U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

16-30 September 2023

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

POC: Jeffrey Hardimon, Kevin Bird &
SGT Christian Shager
706-849-9259

Table of Contents

Cyber

Electronic Warfare

Information Advantage

Signal

3. Indian Army Seeking Modern, Satellite-Based Communication Capability – 20 SEP
4. US Army taps CACI-owned company for jamming kit that troops can carry – 20 SEP
5. The HF Renaissance – The Evolving Electronic Warfare Threats and the Need for Resilient Waveforms (Studio) – 14 SEP

Items of Interest

1. Undersecretary of the Army directs review of electronic warfare portfolio – 27 SEP
2. US officials say Travis King, who crossed into North Korea, is in American custody – 27 SEP
3. NATO to publish first C-UAS doctrine this year – 26 SEP
4. Taiwan Finds 1 In 3 Spies Serving In Military – 27 SEP
5. Israeli companies showcase drones that take off, land vertically – 19 SEP
6. US sanctions firms in China , Russia, Turkey over Iran's drone program – 19 SEP
7. North Korea's Leader Wraps Up Russia Trip With Drones Gift – 18 SEP

Russia-Ukraine Situation

1. Russia-Ukraine Situation Report
2. Ukraine conflict: European countries approve new weapons donations – 21 SEP
3. Poland is done sending arms to Ukraine, as trade dispute escalates – 21 SEP
4. US charges Russian man with smuggling microelectronics amid Ukraine war – 19 SEP
5. Russia's Tiny Drones Are Now Flying Far Enough To Blow Up Ukrainian MiGs At Their Bases – 19 SEP
6. Ukraine fires 6 deputy defense ministers as counteroffensive continues – 18 SEP
7. With A Special Warhead Blew Up That Russian Submarine From The Inside – 18 SEP
8. South Korean Breaching Vehicles Will Help Ukraine Replace Its Counteroffensive Losses – 18 SEP

Cyber

1. **[Russian Zero-Day Acquisition Firm Offers $20 Million for Android, iOS Exploits] (Security Week, 28 SEP, Ionut Arghire)**

   Operation Zero, a Russian zero-day acquisition firm, announced this week that it is offering up to $20 million for full exploit chains targeting Android and iOS devices.

   Launched in 2021, the firm says it provides "technologies for offensive and defensive operations in cyberspace" and claims to be working with private and government organizations in Russia.

   On its website, Operation Zero claims to be "the only official Russian zero-day purchase platform", which was "created by information security professionals and for professionals". It also claims that researchers should rest assured that these exploits will not fall "into the wrong hands".

   Zero-day acquisition firms such as Operation Zero typically purchase exploits targeting unreported vulnerabilities to sell them to government agencies or private organizations, without informing vendors of the bugs.

2. **[Government Shutdown Could Bench 80% of CISA Staff] (Security Week, 28 SEP, Eduard Kovacs)**

   The US government will partially shut down on Sunday, 01OCT23, unless lawmakers reach a deal on a funding bill. A shutdown will result in the furlough of hundreds of thousands of non-essential federal employees and the suspension of many services.

   The Department of Homeland Security has announced the number of employees that would stay on during a shutdown for each of its agencies. In the case of CISA, which had 3,117 employees as of 17JUN23, only 571 would remain during a lapse in appropriations. This means that more than 80% of its workers would be furloughed.

   A government shutdown can have a significant impact on cybersecurity, including increasing criminal activity, failure to renew digital certificates, failure to deploy security patches, and denting the government's ability to recruit talent.

   In CISA's case, the agency plays an important role in protecting the government and the private sector against cyber threats. This includes issuing warnings over actively exploited vulnerabilities, helping investigate high-impact cyberattacks, creating guidance, aiding critical infrastructure organizations beef up their security, conducting cyber exercises, and assisting with incident response.

3. **[Chinese Gov Hackers Caught Hiding in Cisco Router Firmware] (Security Week, 27 SEP, Ryan Naraine)**

   A Chinese state-sponsored APT called BlackTech has been caught hacking into network edge devices and using firmware implants to stay hidden and silently hop around the corporate networks of U.S. and Japanese multinational companies.

   According to a high-powered joint advisory from the NSA, FBI, CISA and Japan's NISC, BlackTech has been observed modifying router firmware on Cisco routers to maintain stealthy persistence and pivot from international subsidiaries to headquarters in Japan and the United States.

   To extend their foothold across an organization, the BlackTech attackers target branch routers — typically smaller appliances used at remote branch offices to connect to a corporate headquarters — and abuse the trusted relationship of the branch routers within the corporate network being targeted.

Back to Table of Contents

The attackers then use the compromised public-facing branch routers as part of their infrastructure for proxying traffic, blending in with corporate network traffic, and pivoting to other victims on the same corporate network.

4. **AE-Linked APT Targets Middle East Government With New 'Deadglyph' Backdoor (Security Week, 26 SEP, Ionut Arghire)**

The advanced persistent threat (APT) actor Stealth Falcon has been observed deploying a new backdoor on the systems of a governmental entity in the Middle East, for espionage purposes, ESET reports.

The new backdoor, which ESET has named Deadglyph, consists of a native x64 binary that functions as an executor, and a .NET assembly that functions as an orchestrator.

The malware is delivered on the system in the form of a DLL that abuses Windows Management Instrumentation (WMI) event subscription for persistence, and which functions as a registry shellcode loader.

Once executed, the DLL loads, decrypts, and executes encrypted shellcode stored in the Windows registry, which leads to decrypting and running the executor component of Deadglyph.

5. **Army cyber tool will focus on broader information environment (Defense Scoop, 25 SEP, Mark Pomerleau)**

A tool the Army had been developing to allow commanders to visualize the cyberspace environment is evolving to encompass the entire information environment, including social media.

Back to Table of Contents

Cyber Situational Understand, or Cyber-SU, is specifically designed for ground commanders to have better insight into the cyber and electromagnetic landscape to make more informed decisions, but it is not meant to be used for cyberspace operations.

To date, they've only done basic threads on the publicly available information aspect at the recent Cyber Quest, an experimentation venue where the Army seeks to test emerging technologies on either existing or desired capabilities brought by contractors to help inform future requirements and concepts. The plan is to soon bring this to the field with actual units. Only about a month ago, the Army started integrating the Cyber-SU capability with the data fabric solution.

6. **Stealthy APT Gelsemium Seen Targeting Southeast Asian Government (Security Week, 25 SEP, Ionut Arghire)**

A stealthy advanced persistent threat (APT) actor known as Gelsemium has been observed targeting a government entity in Southeast Asia to establish persistence and collect intelligence, cybersecurity firm Palo Alto Networks reveals.

As part of the observed activity, spanning over a period of six months in late 2022 and into 2023, the threat actor deployed a variety of web shells to support lateral movement and malware delivery, along with backdoors, a Cobalt Strike beacon, and various other tools.

Palo Alto Networks did not make any claims regarding attribution but noted that others linked Gelsemium to China in the past.

The cybersecurity firm identified three web shells used in these attacks, namely reGeorg, China Chopper, and AspxSpy (publicly available). In some instances, the threat actor deployed a shell-like tool to run additional commands, and several privilege escalation tools.

7. **[China's Offensive Cyber Operations in Africa Support Soft Power Efforts] (Security Week, 22 SEP, Eduard Kovacs)**

Chinese state-sponsored threat groups have targeted telecommunications, financial and government organizations in Africa in support of Beijing's soft power agenda in the region, according to SentinelOne.

Earlier this year, SentinelOne reported seeing a Chinese cyberespionage group targeting telecoms providers in the Middle East as part of an operation dubbed Tainted Love.

The cybersecurity firm revealed on Thursday that the same threat actor, which could be linked to China's APT41 group, has also been observed targeting a North African telecommunications organization as part of what appears to be an operation supporting China's soft power efforts.

In addition, SentinelOne has been monitoring a China-linked APT named BackdoorDiplomacy, which has targeted Africa for several years. Reuters reported recently that the group has targeted the Kenyan government, possibly in an effort to collect information on debt owed to China.

8. **[MGM Resorts Computers Back Up After 10 Days as Analysts Eye Effects of Casino Cyberattacks] (Security Week, 20 SEP, Associated Press**

MGM Resorts brought to an end a 10-day computer shutdown prompted by efforts to shield from a cyberattack data including hotel reservations and credit card processing, the casino giant said Wednesday, as analysts and academics measured the effects of the event.

Back to Table of Contents

Rival casino owner Caesars Entertainment also disclosed last week to federal regulators that it was hit by a cyberattack Sept. 7. It said that its casino and online operations were not disrupted but it could not guarantee that personal information about tens of millions of customers, including driver's licenses and Social Security numbers of loyalty rewards members, had not been compromised.

Caesars, based in Reno, is widely reported to have paid $15 million of a $30 million ransom sought by a group called Scattered Spider, a group of English-speakers also sometimes known as Øktapus operating under a Russia-based operation called ALPHV or BlackCat. for a promise to secure the data.

9. **[Chinese Hackers Target North American, APAC Firms in Web Skimmer Campaign] (Security Week, 19 SEP, Ionut Arghire)**

BlackBerry is warning of a widespread campaign targeting online payment businesses with web skimmers for more than a year.

Dubbed Silent Skimmer, the campaign initially focused on organizations in the APAC region but has been targeting businesses in Canada and the United States as well since October 2022, and appears to be expanding to new areas.

The attackers have been observed targeting multiple industries that host or create payment infrastructure, including online businesses and point-of-sales (PoS) providers, exploiting internet-facing applications for initial access, and deploying various tools to escalate privileges, execute code, and gain remote access.

Analysis of the server the RAT connects to reveal a broad range of tools, including downloader scripts, remote access scripts, webshells, exploits, and Cobalt Strike beacons. On the server, BlackBerry also discovered Fast Reverse Proxy (RFP), a tool that allows attackers to expose local servers located behind a NAT.

10. **[Thousands of Juniper Appliances Vulnerable to New Exploit](#) (Security Week, 19 SEP, Ionut Arghire)**

Threat intelligence firm VulnCheck has published details on a new exploit targeting a recent Junos OS vulnerability and says that thousands of Juniper Networks appliances that have not been patched are at risk.

The flaw, tracked as CVE-2023-36845, is described as a PHP environment variable manipulation issue in the J-Web interface of Juniper's SRX series firewalls and EX series switches running specific Junos OS versions.

In mid-August 2023, the networking appliances maker released patches for this bug and three other medium-severity issues, warning that an attacker could chain them to achieve remote code execution (RCE) on a vulnerable device, and that the exploit chain should be considered as having a 'critical severity' rating.

11. **[Pakistani APT Uses YouTube-Mimicking RAT to Spy on Android Devices](#) (Security Week, 19 SEP, Ionut Arghire)**

Pakistan-linked state-sponsored threat actor Transparent Tribe has been observed using new versions of the CapraRAT Android trojan that mimic the appearance of YouTube, SentinelOne reports.

Earlier this year, the threat actor was seen distributing CapraRAT iterations masquerading as a dating service app, most likely via a romance scam. The three recent CapraRAT samples that mimic YouTube appear to use the same scheme for distribution, SentinelOne says.

[Back to Table of Contents](#)

The samples borrow the YouTube icon and request permissions typically associated with the legitimate video sharing service, including microphone access. When executed, the malware launches a WebView object to load the YouTube website, so as not to raise suspicion.

Once installed on a victim's device, the malware can make recordings using the microphone and cameras, collect messages and call logs, send and block messages, make phone calls, take screenshots, override system settings for GPS and network, and modify files.

12. **[Russia-Ukraine conflict forces DOD to revise assumptions about cyber's impact in war](#) (Defense Scoop, 18 SEP, Mark Pomerleau)**

Russia's invasion of Ukraine in February 2022 — and the subsequent year-and-half of combat — has made the Pentagon rethink the role cyber will play in war, namely, that there won't be immediate payoff of effects.

While many government officials and cybersecurity experts have all acknowledged Russian missteps and flawed assumptions going into the war — to include how their application of cyber in the conflict underperformed — the Department of Defense has observed that cyber operations will not have the role previously thought.

The DOD's 2023 cyber strategy, unveiled mid-September 2023, notes that cyber capabilities by themselves are unlikely to deter adversaries. Rather, they are best used alongside other instruments of national power.

The DOD for years has believed that cyber will be a part of conflicts and has worked to create mechanisms and organizations to integrate digital operations into the planning cycles alongside the traditional domains of war. Indeed, Eoyang in the past has suggested that the Russia-Ukraine conflict has forced the department to think differently about cyber.

13. **Canadian Government Targeted With DDoS Attacks by Pro-Russia Group (Security Week, 18 SEP, Ionut Arghire)**

The pro-Russian cybercrime group named NoName057(16) has been observed launching distributed denial-of-service (DDoS) attacks against Canadian organizations, a fresh government alert warns.

Since March 2022, the threat actor – also known as NoName05716, 05716nnm or Nnm05716 – has been launching disruptive attacks in support of Russia's invasion of Ukraine.

To date, the group has targeted financial, government, military, media, supply, telecoms, and transportation organizations in Ukraine and NATO-associated targets, including the Czech Republic, Denmark, Estonia, Lithuania, Norway, and Poland.

14. **Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets (Microsoft, 14 SEP, Microsoft Threat Intelligence)**

Since February 2023, Microsoft has observed password spray activity against thousands of organizations carried out by an actor we track as Peach Sandstorm (HOLMIUM). Peach Sandstorm is an Iranian nation-state threat actor who has recently pursued organizations in the satellite, defense, and pharmaceutical sectors around the globe. Based upon the profile of victim organizations targeted and the observed follow-on intrusion activity, Microsoft assesses that this initial access campaign is likely used to facilitate intelligence collection in support of Iranian state interests.

Back to Table of Contents

Electronic Warfare

1. **Undersecretary of the Army directs review of electronic warfare portfolio (Defense Scoop, 27 SEP, Mark Pomerleau)**

   The undersecretary of the Army has directed a complete review of the service's electronic warfare capabilities, Defense Scoop has learned. In what is called a capability portfolio review, Gabe Camarillo has directed the Army to examine potential gaps and priority investments in its electronic warfare portfolio.

   The Army currently has no fielded program-of-record jammers – relying for years on quick reaction capabilities developed to address capability gaps in Europe. It is working to develop a bevy of capabilities to include airborne platforms as well as vehicle-mounted and dismounted systems that span the tactical sphere as well as long-range. Despite taking several years of development, with program-of-record systems slated to field in the next year, Camarillo told reporters he is largely pleased with the Army's progress but noted that there is more work to do, adding "there's always room for us to improve the speed and acceleration at which we can turn out capabilities."

1. **Electronic warfare: all systems go (Military Aerospace, 27 SEP, Jim Romeo)**

   Many new technologies, processes, and collaborations all are converging on electronic warfare (EW), providing reason to be optimistic and bullish about its future.

   Jonathan Roberts is an engineer at the RAND Corporation in Santa Monica, Calif., whose research focuses on EW, radar, and low-observable technology.

   "Since the Electromagnetic Spectrum Superiority Strategy was released in 2020 there has been a lot of work put into harmonizing capabilities between services and partner nations. In terms of general EW technology, cognitive EW is the future," Roberts says. "Cognitive EW is driving advances in data science and signal processing related to what we field and how we think about data that would have previously been discarded."

2. **NATO conducts major electronic warfare exercise (UK Defense Journal, 25 SEP, George Allison)**

   Standing NATO Maritime Group Two (SNMG2) spearheaded an electronic warfare and anti-ship missile defence exercise called "Dynamic Guard" from Sept. 4-8 in the Alboran Sea, off Cartagena, Spain.

   "Dynamic Guard 23-II" aimed to give Allied forces the opportunity to "test, train and enhance the techniques required to operate in a degraded or denied electro-magnetic environment."

3. **Soldiers Experiment with Electronic Warfare in Contested Environment (DVIDS, 25 SEP, David Overy)**

   During a four-day exercise at Camp Shelby Joint Forces Training Center (CSJFTC), Soldiers from the Mississippi Army National Guard (MSARNG) trained for a scenario where four Soldiers of the 2nd Battalion, 198th Armored Regiment (2-198 AR), were killed in action during an ambush.

   The 2-198 AR unit was utilizing electronic warfare (EW) to conduct an intelligence, surveillance, and reconnaissance (ISR) operation in a contested environment. However, the unit was unaware that EW was being utilized by their adversary to locate their position, jam their communication, and attack. For most of the warfighters, this was their first experience facing a threat from a near-peer adversary in multi-domain warfare.

The exercise, named Thunderstrike II, allowed 2-198 AR warfighters to immerse themselves in live, unscripted, force-on-force scenarios to experiment with how the Army needs to train and condition its units to fight in this new environment.

4. **US Army Testing Drone-Borne Electronic Warfare Capability (The Defense Post, 22 SEP, Joe Saballa)**

   The US Army has begun testing a new electronic warfare (EW) payload designed to be integrated into unmanned aerial vehicles.

   The drone-borne tech, called the Multi-Function Electronic Warfare – Air Large (MFEW-AL), is being assessed at Joint Base McGuire-Dix-Lakehurst in New Jersey ahead of its integration into an MQ-1C Gray Eagle.

   According to the service, the system features cutting-edge components to provide improved electronic attack and EW support capability to warfighters.

5. **Lockheed Conducts AI-Commanded Electronic Warfare Mission (The Defense Post, 19 SEP, Joe Saballa)**

   Lockheed Martin has demonstrated the ability of artificial intelligence (AI) to assist in electronic warfare missions.

   The company recently announced that trained AI agents successfully commanded two piloted L-29 aircraft to perform jamming support in a simulated air-to-ground mission.

   During the demonstration, the L-29s acted as autonomous uncrewed aerial system surrogates and followed instructions from the AI agents for their flight altitude and speed.

6. **Boeing to Upgrade Japan's F-15s With Advanced Electronic Warfare Suite (The Defense Post, 18 SEP, Inder Bisht)**

   Boeing has been contracted to outfit Japanese F-15 Super Interceptor fighter jets with an advanced electronic warfare system.

   The Boeing-BAE Systems Eagle Passive Warning Survivability System (EPWSS) will enhance the aircraft's survivability in contested, signal-dense environments.

   According to BAE, the system's advanced radio frequency electronic countermeasures provide rapid response capabilities and enable deeper penetration against modern integrated air defense systems.

   The system features "broad instantaneous bandwidth and a high-speed scan capability to detect all radio frequency threat classes, including low probability of intercept and modern agile threats."

7. **European airborne electronic-attack program kicks into high gear (Defense News, 18 SEP, Vivienne Machi)**

   An Indra-led consortium of European companies is set to launch work on an electronic-warfare capability for the European Union aimed at protecting friendly aircraft against missile attacks.

   In a few months, the bloc's Responsive Electronic Attack for Cooperative Tasks (REACT) effort will begin its second phase, company officials told Defense News. The consortium, which includes European sensor makers Hensoldt, Elettronica and Saab, was selected in June to receive tens of millions of euros in funds from the European Defence Fund (EDF) for the work.

The REACT program is intended to develop a system capable of jamming any signals used for targeting European aircraft while being able to disable adversary electronic-warfare emitters, according to a European Defence Fund fact sheet. As European forces are facing increasingly sophisticated long-range, integrated air defense systems, airborne electronic attack (AEA) capabilities become “essential to create safe bubbles around formations of aircraft,” said Pablo González, director for NATO and European defense and space programs at Indra.

8. Electronic warfare in Ukraine informing US playbook (C4ISRNet, 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.

Back to Table of Contents

Information Advantage

1. **US issues stern warning on China's global information efforts (TRT World, 28 SEP, Baba Umar)**

   State Department report warns of Beijing's efforts in information sphere, alleging the Asian giant's "digital authoritarianism" and "disinformation" could reshape the world if unchecked.

   China has invested billions of dollars to construct a global information ecosystem that promotes its "propaganda" and "disinformation", but the country has faced setbacks in democratic countries, a US State Department report alleged.

   The report released on Thursday accused Beijing of "bending" the global information environment to its advantage, arguing that China was "leveraging propaganda and censorship, promoting digital authoritarianism, exploiting international organisations and bilateral partnerships, pairing co-optation and pressure, and exercising control over Chinese-language media."

2. **China Spending Billions on Global Disinformation, Us Contends (Bloomberg, 28 SEP, Lain Marlow)**

   China spends billions of dollars each year to enhance its image around the world, including by sponsoring online influencers and bolstering authoritarian governments through the export of “smart cities” technology, the US government says in a new report.

   The State Department’s Global Engagement Center, which works to counter foreign disinformation and propaganda, labeled China a “leading concern” in an 81-page report released Thursday that argues Beijing has worked to spread false information around the world, amplify its propaganda and suppress and censor dissenting voices.

3. **The Future Of AI Policy In China – Analysis (Eurasian Review, 28 SEP, Huw Roberts & Emmie Hines)**

   Rapid developments in generative artificial intelligence (AI) — algorithms used to create new text, pictures, audio, or other types of content — are concerning regulators globally. These systems are often trained on personal and copyrighted data scraped from the internet, leading to privacy and intellectual property fears. They can also be used to generate harmful misinformation and disinformation.

   On 15 August 2023, a new Chinese law designed to regulate generative AI came into force. This law, the latest in a series of regulations targeting different aspects of AI, is internationally groundbreaking as the first law that specifically targets generative AI. It introduces new restrictions for companies providing these services to consumers regarding both the training data used and the outputs produced.

4. **Army awards contracts for first AI program of record (Defense Scoop, 27 SEP, Mark Pomerleau)**

   The Army has awarded the first of what it anticipates being many contracts related to the service’s first artificial intelligence and machine learning program of record.

   Booz Allen Hamilton and Red Hat both won a contract through a Broad Agency Announcement worth a combined value of $2 million to support research and development for Project Linchpin, the Army said in a release Wednesday.

   Project Linchpin aims to provide an artificial intelligence operations pipeline for Army programs, beginning with the Tactical Intelligence Targeting Access Node (TITAN)

program.

The deal has a six-month period of performance along with an option of no more than five years. Specifically, the contract deals with research for principles of Traceability, Observability, Replaceability and Consumability (TORC), according to a release from Program Executive Office Intelligence, Electronic Warfare and Sensors.

5. **Fact check: Fake Zelenskyy video raises fears of AI disinfo (DW, 26 SEP, Rachel Baig)**

Social media users are claiming a video was showing Volodymyr Zelenskyy belly dancing. But the viral clip of the Ukrainian president is not genuine, it was manipulated – and shows somebody else.

Since Russia's invasion of Ukraine in February 2022, a lot of mis- and disinformation has been spread by both sides. However, when it comes to mis- and disinformation about Ukraine, it is often President Zelenskyy himself who is the target of smear campaigns.

6. **Air Force issues BAA for 'extreme' computing tech (Defense Scoop, 21 SEP, Jon Harper)**

The Air Force Research Lab is soliciting white papers for cutting-edge computing capabilities that could address size, weight, and power constraints for military platforms.

The broad agency announcement, released Wednesday on Sam.gov, comes about a month after AFRL's information directorate opened a new Extreme Computing Facility in Rome, New York.

The lab is looking for vendors for research, development, integration, test and evaluation of "technologies/techniques to support research in the focus areas computational diversity and efficient computing architectures, machine learning and artificial intelligence in embedded system and architectures, computing at the edge, nanocomputing, space computing, and robust algorithms and applications," per the BAA.

Potential applications of the technology could include autonomous systems and neuron-electronic bio-interfaces, according to AFRL.

7. **China to Introduce Model Zone for "Taiwan Reunification" in Fujian Province (US Army Asian Studies Detachment, 20 SEP)**

On 12SEP23, to "resolve the Taiwan issue and realize the complete reunification of the motherland," China has announced plans to make Fujian Province, located on the opposite coast of Taiwan, a model zone for the integration and development of China and Taiwan. According to a Taiwanese researcher, the political purpose of these measures is to bypass the Taiwanese government and give the Chinese government direct control over Taiwanese people and businesses.

Chinese state media Xinhua reported that China will make Fujian Province a demonstration zone for integrated development across the Taiwan Straits, according to a statement released on 12SEP23. The statement, jointly issued by the CCP Central Committee and the State Council, said the move is aimed at deepening cross-Straits integrated development in all fields and advancing the peaceful reunification of the motherland.

The statement points out that it should facilitate the life of "Taiwanese compatriots" in Fujian by:

- Abolishing the registration of Taiwanese as temporary residents in Fujian
- Encouraging Taiwan compatriots to apply for the Taiwan Resident Residence Card
- Making it so that "all Taiwan compatriots who wish to settle here can settle"

- Expanding the scope of application of identity verification of the Taiwan Resident Residence Permit Striving to make it equally convenient to apply for a Taiwan Resident Residence Permit or a Mainland Resident Identity Card.

Back to Table of Contents

Signal

1. **[China plans second megaconstellation, G60 Starlink with 12,000 satellites, to rival American SpaceX programmed] (South China Morning Post, 30 SEP, Ling Xin)**

   China is pushing ahead with the construction of a second satellite megaconstellation to provide broadband internet services and compete with SpaceX's Starlink.

   G60 Starlink, which is backed by the Shanghai municipal government, will eventually comprise more than 12,000 satellites in low earth orbit.

   Its potential size is similar to Guo Wang, or National Network, a separate constellation consisting of some 13,000 satellites and commonly known as China's answer to Starlink. It is now under construction by the state-owned Guo Wang company.

2. **[Post-Quantum Cryptography: Finally Real in Consumer Apps?] (The Hacker News, 29 SEP)**

   Most people are barely thinking about basic cybersecurity, let alone post-quantum cryptography. But the impact of a post-quantum world is coming for them regardless of whether or not it's keeping them up tonight.

   Today, many rely on encryption in their daily lives to protect their fundamental digital privacy and security, whether for messaging friends and family, storing files and photos, or simply browsing the web. The question experts have been asking for a long time, with their eye on the advances in quantum computing, is, "How long before these defenses fail?"

3. **[Indian Army Seeking Modern, Satellite-Based Communication Capability] (The Defense Post, 20 SEP, Joe Saballa)**

   The Indian Army is acquiring various advanced SATCOM systems to assist its troops on missions. Around mid-September 2023, the service reportedly contracted Bharat Electronics to supply more than 160 mobile secure satellite terminals.

   This is on top of the defense deals inked earlier, which include 150 man-portable Ku-band satellite terminals, 400 S-band hand-held terminals, and 300 S-band manpack terminals. The Indian Army has SATCOM sets that assist troops on long-range patrols along the line of actual control (LAC) bordering China.

   However, such systems have become obsolete over the years, with operators complaining about not being able to communicate effectively with their operating bases. The SATCOM systems will reportedly "plug this void" because they "cannot be intercepted" by enemies.

4. **[US Army taps CACI-owned company for jamming kit that troops can carry] (Defense News, 18 SEP, Colin Demarest)**

   The U.S. Army selected a CACI International-owned company to prototype a jammer that soldiers can carry and use on foot to spy on electronic signals.

   The preliminary deal with Mastodon Design for the Terrestrial Layer System-Brigade Combat Team Manpack effort is worth $1.5 million and runs for nine months, the service's Program Executive Office for Intelligence, Electronic Warfare and Sensors said Sept. 15. The contract award follows a half-year of white paper submissions and technical evaluations.

   The TLS-BCT Manpack is meant to give troops on the move a means of conducting

electronic warfare and signals intelligence. It is a smaller offshoot of the TLS-BCT, to be installed aboard Stryker combat vehicles, and the even beefier TLS-Echelons Above Brigade, envisioned for use by larger formations including divisions and corps.

5. **The HF Renaissance – The Evolving Electronic Warfare Threats and the Need for Resilient Waveforms (Studio) (Shephard Media, 14 SEP Studio)**

   Amid modern warfare's complexity and electronic warfare threats, NATO and its allies are balancing legacy systems with new technologies. With the importance of resilient waveforms underscored, High Frequency (HF) technology has emerged as a robust solution, leading to an "HF renaissance".

Back to Table of Contents

Items of Interest

1. **US officials say Travis King, who crossed into North Korea, is in American custody (AP News, 27 SEP, Kim Tong-Hyung et al.)**

   Pvt. Travis King, the American soldier who crossed into North Korea two months ago, is in U.S. custody, two U.S. officials said 27SEP23.

   One official said King was transferred to American custody in China. The officials spoke on condition of anonymity to discuss King's status ahead of the announcement. Earlier, North Korea said it would expel King, 23. That announcement surprised some observers who had expected the North to drag out his detention in the hopes of squeezing concessions from Washington at a time of high tensions between the rivals.

   The North's official Korean Central News Agency reported 27SEP23, that authorities have finished their questioning of King. It said that he confessed to illegally entering the North because he harbored "ill feeling against inhuman maltreatment and racial discrimination" within the U.S. Army and was "disillusioned about the unequal U.S. society."

2. **NATO to publish first C-UAS doctrine this year (Janes, 26 SEP, Olivia Savage)**

   NATO will publish its first counter-unmanned aircraft systems (C-UASs) doctrine in 2023, which will lay the foundations for how militaries should standardize and operationalize countering UASs, Janes has learnt.

   Along with informing members how best to plan and execute C-UAS missions, the high-priority document will address and outline the strategic environment, Senior Advisor for NATO's Science for Peace and Security programme Claudio Palestini told Janes at NATO's 'C-UAS Technical Interoperability Exercise 2023' (TIE23) in Vredepeel, Netherlands, held from 12-22SEP23.

   Several strategic recommendations will be outlined in the doctrine, according to Palestini. These include advising member states that C-UAS must be integrated into the wider air-defense domain, rather than being 'considered in isolation'; that it should be a multidomain solution; and that continuous innovation and improvement must be adopted because of the rapidly evolving threat.

3. **Taiwan Finds 1 In 3 Spies Serving In Military (U.S. Army Asian Studies Detachment, 27 SEP, Taiwan News Online)**

   One out every three spies caught passing on confidential information to China did so while still serving in the military, Defense Minister Chiu Kuo-cheng said 26SEP23. The other two thirds of spy cases in the military involved retired officers, he told lawmakers. The defense chief insisted he would take a tougher approach, Radio Taiwan International (RTI) reported.

   Both Chiu and Justice Minister Tsai Ching-hsiang agreed that courts were reaching too lenient verdicts for national security violations. The latter said he believed that in such cases, prosecutors would still file appeals. Chiu warned that officers who had already retired and left the military should not expect any different treatment. If they were found to have violated the law, they would still have to face the consequence of their actions, the minister replied to questions at the Legislative Yuan.

   Democratic Progressive Party (DPP) Legislator Liu Shyh-fang said that in other countries, violators of national security laws would on average have to spend 19 years in prison, but in Taiwan sentences were much shorter. The difference meant that prison

Back to Table of Contents

terms failed to pose a deterrent and would not put a stop to more spying scandals, she said. The Ministry of Justice said it would intensify cooperation with the Ministry of National Defense (MND) and improve the training of prosecutors in national security issues.

4. Israeli companies showcase drones that take off, land vertically (C4ISR, 19 SEP, Elisabeth Gosselin-Malo)

Israeli defense companies made drone technology with a vertical-takeoff-and-landing capability a focus at this year's DSEI defense conference in London, unveiling two new systems with customers already secured.

This past year, the tube-launched Hero series of loitering munitions produced by German company Rheinmetall and its Israeli-based partner Uvision have seen great success in Europe, with sales announced to Italy and Hungary.

To solve this issue and provide customers with greater flexibility for launch sites, IAI developed the Rotem Alpha loitering munition, capable of hovering, taking off and landing vertically. Unveiled at DSEI, the system is equipped with a demonstrated anti-tank warhead and was designed based on lessons learned from Russia's war against Ukraine, according to the company representative.

5. US sanctions firms in China , Russia, Turkey over Iran's drone program (C4ISR, 19 SEP, Fatima Hussein)

The U.S. on 19SEP23, imposed sanctions on seven people and four companies in China, Russia, and Turkey who officials allege are connected with the development of Iran's drone program.

Back to Table of Contents

The U.S. accuses Iran of supplying Russia with drones used to bomb Ukrainian civilians as the Kremlin continues its invasion of Ukraine.

The latest development comes after Iran's President Ebrahim Raisi denied his country had sent drones to Russia for use in the war in Ukraine.

Among other things, the sanctions deny the people and firms access to any property or financial assets held in the U.S. and prevent U.S. companies and citizens from doing business with them.

6. North Korea's Leader Wraps Up Russia Trip With Drones Gift (AFP, 18 SEP, AOSP)

North Korean leader Kim Jong Un left Russia on 17SEP23 after a rare six-day visit that appeared to solidify his country's ties with President Vladimir Putin, fanning Western fears that Pyongyang could provide Moscow with weapons for its assault on Ukraine.

Kim's tour of Russia's Far East, which began on 12SEP23, has focused intensely on military cooperation, including a symbolic exchange of rifles with Putin and an inspection of state-of-the-art Russian weapons.

Before departing from Vladivostok, the Pacific port city just over the border, Kim was presented with five explosive drones, a reconnaissance drone, and a bulletproof vest as gifts from the governor of the Primorye region, which borders China and North Korea.

Government officials from the two countries also agreed to meet in Pyongyang in November, Kozlov added.

Russia-Ukraine

1. Russia-Ukraine Situation Report

Russia-Ukraine Situation Report, 29 September 2023
Russia-Ukraine Situation Report, 28 September 2023
Russia-Ukraine Situation Report, 26 September 2023
Russia-Ukraine Situation Report, 25 September 2023
Russia-Ukraine Situation Report, 22 September 2023
Russia-Ukraine Situation Report, 21 September 2023
Russia-Ukraine Situation Report, 20 September 2023
Russia-Ukraine Situation Report, 19 September 2023
Russia-Ukraine Situation Report, 15 September 2023

2. The Drive/The War Zone Ukraine Situation Report:

Ukraine Situation Report: U.K. Considers Returning To Training Troops In Ukraine – 30 SEP

Ukraine Situation Report: Russia Has Gained The Most Ground This Year – 28 SEP

Ukraine Situation Report: Pilots Train On Commercial F-16 Simulators At Home Bases – 27 SEP

Ukraine Situation Report: Black Sea Fleet Commander Reappears After Kyiv Declared Him Dead – 26 SEP

Ukraine Situation Report: Landmark Odesa Hotel Pummeled By Missile Barrage – 25 SEP

Ukraine Situation Report: Signs Small Number Of ATACMS May Soon Be On Way – 22 SEP

Ukraine Situation Report: Russia's Main Defensive Line Breached – 21 SEP

Ukraine Situation Report: Kyiv Unleashes New Wave Of Cruise Missiles On Crimea – 20 SEP

Ukraine Situation Report: M109 Paladins Are Proving Too Wily For Russian Gunners – 18 SEP

Ukraine Situation Report: Rumors Swirl Of New Attacks On Black Sea Fleet – 16 SEP

3. Ukraine Getting ATACMS Cluster Variant Would Be A Big Problem For Russia (The Drive/The Warzone, 27 SEP, Joseph Trevithick & Tyler Rogoway)

Cluster munition-laden ATACMSs would be able to take out aprons full of aircraft and key air defense batteries from nearly 200 miles away.

In the course of the discussions about what Army Tactical Missile System (ATACMS) ballistic missiles could offer Ukraine, much of the focus has been on variants of these weapons equipped with unitary (single high-explosive) warheads. However, versions loaded with cluster munitions could introduce a whole other set of dire complications to Russian forces.

ATACMS, a late Cold War-era American short-range ballistic missile, comes in two primary flavors. The first two variants of this missile were cluster munition dispensing models loaded with 950 and 275-300 submunitions and with maximum ranges of 165 kilometers (102 miles) and 300 kilometers (186 miles), respectively. The two missiles are known variously as the MGM-140A and B, the Block I and IA, and the M39 and M39A1.

4. **[The Russian weapons Ukrainian soldiers most fear, according to an expert] (Business Insider, 23 SEP, Tom Porter)**

Ukraine appears to have made an important breakthrough in its counteroffensive against Russia with reports suggesting it has breached Russia's defensive line with vehicles for the first time.

But it's far from clear if Ukraine will be able to exploit the breakthrough, and the battle remains in the balance.

5. **[Ukraine conflict: European countries approve new weapons donations] (Janes, 21 SEP, Nicholas Fiorenza)**

European countries announced new weapon donations to Ukraine in the lead up to or during the 15th meeting of the Ukraine Defense Contact Group at Ramstein Air Base, southwestern Germany, on 19 September.

In a press conference following the meeting, US Secretary of Defense Lloyd Austin, who chairs the Ukraine Defense Contact Group, noted announcements by Germany on 18 September of a package with ammunition, mine-clearing equipment, and "other critical capabilities"; by Denmark of an USD833 million package including ammunition and armour capabilities; and by Sweden in August of a USD300 million military aid package consisting of ammunition and spare parts. He also reported that Poland told the Ukraine Defense Contact Group meeting that it had provided Ukraine with additional mine-clearing equipment and over 100 armoured personnel carriers and tens of thousands of munitions.

Back to Table of Contents

6. **[Poland is done sending arms to Ukraine, as trade dispute escalates] (Defense News, 21 SEP, Vera Gera, AP)**

Poland's prime minister said his country is no longer sending arms to Ukraine, a comment that appeared aimed at pressuring Kyiv and put Poland's status as a major source of military equipment in doubt as a trade dispute between the neighboring states escalates.

Prime Minister Mateusz Morawiecki said in an interview late on 20SEP23, that Poland is no longer transferring weapons to Ukraine. He made the comment as his populist party faces pressure from a far-right party in a national election on Oct. 15. The far-right party, Confederation, says Poland is not getting the gratitude it deserves for arming Ukraine and accepting its refugees.

The prime minister then spoke of a military modernization plan underway, spurred by fears of Russian aggression in the region.

A government spokesman, Piotr Mueller, appeared to confirm 21SEP23, that Warsaw would not agree to more military aid. He said the country was now only providing supplies of ammunition and armaments that had previously been agreed to, noting that "a series of absolutely unacceptable statements and diplomatic gestures appeared on the Ukrainian side."

7. **[US charges Russian man with smuggling microelectronics amid Ukraine war] (C4ISR, 19 SEP, Colin Demarest)**

Authorities arrested a man living in Hong Kong accused of deceiving U.S. companies and shuttling sensitive microelectronics into Russia amid its bloody invasion of neighboring Ukraine.

Maxim Marchenko, originally from Russia, was arrested outside the U.S. this week and extradited to Westchester County, New York, documents filed in federal court show. He's

facing several charges, including alleged conspiracy to defraud the U.S., conspiracy to commit wire fraud and the smuggling of goods.

The dual-use technologies Marchenko is accused of surreptitiously middle-manning for Russia — namely OLED micro-displays from a company based in Dutchess County, New York — can be used for medical imaging and rifle scopes, video games and night-vision goggles, according to the U.S. Department of Justice.

Russian military hardware, including drones, radios and electronic warfare devices, are reliant upon Western-sourced components, the court documents note. To access them, especially now, as export controls tighten, "Russia relies on third-party transshipment hubs and clandestine procurement and payment networks," they continue.

8. Russia's Tiny Drones Are Now Flying Far Enough To Blow Up Ukrainian MiGs At Their Bases (Forbes, 19 SEP, David Axe)

An explosives-laden Russian drone struck and damaged an air force Mikoyan MiG-29 fighter on the tarmac at Dolgintsevo air base near Kryvyi Rih on or before 19SEP23. Despite claims to the contrary from some observers, there's little reason to believe footage of the attack is fake.

The Russian Lancet is among the most numerous, and most effective, of these explosive drones. But until now, a baseline "Product 51" Lancet—weighing just 25 pounds—could range only as far as 25 miles. But the Kremlin has been developing longer-range Lancets and isn't shy about it. Russian propagandists back in August 2023 touted a new "Product 53" Lancet with a nearly 45-mile range. Sputnik described Product 53 as "the next step in the evolution of the Lancet—and one which, designers hope, will become nearly impossible to stop."

Back to Table of Contents

A Lancet ranging 45 miles can threaten not just the MiGs at Dolgintsevo, but also any Ukrainian warplanes using the reserve base at Voznesensk in Mykolaiv Oblast. To mitigate the threat, Ukrainian air force planners could move the jets to more northern bases, boost air-defense coverage over vulnerable facilities or put parked jets under shelters—or do all three.

9. Ukraine fires 6 deputy defense ministers as counteroffensive continues (Defense News, 18 SEP, Illia Novikov, AP)

Six Ukrainian deputy defense ministers were fired 18SEP23 following the dismissal two weeks prior of Defense Minister Oleksii Reznikov in a corruption scandal, officials said, as heavy fighting continued in the east.

Deputy defense ministers including Hanna Maliar, Vitalii Deyneha and Denys Sharapov, as well as the state secretary of the Ministry of Defense, Kostiantyn Vashchenko, were fired, according to the Telegram account of Taras Melnychuk, permanent representative of the Cabinet of Ministers.

Melnychuk provided no explanation of the firings, but the government has been investigating accusations of corruption in the military related to purchasing equipment. Rustem Umerov, a Crimean Tatar lawmaker who took over as defense minister, did not immediately issue a statement.

10. With A Special Warhead Blew Up That Russian Submarine From The Inside (Forbes, 18 SEP, David Axe)

The Ukrainian Storm Shadow cruise missile that knocked out the Russian Black Sea Fleet's submarine Rostov-on-Don in a nighttime raid on the fleet's anchorage in Sevastopol, in occupied Crimea on 13SEP23, didn't just damage the Kilo-class boat in its drydock—it blew it up from the inside.

Photos depicting the submarine's wreckage that appeared online on 18SEP23 tell a clear story. The outward-curling metal at the Storm Shadow's impact point, amidships on the 240-foot, 3,100-ton Rostov-on-Don, indicates the missile punched through the nine-year-old vessel's hull before exploding.

This was by design. British firm BAE Systems specifically developed the Storm Shadow's 880-pound Bomb Royal Ordnance Augmented Charge warhead for destroying hardened targets such as underground bunkers. But the two-warhead, "tandem" fit obviously works equally well against ships.

11. South Korean Breaching Vehicles Will Help Ukraine Replace Its Counteroffensive Losses (Forbes, 18 SEP, David Axe)

In a single cataclysmic assault across an impossibly dense Russian minefield in southern Ukraine's Zaporizhzhia Oblast in early June 2023, the Ukrainian army's 47th Mechanized Brigade abandoned three of its rare, ex-Finnish Leopard 2R breaching vehicles alongside a couple of dozen other armored vehicles.

Fortunately for Ukraine, South Korean firm Hyundai produces a similar breaching vehicle: the K600. And Seoul just pledged two of the 62-ton vehicles to Kyiv. South Korea will deliver the K600s "as soon as possible," a government source told Chosun.

Hyundai makes a two-person K600 by removing the turret from a K1 tank—a South Korean variant of the American M-1—and adding a plow, an articulated excavator arm and a device for safely triggering magnetic mines.

Back to Table of Contents