U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

01-15 September 2023

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

Table of Contents

Spaceport – 14 SEP

3. Kim Jong Un vows full support for Russia as Putin pledges space tech for North Korea – 13 SEP
4. N. Korea Fires Ballistic Missile Toward East Sea: S. Korean Military – 13 SEP
5. Sweden's Saab snags Silicon Valley-based CrowdAI – 07 SEP

Russia-Ukraine Situation

1. Russia-Ukraine Situation Report
2. The DRIVE/Warzone Ukraine Situation Report
3. Ukraine just carried out the same kind of strike on Russia's navy that Elon Musk blocked, believing it could start a nuclear war – 13 SEP
4. Starlink vital despite not working for 'some time,' says Ukrainian official – 11 SEP
5. Cuba arrests 17 for allegedly helping recruit some of its citizens to fight for Russia in Ukraine – 08 SEP
6. Elon Musk denies sabotaging Starlink in Ukraine-Russia conflict – 08 SEP
7. First Ukrainian M1 Abrams Tank Crews Complete Training – 01 SEP

Cyber

1. **Microsoft: Iranian espionage campaign targeted satellite and defense sectors (CyberScoop, 14 SEP, A.J. Vicens)**

   An Iranian cyber espionage group successfully compromised dozens of entities and exfiltrated data from a subset of them as part of a campaign targeting organizations in the satellite, defense and pharmaceutical sectors, Microsoft said in a report published Thursday.

   The group in question — which Microsoft tracks as Peach Sandstorm but known otherwise as Holmium, APT33 or Elfin — compromised the accounts as part of a high volume of password spray attacks, where attackers try one known password against a list of usernames. The campaign began in February 2023 and targeted thousands of organizations, according to Microsoft.

   Microsoft did not say where the targeted organizations are based but noted that previous Peach Sandstorm activity occurred during a "rise in tensions between the United States and the Islamic Republic of Iran." Researchers have linked some of the group's previous operations to the devastating destructive Shamoon malware attacks that targeted Saudi Aramco, the oil company, in 2012 and other targets in subsequent years.

   The news comes on the heels of an incipient deal between the U.S. and Iranian governments that would allow banks to transfer $6 billion in frozen Iranian oil funds and see U.S. authorities release of five Iranian citizens held in the United States in exchange for the release of five American citizens detained in Iran, the Washington Post reported 11SEP23.

Back to Table of Contents

2. **Groups linked to Las Vegas cyber attacks are prolific criminal hacking gangs (CyberScoop, 14 SEP, A.J. Vicens)**

   A pair of criminal hacking groups have been linked with attacks in recent weeks on two prominent Las Vegas hotel and casino operators that has left one struggling to resume operations and prompted another to reportedly pay a multimillion-dollar ransom payment.

   The attacks on MGM Resorts and Caesars Entertainment have resulted in widespread outages at MGM properties, and according to a Wall Street Journal report, forced Caesars to pay roughly half of a $30 million ransom demand.

   Exactly who is behind the attacks remains unclear, but two hacking groups have been linked with the breaches: ALPHV and Scattered Spider. A person claiming to be a member of the latter told CyberScoop that their group was responsible for the attack on MGM but denied responsibility for the breach of Caesars. Earlier this week VX-Underground, a well-known online malware research repository, wrote on the social media platform X that an ALPHV representative said they were behind the MGM hack.

   Late Thursday, 14SEP23, ALPHV claimed responsibility for the attack on MGM in a statement on its website. It is unclear whether Scattered Spider's claim of responsibility for the breach of MGM is false or whether overlaps between the two groups mean that members of both hacking collectives were involved in the breach of MGM. The Scattered Spider member who spoke with CyberScoop described their group as a well-known affiliate of ALPHV.

3. **Estonian firm develops virtual 'shooting range' to test cyber defenses (C4ISR, 14 SEP, Jaroslaw Adamowski)**

   Estonia's CybExer Technologies has developed what it describes as virtual shooting ranges for testing cyber defense capacities in Ukraine and other countries.

"Together with our customers, we design different attacks on their cyber infrastructure," Mihkel Mooste, who is responsible for the firm's business development activities, told Defense News at this year's DSEI show in London. "This allows us to help them prepare for any real attacks that could penetrate their cyber defenses."

The company was established by co-founders of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, the Estonian capital. CybExer Technologies' representatives say the firm's collaboration with the Ukrainian military, which is continuously targeted by Russian hacking attacks, is one of the main factors driving its international expansion.

In addition to Ukraine's military, CybExer Technologies has a longstanding cooperation with the Estonian Defence Forces, as well as armed forces in South and East Asia, according to Mooste.

4. US Agencies Publish Cybersecurity Report on Deepfake Threats (Security Week, 13 SEP, Eduard Kovacs)

On 12SEP23, Several US government agencies published a cybersecurity information sheet focusing on the threat posed by deepfakes and how organizations can identify and respond to deepfakes.

In their new report, Contextualizing Deepfake Threats to Organizations, the FBI, NSA and CISA warn that deepfakes can also pose a significant threat to organizations, including government, national security, defense, and critical infrastructure organizations.

The agencies have made a series of recommendations for implementing technology to detect deepfakes and demonstrate media provenance. In addition, they urge organizations to protect the data of important individuals that may be targeted — deepfakes are more realistic if the attacker possesses the target's personal information and has significant amounts of unwatermarked media content that they can feed to their deepfake creation software.

Back to Table of Contents

5. China, Russia will use cyber to sow chaos if war starts, Pentagon says (C4ISR, 12 SEP, Colin Demarest)

China and Russia are prepared to unleash a flurry of cyberattacks on U.S. critical infrastructure and defense networks should war break out, according to a Pentagon strategy unveiled this week.

Such tactics, meant to sow chaos, divert precious resources and paralyze military mobilization, were observed in Eastern Europe during Russia's invasion of neighboring Ukraine, a conflict that colors the Pentagon's new 2023 Cyber Strategy. An unclassified summary of the document was made public Sept. 12.

Defense officials have long considered China and Russia national security hazards. While China poses the most-serious and long-term threat, they say, Russia presents more-immediate concerns. Both countries wield serious cyber arsenals. An International Institute for Strategic Studies report in 2021 placed China and Russia in tier two of its cyber powerhouse rankings. The U.S. sat in first.

The strategy, which supersedes a 2018 version, describes China as a "broad and pervasive" cyber espionage threat, one capable of absconding with defense trade secrets and monitoring U.S. citizens. It further labels Russia an online manipulator and harasser of critical infrastructure such as pipelines, hospitals, and transportation.

6. DOD Releases 2023 Cyber Strategy Summary (DOD, 12 SEP)

On 12SEP23, the Department of Defense (DOD) released an unclassified summary of

its classified 2023 Cyber Strategy.

The 2023 DOD Cyber Strategy, which DOD transmitted to Congress in May, is the baseline document for how the Department is operationalizing the priorities of the 2022 National Security Strategy, 2022 National Defense Strategy, and the 2023 National Cybersecurity Strategy. It builds upon the 2018 DOD Cyber Strategy and will set a new strategic direction for the Department.

7. China-Linked 'Redfly' Group Targeted Power Grid (Security Week, 12 SEP, Ionut Arghire)

Symantec has identified a new advanced persistent threat (APT) actor that appears to be focusing exclusively on targeting critical national infrastructure organizations.

Dubbed Redfly, the threat actor has been observed using the ShadowPad remote access trojan (RAT), a successor of Korplug/PlugX, to maintain presence on a compromised national power grid in Asia for as long as six months.

Discovered earlier this year, the attack is the latest in a series of intrusions targeting critical national infrastructure entities, employing tools and infrastructure that overlap with previous activity attributed to Chinese state-sponsored group APT41 (also tracked as Winnti, Wicked Panda, Blackfly, and Grayfly).

In addition to ShadowPad, Redfly was seen deploying PackerLoader, a tool for loading and executing shellcode, and a keylogger, which was dropped under various names on different machines.

Redfly, Symantec says, does not appear to be engaging in disruptive activities, but the cybersecurity company does not eliminate this possibility entirely.

Back to Table of Contents

8. After Microsoft and X, Hackers Launch DDoS Attack on Telegram (Security Week, 11 SEP, Ionut Arghire)

The hacker group Anonymous Sudan has launched a distributed denial-of-service (DDoS) attack against Telegram in retaliation to the messaging platform's decision to suspend their primary account, threat intelligence firm SOCRadar reports.

Claiming to be a hacktivist group motivated by political and religious causes, Anonymous Sudan has orchestrated DDoS attacks against organizations in Australia, Denmark, France, Germany, India, Israel, Sweden, and the UK.

Anonymous Sudan came to fame in June, after launching a series of disruptive DDoS attacks targeting Microsoft 365, impacting Outlook, Microsoft Teams, OneDrive for Business, and SharePoint Online. Microsoft's Azure cloud computing platform was also affected.

According to previous reports from SOCRadar and Truesec, the Anonymous Sudan group currently engaging in DDoS and defacement attacks might not operate out of Sudan and might, in fact, have ties to the Russian hacking group KillNet.

9. Powerful Ethnic Militia in Myanmar Repatriates 1,200 Chinese Suspected of Involvement in Cybercrime (Security Week, 10 SEP, Associated Press)

One of Myanmar's biggest and most powerful ethnic minority militias has arrested and repatriated more than 1,200 Chinese nationals allegedly involved in criminal online scam operations, an official of the group said on 09SEP23.

Cybercrime scams have become a major issue in Asia, as many of the workers employed to carry out the online scams are themselves victims of criminal gangs, who lure them

with fake job offers and then force them to work in conditions of virtual slavery.

Shwe Kokko, a small town in northern part of Kayin state's Myawaddy township, is notorious for casino complexes that allegedly host major organized crime operations, including online scamming, gambling and human trafficking. The complexes were developed by Chinese investors in cooperation with the local Border Guard Forces, which are militias affiliated with Myanmar's army.

10. **New Phishing Campaign Launched via Google Looker Studio (Security Week, 08 SEP, Ionut Arghire)**

Cybersecurity firm Check Point is warning of a new type of phishing attacks that abuse Google Looker Studio to bypass protections.

Google Looker Studio is a legitimate online tool for creating customizable reports, including charts and graphs, that can be easily shared with others.

As part of the observed attacks, threat actors are using Google Looker Studio to create fake crypto pages that are then delivered to the intended victims in emails sent from the legitimate tool itself.

Check Point's analysis shows that the attack manages to pass email authentication checks that prevent spoofing because the sender's IP address is listed as authorized for a google.com subdomain.

11. **US Aeronautical Organization Hacked via Zoho, Fortinet Vulnerabilities (Security Week, 08 SEP, Ionut Arghire)**

Back to Table of Contents

Advanced persistent threat (APT) actors have exploited known vulnerabilities in Zoho ManageEngine and Fortinet VPN products to hack an organization in the aeronautical sector, according to a joint report from the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Cyber Command's Cyber National Mission Force (CNMF).

The critical-severity issue was patched in November 2022, but the first signs of exploitation were observed in January 2023, shortly before a proof-of-concept (PoC) exploit targeting the flaw was published. At the time, security firms identified thousands of exposed ManagedEngine instances.

After investigating between February and April 2023, CISA, FBI, and CNMF discovered that multiple APTs exploited the two flaws starting in January this year, to establish persistence on an aeronautical organization's network.

The investigation revealed that the threat actors used multiple readily available tools during their attacks, including Mimikatz (credential dumping), Ngrok (creates private connection tunnel), ProcDump (process dumper), Metasploit, anydesk.exe (remote access), and others.

12. **Ransomware Attack on Fencing Systems Maker Zaun Impacts UK Military Data (Security Week, 05 SEP, Ionut Arghire)**

British mesh fencing systems maker Zaun has disclosed a LockBit ransomware attack that potentially led to the compromise of data related to UK military and intelligence sites.

In a data breach notice posted on September 1, Zaun announced that the cyberattack occurred in early August, that it was able to thwart it before data was encrypted, and that its services were not interrupted by the incident.

According to the company, although file-encrypting ransomware was not executed on its systems, the LockBit ransomware group did manage to exfiltrate data from the network.

13. **7 Million Users Possibly Impacted by Freecycle Data Breach (Security Week, 05 SEP, Ionut Arghire)**

Freecycle.org, a platform that allows users to recycle their belongings, has prompted millions of users to reset their passwords after their credentials were compromised in a data breach.

“The breach of data includes usernames, User IDs, email addresses and passwords,” Freecycle says in an incident notice on its website. The passwords were hashed, the platform said in the email notification sent to users, a copy of which was posted on social media.

According to the organization, no other personal information aside from the exposed credentials was compromised during the incident.

14. **Five Eyes Report: New Russian Malware Targeting Ukrainian Military Android Devices (Security Week, 31 AUG, Eduard Kovacs)**

Five Eyes agencies have issued a joint report on the malware used recently by Russian state-sponsored hackers to target Android devices belonging to the Ukrainian military.

The new malware, named Infamous Chisel, is a collection of components designed to provide persistent backdoor access to compromised Android devices over the Tor network, and enable the attackers to collect and exfiltrate data.

The campaign has been linked to the threat actor known as Sandstorm, which was previously connected to Russia’s GRU foreign military intelligence agency.

The report does not mention how the malware has been distributed. However, in early August 2023, the Security Service of Ukraine (SBU) reported that Russian forces had captured Ukrainian tablets on the battlefield and attempted to use them to spread malware. They also tried to leverage the access provided by the tablets to breach military networks.

Back to Table of Contents

Electronic Warfare

1. **[DSEI 2023: Norway opts for new EW solutions from Rohde & Schwarz] (Janes, 14 SEP, Olivia Savage)**

   The Norwegian Army will be equipped with new communications intelligence (COMINT) and jamming solutions from Rohde & Schwarz (R&S), Janes learnt at DSEI 2023, held from 12 to 15 September in London.

   The new electronic warfare (EW) solutions are being delivered under the Heimdall project, which will enable the Norwegian Army to detect, locate, and analyze information faster and more efficiently while increasing their EW capabilities, Wolfgang Marchl, vice-president of R&S Government Solutions said in a company press release.

   Norwegian publication ITromso reported on the Heimdall project noting that the military, specifically the Intelligence Battalion of the Army, are trialing the EW solutions at the Setermoen firing range.

2. **[Electronic warfare in Ukraine informing US playbook] (C4ISR, 13 SEP, Colin Demarest)**

   Ukrainian forces are exploiting gaps in Russian jamming and spoofing capabilities, opening seams in which they make noticeable gains on the battlefield, according to a U.S. Air Force commander.

   While the Russian military seeks to break Ukrainian command and control and block access to the electromagnetic spectrum, used for communications and weapons guidance, among other vital tasks, Ukrainians are resilient and resourceful in their application of electronic warfare, said Col. Josh Koslov, the leader of the 350th Spectrum Warfare Wing.

   The U.S. is observing the invisible back-and-forth and is taking notes as the Pentagon works to reinvigorate jamming and deception arsenals in preparation for potential conflicts with China or Russia.

   The 350th Spectrum Warfare Wing, established two years ago, is the first of its kind and the outgrowth of an electromagnetic spectrum superiority study.

3. **[US Air Force receives first new Compass Call electronic warfare plane] (C4ISR, 12 SEP, Stephen Losey)**

   The U.S. Air Force has received its first EC-37B Compass Call electronic warfare aircraft from contractors BAE Systems and L3Harris Technologies, industry officials announced Tuesday.

   BAE Systems said in a release that the Air Force will next start combined developmental and operational testing for this Compass Call, the first of 10 aircraft planned for the Air Force.

   The Compass Call will conduct a variety of electronic warfare missions to jam enemy signals, including communications, radar and navigation systems. BAE said this will include suppressing enemy air defenses by blocking their ability to transmit information between weapon systems and command-and-control networks.

Back to Table of Contents

Information Advantage

1. **DHS warns of malicious AI use against critical infrastructure (CyberScoop, 14 SEP, Christian Vasquez)**

   The Department of Homeland Security's Homeland Threat Assessment is warning of bad actors potentially using artificial intelligence to disrupt critical infrastructure either through election influence campaigns or by targeting industrial systems.

   The annual report — Homeland Threat Assessment 2024 — which outlines the key concerns for the next year — points to adversaries increasingly focusing and learning how to target critical infrastructure, like energy, the upcoming 2024 election, transportation, pipelines, and other vital services, with emerging technologies like AI.

   While industrial-specific malware is rare, the report warns that hackers are seeking to develop or are developing malicious code that seeks to disrupt the industrial control systems found in the energy, transportation, health care, and election sectors. The malware dubbed "pipedream" by security researchers is one such example of malware made specifically to target industrial devices.

2. **Australian, UK and US tech companies already reaping AUKUS benefits (C4ISR, 14 SEP, Megan Eckstein)**

   Artificial intelligence and autonomy companies from Australia, the United Kingdom and the United States are already feverishly developing and pitching tools to gather ever-more data and then help operators make sense of an information-overload environment.

Back to Table of Contents

   They're hoping all this work will lead to contracts at home and with the allies soon, as more details about the second phase of the AUKUS trilateral arrangement, focused on advanced technology, come to light this fall.

   Little has been formally revealed about the effort. The AUKUS collaboration was announced in September 2021, and in March 2023 the three nations' top leaders gathered in California to reveal plans for the Pillar 1 that's focused on nuclear-powered submarines — first involving U.K. and U.S. vessels operating from an Australian base, then Australia buying American submarines as an interim solution, and then the nations collaborating on an AUKUS-specific attack submarine for the U.K. and Australia to each build and operate.

   Pillar 2 will cover critical technologies: artificial intelligence, quantum computing, hypersonics, autonomy and more, it is believed.

3. **Spies, Hackers, Informants: How China Snoops on the West (Security Week, 11 SEP, Eduard Kovacs)**

   British authorities have arrested a man who reportedly spied for China at the heart of the government in London, sparking fresh fears over how Beijing gathers intelligence.

   The incident follows allegations earlier this year that China flew a surveillance balloon over the United States, causing a diplomatic uproar. Here are some of the ways China has worked to spy on the West in recent years:

   - Cyber warfare
   - Tech fears
   - Industrial and military espionage

- Spying on politicians
- 'Police stations'

4. Defense firms research voice commands to speak with drones (C4ISR, 07 SEP, Elisabeth Gosselin-Malo)

Not far from the front lines, under dense vegetation that obstructs satellite signals, a military nano-sized drone is conducting a reconnaissance mission. From a safe distance, the operator utters a voice command that an artificial intelligence-based software turns into drone language, causing the tiny robot to change course: "Sharp turn left and head straight."

The scenario is hypothetical but seeing drones in conflict zones embedded with an AI-assistant capability, enabling two-way voice communication between drones and their handlers, could become a reality in the not-so-distant future, according to defense analysts.

One of the ways defense manufacturers are approaching the problem is by developing ways to simplify how humans steer drones on the battlefield, injecting voice control into the mix to replace the traditional control panels of sticks and levers.

A company who has been experimenting with the technology is U.S.-based Teledyne Flir Defense, which has partnered with AI startup Primordial Labs, of New Haven, Conn., to include voice control to the Black Hornet micro-drone, widely used by militaries globally.

5. China turns to AI in hopes of creating viral online propaganda, Microsoft researchers say (CyberScoop, 07 SEP, A.J. Vicens)

Back to Table of Contents

Chinese state-affiliated hacking groups are become more adept at using artificial intelligence to generate content designed to "go viral across social networks in the U.S. and other democracies," researchers with the Microsoft Threat Intelligence Center said 07SEP23.

The activity is part of Chinese information operations' increasing success at engaging target audiences around the world, which includes "China's state-affiliated multilingual social media influencer initiative" that has "successfully engaged target audiences in at least 40 languages and grown its audience to over 103 million," the researchers said in the report. Chinese state-sponsored propaganda is pushed by a network of more than 230 "state media employees and affiliates who masquerade as independent social media influencers across all major Western social media platforms," the researchers said.

Part of this activity includes social media personas operated by real people that employ fictitious or stolen identities that conceal connections with the Chinese government and share artificially-generated content. "This relatively high- quality visual content has already drawn higher levels of engagement from authentic social media users," the researchers said.

6. BRI - Belt and Road Initiative - Highlights, 6 September 2023 (U.S. Army Asian Studies Detachment, 12 SEP)

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.

7. **Sluggish deployment of emerging tech hampers US military, officials say (C4ISR, 06 SEP, Colin Demarest)**

The pace at which the U.S. Defense Department is seeking and then deploying cutting-edge technologies, such as those fueled by artificial intelligence, can be slower than the clip at which new dangers arise, leaving troops at a potential disadvantage, according to one official.

U.S. Central Command's chief technology officer, Schuyler Moore, on Sept. 6 said there is a desire to tap "exquisite technologies, that exist both in the department and out in industry, inside a 12-month time frame" should the conditions be right.

To fully exert the power of emerging tech, particularly tied to AI or autonomy, the department must understand that "capabilities require constant innovation and investment," according to Joe Larson, an algorithmic warfare leader within the Chief Digital and AI Office.

The Pentagon rolled out its largest-ever innovation and modernization budget earlier this year, requesting $145 billion from Congress in fiscal 2024. The ask, about $15 billion more than the year prior, designates $687 million for the Rapid Defense Experimentation Reserve, an initiative spearheaded by Heidi Shyu, the undersecretary of defense for research and engineering, that aims to fill high-priority gaps with advanced tech.

Back to Table of Contents

Signal

1. **North American Airspace Defense Getting Cloud-Based Backbone Next Month (The Drive/The Warzone, 15 SEP, Hope Hodge Seck)**

   Cloud-based command-and-control for air defense over North America is set to be declared operational next month.

   The cloud-based system the Air Force is co-developing with Canada to enable instantaneous combat data-sharing is just about ready for prime time, although the looming threat of a budget gap may slow its global deployment.

2. **How two SATCOM companies are responding to Starlink's dominance (C4ISR Net, 15 SEP, Courtney Albon)**

   With SpaceX's Starlink constellation dominating the space-based communications market, longstanding satellite operators are positioning themselves to compete with the billionaire-owned company — particularly when it comes to military and government services.

3. **DSEI 2023: Saab debuts deployable variant of Giraffe 1X radar (Janes, 13 SEP, Olivia Savage)**

   Saab has launched a deployable variant of its Giraffe 1X 3D radar at DSEI 2023, held from 12 to 15 September in London.

   Known as the Deployable Set, the new configuration is designed as a compact, robust, and highly deployable radar that can be easily transported and quickly set up.

   A key difference with the deployable variant is its ability to operate on the move when deployed on naval vessels or land vehicles, while maintaining the same radar performance as the original system, Fredrik Sämfors, head of Giraffe 1X radar solutions told Janes.

4. **Spectra to provide SlingShot satcom systems to Indonesian Army (Janes, 07 SEP, Oishee Majumdar)**

   The UK's Spectra Group will supply its SlingShot satellite communication (satcom) systems to the Indonesian Army.

   Spectra announced on 07SEP23, that it has partnered with Jakarta-based defence equipment provider, PT Mora Armamen Perkasa, to provide an undisclosed number of SlingShot manpack systems, SlingShot vehicle systems, and SlingShot Tactical Operations Centre Systems (STOCSs) to the Indonesian Army.

   A company spokesperson told Janes that Spectra has started delivering the SlingShot systems to the Indonesian Army and expects to complete the deliveries by the end of 2023.

Back to Table of Contents

Items of Interest

1. **North Korea: Kim Jong Un and Russian President Putin in Talks (U.S. Army Asian Studies Detachment, 14 SEP)**

   Kim Jong Un is visiting Russia and holding talks with Russian President Putin. A translation of North Korean media coverage of the visit and talks follow.

2. **North Korea: Kim Jong Un's "Historic" Meeting with Russian President Putin at Vostochny Spaceport (U.S. Army Asian Studies Detachment, 14 SEP)**

   Kim Jong Un is visiting Russia and holding talks with Russian President Putin. A translation of North Korean media coverage of the visit and talks follow.

3. **Kim Jong Un vows full support for Russia as Putin pledges space tech for North Korea (NPR, 13 SEP, Anthony Kuhn)**

   North Korean leader Kim Jong Un promised his full support for Russian President Vladimir Putin in what he called a "fight against imperialism" in a summit in Russia, saying the countries' relations are a "top priority."

   Putin offered North Korea technological assistance to launch a satellite into space and said there are "possibilities" for military cooperation between them.

   The meeting, which lasted more than four hours 13SEP23 in Russia's Far East, showed how geopolitical tensions have brought the two neighbors isolated by the West into closer alignment. It comes as the U.S. has warned that Putin and Kim could strike an arms deal that would provide North Korean munitions for Russia's war in Ukraine.

   Asked if Russia would help North Korea with its satellites, Putin was quoted by Russian media as saying that was why Vostochny was chosen as the venue for their meeting. North Korea failed twice this year to put a spy satellite in orbit but says it will try again next month.

4. **N. Korea Fires Ballistic Missile Toward East Sea: S. Korean Military (The Korea Herald, 13 SEP, Yonhap)**

   North Korea fired an unspecified ballistic missile toward the East Sea on Wednesday, South Korea's military said, as the North's leader Kim Jong-un is set to hold a rare summit with Russian President Vladimir Putin. The Joint Chiefs of Staff announced the launch but gave no further details, pending an analysis. Pyongyang's latest saber-rattling came as the country's leader departed for Russia on Sunday to meet with Putin amid concerns over a possible arms deal that could support Moscow's war in Ukraine. It remains unknown exactly when and where Kim and Putin would hold their meeting, although some foreign media reports said the summit would likely take place Wednesday at Russia's Vostochny Cosmodrome space center in the Amur region. The North has continued to press ahead with weapons tests in defiance of U.N. Security Council resolutions banning the country from launches using ballistic missile technology.

5. **Sweden's Saab snags Silicon Valley-based CrowdAI (C4ISR, 06 SEP, Colin Demarest**

   wedish defense company Saab AB acquired artificial intelligence firm CrowdAI, again expanding its footprint in the fast-growing sector.

The deal's closing was announced Sept. 7. No financial details were shared. Saab ranked No. 33 in the latest Defense News "Top 100" analysis of the world's largest defense companies, raking in $3.7 billion in defense revenue in 2022.

Erik Smith, president of Saab in the U.S., in a statement said the takeover provides the company "a new capability as well as deeply rooted relationships with new customers." It also underscores "our commitment to innovation and growth in the United States," he added.

Saab last month acquired BlueBear Systems, a British company that specializes in autonomy, avionics, and modeling and simulation. Terms were not disclosed at the time. BlueBear last year had a turnover of £8 million, or $10 million, Defense News reported.

Back to Table of Contents

Russia-Ukraine

1. Russia-Ukraine Situation Report

Russia-Ukraine Situation Report,14 September 2023
Russia-Ukraine Situation Report,13 September 2023
Russia-Ukraine Situation Report,11 September 2023
Russia-Ukraine Situation Report,08 September 2023

2. The DRIVE/Warzone Ukraine Situation Report

Ukraine Situation Report: Small Town Near Bakhmut Recaptured – 15 SEP
Ukraine Situation Report: Kyiv Claims It Knocked Out S-400 In Crimea – 14 SEP
Ukraine Situation Report: U.S. Warns North Korea, Russia Against Arms Deals – 13 SEP
Ukraine Situation Report: Kyiv Says Black Sea Platforms Recaptured From Russia – 11 SEP
Ukraine Situation Report: M1 Abrams Tank Training Extended – 08 SEP
Ukraine Situation Report: Breakthrough At Russia's Second Defensive Line – 07 SEP
Ukraine Situation Report: Counteroffensive Pushes Toward Second Defensive Line – 05 SEP
Ukraine Situation Report: Wild Video Shows Bradley Blasting Another In Training – 01 SEP

3. Ukraine just carried out the same kind of strike on Russia's navy that Elon Musk blocked, believing it could start a nuclear war (Insider, 13 SEP)

Flames engulfed Russian naval ships in a major dockyard in the occupied Ukrainian peninsula of Crimea on 12SEP23 after a Ukrainian missile attack.

The attack was notable not just as another example of Ukraine's capacity to strike Russia deep behind its front line but also, said critics, because it exposed the falsity of SpaceX founder Elon Musk's reasons to scupper a similar Ukrainian strike.

The SpaceX CEO last year effectively sabotaged a Ukrainian attack as drones were bearing down on Russian naval vessels in Sevastopol in the early weeks of the conflict.

Musk decided not to activate the Starlink satellites used to guide the drones, fearing the attack could be a new Pearl Harbor that would escalate the conflict and potentially invite a nuclear response from Russia.

4. Starlink vital despite not working for 'some time,' says Ukrainian official (AeroTime, 11 SEP, Emilia Stankeviciute)

Elon Musk's Starlink satellite connection is being used by Ukrainian soldiers on all front lines in the war with Russia, a top Ukrainian official has said.

Speaking at the annual Yalta European Strategy meeting on 09SEP23, Kyrylo Budanov, head of the Main Ukrainian Intelligence Directorate, also confirmed that Starlink coverage "did not work for some time" in Russian-occupied Crimea but continues "to play a significant role" in the battlefield.

Budanov's comments follow allegations that Musk was involved in sabotaging his company's Starlink satellite communications network.

However, on September 8, 2023, Musk denied any involvement in the sabotage

mentioned in the biography and stated that the Starlink network in the region could not be turned off as it was not actually turned on.

5. **Cuba arrests 17 for allegedly helping recruit some of its citizens to fight for Russia in Ukraine (AP, 08 SEP, Cristiana Mesquita and Milexsy Durán)**

Cuban authorities have arrested 17 people in connection with what they described as a network to recruit Cuban nationals to fight for Russia in Ukraine.

The head of criminal investigations for Cuba's Interior Ministry, César Rodríguez, said late Thursday, 07SEP23, on state media that at least three of the 17 arrested are part of recruitment efforts inside the island country.

He did not identify the alleged members of the network but said they had previous criminal records. Some families started speaking up about the case on 08SEP23, and at least one mother said that her son was promised a job in construction in Russia.

Cuba's Foreign Ministry said on Monday that the government had detected a network operating from Russia to recruit Cuban citizens living both in Russia and in Cuba to fight in Ukraine. It said authorities were working "to neutralize and dismantle" the network but gave no details.

6. **Elon Musk denies sabotaging Starlink in Ukraine-Russia conflict (AeroTime, 08 SEP, Emilia Stankeviciute)**

Back to Table of Contents

Elon Musk claims he did not order to shut down the Starlink satellite connection near the coast of Russian-occupied Crimea to hinder a Ukrainian attack on the Russian naval fleet, he simply refused to activate it.

SpaceX has been supplying Starlink terminals to Ukraine since the beginning of the war in 2022 to provide internet connection to the country's civilians and military.

Starlink's high-speed connectivity has proved crucial for the Ukrainian military, especially for unmanned systems such as drones. However, according to an upcoming book, Musk has found himself entangled in the ongoing Ukraine-Russia conflict.

7. **First Ukrainian M1 Abrams Tank Crews Complete Training (The Drive/The Warzone, 01 SEP, Thomas Newdick)**

Ukraine's M1 Abrams tanks are set to arrive in the next few weeks and they are likely to be rushed to the front before the rains hit.

The first of Ukraine's U.S.-supplied M1 Abrams main battle tanks appear to be on track to go into combat starting from mid-September, with the news that a cadre of Ukrainian crews have finished their training on them. Meanwhile, as we have reported in the past, 31 Abrams tanks destined for Ukraine — all older M1A1 variants — have been undergoing refurbishment and preparation for delivery.