sides, but not all are real.

16. Prigozhin Is Back On His Soapbox Two Days After Outright Mutiny (The Drive, 26 JUN, Howard Altman)

After more than a day of uncharacteristic silence, the head of the Wagner mercenary group opened up about his mutinous march on Moscow.

In a new audio message posted on his Telegram channel Monday, Wagner Private Military Corporation leader Yevgeny Prigozhin took yet another swipe at Russian military leadership, saying his mutinous march toward Moscow was a lesson in how to conduct maneuver warfare aimed at preserving his organization. He also expressed regret at "being forced" to shoot down nearly a dozen Russian aircraft in the process.

"The march showed many things demonstrated before," Prigozhin said, according to a translation by the Wartranslated Twitter handle. "Serious security concerns around the country. All military bases and airfields were blocked. If actions on 24 Feb 2022 were done by forces as trained as Wagner, the special operation could have ended in one day. This shows the level of organization that the Russian Army should be following."

17. How the Wagner Group mutiny became a Belarusian PR triumph (DW, 26 JUN, Grzegorz Szymanowski)

Belarusian President Alexander Lukashenko helped Russia end the weekend's revolution led by Wagner Group leader Yevgeny Prigozhin. He's gone from being seen as Moscow's vassal to a regional statesman. Can it last?

He wanted to go all the way to Moscow but has likely ended up in Minsk instead.

Fighters from the infamous Russian private military company the Wagner Group were already on their way to the capital when news came from the government in Belarus.

"[Wagner Group boss] Yevgeny Prigozhin accepted the proposal of the president of Belarus, Alexander Lukashenko, to stop the movement of armed personnel of the Wagner company inside Russia, and take additional steps to de-escalate tensions," the official statement said.

Prigozhin's whereabouts are currently unknown but he reportedly left Russia for Belarus, with his departure marking the end of his rebellion.

18. Prigozhin Calls Off Coup (Updated) (The Drive, 24 JUN, Howard Altman, Thomas Newdick & Tyler Rogoway)

Yevgeny Prigozhin has told his forces to stand down after a deal was brokered by Belarus to end the Wagner insurrection.

On the second day of an attempted coup that has the world watching warily, Wagner boss and now enemy of the Russian state Yevgeny Prigozhin and the core of his forces remain entrenched in Rostov, while other elements are now holding Voronezh, which sits between Rostov and Moscow along the M4 highway. Additional Wagner forces are said to have splintered off and continued on a push to the Russian capital. Now, it appears that some of those elements have come under fire.

19. Wagner Boss Declares War On Russian Defense Ministry (Updated) (The Drive, 24 JUN, Howard Altman & Tyler Rogoway)

After claiming his forces were attacked by Russia, Wagner leader Yevgeny Prigozhin said he would march on Moscow.

The long-standing verbal war between Wagner mercenary group kingpin Yevgeny Prigozhin and Russian military and political leadership took a kinetic turn Friday that could lead to a potential coup attempt.

Prigozhin, in audio recordings posted on his Telegram channel is threatening a march on Moscow after claiming his troops were attacked by Russian forces.

20. Russia's Wagner Group: Where is it active? (DW, 25 JUN, Silja Thoms)

Russia's notorious private military company, the Wagner Group, has been training soldiers, escorting politicians and allegedly committing human rights violations all over the globe for years.

The Wagner Group isn't just active in Ukraine. It also has a presence in many other countries, including Syria or Mali. And it's not the only Russian private military company either. Over the past few years, there has been an increase in these kinds of groups, also known as PMCs, in Russia, a report from the US-based think tank, the Center for Strategic and International Studies, says.

It is not always possible to accurately track the exact activities of the Wagner Group, headed by Yevgeny Prigozhin, and other PMCs because they allegedly act independently of the Russian government and conventional military forces. However analysts believe that the group is likely active in more than 30 countries around the world.

21. Russia says it downed 3 drones outside Moscow, suspects it was attack by Ukraine (AP News, 22 JUN)

Two drones were brought down outside Moscow as they approached the warehouses of a local military unit, Russian authorities said Wednesday, in what could be the latest attempt by Ukraine to strike targets inside Russia during the early stages of Kyiv's most recent counteroffensive.

At the same time, Russian President Vladimir Putin claimed that the Ukrainian forces were regrouping after what he described as a failed counteroffensive and could be readying new attempts to attack Russian positions.

22. Ukrainian T-72 Tank That Ran Over MRAP Seen In New Ground-Level Video (The Drive, 21 JUN Oliver Parken)

Exactly why the T-72 ended up on top of the MaxxPro MRAP remains a bit of a mystery.

Video has emerged showing a ground-level perspective of a Ukrainian T-72 tank that rolled over and crushed a Ukrainian Mine Resistant Ambush Protected (MRAP) armored vehicle. Earlier footage of that incident, filmed from above via a Russian drone, began circulating online last week. You can read The War Zone's previous article on that incident here.

23. China imposes limits on Russian banks (DW, 21 JUN, Jo Harper)

China clearly doesn't want to be drawn any deeper than it has to into the diplomatic and rhetorical war over Ukraine, which may partly explain its move to aid the US and EU in tightening the sanctions on Russia.

24. North Korea calls botched spy satellite launch 'most serious' failure (C4ISR Net, 19 JUN, Hyung-Jin Kim & Kim Tong-Hyung)

Top North Korean officials vowed to push for a second attempt to launch a spy satellite as they called their country's first, and failed, launch last month "the most serious" shortcoming this year and harshly criticized those responsible, state media reported Monday.

In late May, a North Korean rocket carrying a military reconnaissance satellite crashed soon after liftoff, posing a setback to leader Kim Jong Un's push to acquire a space-based surveillance system to better monitor the United States and South Korea.