U.S. ARMY

Cyber Center of Excellence

Unclassified Threat Read Book

01-15 October 2023

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

Table of Contents

6. Army combat advisors testing military version of Elon Musk's Starlink – 09 OCT
7. LightSpy iPhone Spyware Linked to Chinese APT41 Group – 04 OCT 23
8. Data theft is now the biggest worry for IT admins – 02 OCT

Items of Interest

1. Israel-Gaza Situation Report
2. The Drive Israel-Gaza Update
3. Hybrid war comes to the Middle East. Cyberespionage. New DDoS techniques. Magecart innovation. – 14 OCT

Russia-Ukraine Situation

1. Russia-Ukraine Situation Report
2. The Drive/The Warzone Ukraine Situation Report
3. Germany to send Ukraine $1B in air defense tech, plus more tanks – 11 OCT
4. Ukraine conflict: Ukraine destroys key Russian EW system – 11 OCT

Cyber

1. **Israel-Hamas conflict to heighten cyber espionage and disruptive cyber threats (Control Risks, 13 OCT, Joseph Buckley & Stina Connor)**

   On 7 October 2023, the Palestinian militant group Hamas launched a surprise, multi-pronged terrorist attack by land, air and sea against military and civilian locations in the southern district of Israel. The Israel Defense Forces (IDF) have largely re-established control over southern Lebanon and prepares for an Israeli invasion of Gaza. These attacks have been accompanied by a series of disruptive cyber attacks from cyber activist groups targeting organisations in Israel and those perceived as pro-Israel in other countries. Cyber operations motivated by the conflict are likely to present a growing threat to organisations in the region, and potentially globally, as the conflict progresses.

2. **Israel-Palestine tussle could spill over to cyberspace (The Hindu Business Line, 13 OCT, K V Kurmanath)**

   The ongoing conflict in West Asia could well spill over to the cyber space, and India may be a target for hacktivists from across the border, according to cybersecurity and intelligence provider CloudSEK.

   “Our contextual artificial intelligence digital risk platform XVigil has discovered multiple hacktivist groups planning cyber attacks on India due to their extended support towards Israel amid war-torn situations in West Asia,” said a CloudSEK report.

   It cautioned that the cyber attacks on India are to be conducted under their hacktivist campaign, #OpsIsrael #OpIsraelV2. “The motivations behind these attacks primarily revolve around political factors, most of which are retaliatory actions in the ongoing hacktivist warfare between countries,” it said.

3. **North Korea's State-Sponsored APTs Organize & Align (Dark Reading, 10 OCT, Elizabeth Montalbano)**

   An unprecedented collaboration by various APTs within the DPKR makes them harder to track, setting the stage for aggressive, complex cyberattacks that demand strategic response efforts, Mandiant warns.

   North Korean advanced persistent threat (APT) groups have become aligned in an unprecedented way since the start of the COVID-19 pandemic, evolving in terms of adaptability and complexity, and allowing for individual threat groups to diversify and expand activities — all while making it more difficult for investigators to keep up.

4. **Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks (Security Week, 09 OCT, Eduard Kovacs)**

   Several hacker groups have joined in on the Israel-Hamas conflict escalation that started after the Palestinian militant group launched a major attack.

   Hamas launched an unprecedented attack on Israel out of Gaza, firing thousands of rockets and sending its fighters to the southern part of the country. In response, Israel declared war on Hamas and started to retaliate.

   In addition to the state-sponsored actors that have likely ramped up their cyber efforts behind the scenes, known hacktivist groups supporting both sides have intensified their cyberattacks.

   According to a timeline created by cybersecurity consultant and OSINT enthusiast Julian

Botham, the first hacktivist attacks were launched against Israel by Anonymous Sudan less than one hour after the first rockets were fired by Hamas. The group targeted emergency warning systems, claiming to have taken down alerting applications in Israel.

5. **9th October – Threat Intelligence Report – 09 OCT (Check Point Research, 09 OCT)**

   For the latest discoveries in cyber research for the week of 9th October, please download our Threat_Intelligence Bulletin.

6. **GenAI Is A Hit With Hackers. Here's Why It Will 'Benefit The Defense' Even More. (CRN, 06 OCT, Kyle Alspach)**

   While ChatGPT has made life easier for attackers, over the longer term it's likely that generative AI 'will benefit the defense more than it will the offense,' a top cyberthreat expert tells CRN.

   While threat actors are getting a boost from ChatGPT and other generative AI tools, many cybersecurity experts see a potential for cyber defense teams to see a greater benefit from GenAI over the longer term — thanks to an abundance of promising uses for the technology that are expected to emerge over time.

7. **Espionage fuels global cyberattacks (Microsoft, 05 OCT, Tom Burt)**

   In the past year, cyberattacks have touched 120 countries, fueled by government-sponsored spying and with influence operations (IO) also rising. At times, nearly half of these attacks targeted NATO member states, and more than 40% were leveled against government or private-sector organizations involved in building and maintaining critical infrastructure. While headline-grabbing attacks from the past year were often focused on destruction or financial gain with ransomware, data shows the predominant motivation has swung back to a desire to steal information, covertly monitor communication, or to manipulate what people read.

Back to Table of Contents

8. **Sony Confirms Data Stolen in Two Recent Hacker Attacks (Security Week, 05 OCT, Eduard Kovacs)**

   Sony shared information on the impact of two recent unrelated hacker attacks believed to have been carried out by a couple of known cybercrime groups in the beginning of October 2023.

   One of the incidents is related to the investigation launched recently by Sony after a relatively new ransomware group named RansomedVC claimed to have compromised the company's systems and offered to sell stolen data.

   The screenshots the hackers initially made public to demonstrate their claims seemed to show that they obtained source code, access to Sony applications, and confidential documents. However, most of the content appeared related to Sony's Creators Cloud media production solution, suggesting that their claims were exaggerated.

   In an updated statement, Sony told SecurityWeek that it has been investigating the claims with the help of third-party forensics experts and identified unauthorized activity on a single server located in Japan. The hacked server has been used for internal testing for the company's Entertainment, Technology and Services (ET&S) business.

9. **US Executives Targeted in Phishing Attacks Exploiting Flaw in Indeed Job Platform (Security Week, 03 OCT, Ionut Arghire)**

   A recent phishing campaign targeting executives in senior roles has been exploiting an

open redirection vulnerability in the Indeed website, cybersecurity firm Menlo Security warns.

Headquartered in the US, Indeed is a popular worldwide job search platform, which claims to have more than 350 million unique visitors each month, and more than 14,000 employees globally.

Given its high popularity, the platform is seen as a trusted source by phishing prevention products, and the newly identified phishing campaign shows how threat actors can abuse that trust.

According to Menlo Security, starting July 2023, adversaries have been observed exploiting an open redirection flaw in the indeed.com website to take victims to a phishing page designed to steal their Microsoft credentials.

10. NATO investigating breach, leak of internal documents (Cyber Scoop, 03 OCT, AJ Vicens)

NATO is investigating claims by a politically motivated hacktivist group that it breached the defense alliance's computer systems, which, if confirmed, would mark the second time in the last three months that the group known as SiegedSec has broken into NATO systems.

SiegedSec, a cybercrime group with a history of politically-motived attacks, claimed on its Telegram channel on Saturday that it had stolen roughly 3,000 NATO documents and posted six screenshots allegedly showing access to various NATO web pages. The group claimed the 3,000 stolen files total more than nine gigabytes of data.

According to SiegedSec's message 30SEP23, files from the attack come from the Joint Advanced Distributed Learning platform, the NATO Lessons Learned Portal, the Logistics Network Portal, the Communities of Interest Cooperation Portal and the NATO Standardization Office. CyberScoop was not able to independently confirm the authenticity of the files but is reporting on SiegedSec's claim given its track record of purported attacks against NATO.

Back to Table of Contents

11. 2nd October – Threat Intelligence Report (Check Point Research, 02 OCT)

For the latest discoveries in cyber research for the week of 2nd October, please download our Threat Intelligence Bulletin

.

Electronic Warfare

1. **[US Army to build electronic warfare training ground at Fort Gordon] (Defense News, 13 OCT, Colin Demarest)**

   An electronic-warfare testing range is slated for construction at Fort Gordon in Georgia, a development U.S. Army officials said will greatly bolster troop readiness.

   The plans come as the service, the military's largest, reinvests in electronic warfare and electromagnetic mastery after years of neglect. The renewed interest is spurred by threats posed by Russia and China after years spent in the Middle East

   Maj. Gen. Paul Stanton, Fort Gordon's commanding officer, on Oct. 11 said the facilities will be a place where soldiers can get familiar with their jamming and sensing gear in realistic settings.

4. **[US Army considering aerostat overhaul as focus turns to Russia, China] (Defense News, 12 OCT, Colin Demarest)**

   The U.S. Army is examining how it can reinvigorate its aging fleet of blimp-like aircraft known as aerostats that serve as elevated surveillance and communication platforms.

   The service is interested in the updates amid a focus on countering the Russian and Chinese militaries, forces more sophisticated than those fought for decades in the Middle East.

2. **[US Army's test of Lockheed jammer highlights payload adaptability] (C4ISR Net, 11 OCT, Colin Demarest)**

   An aerial electronic jammer the U.S. Army slated for use aboard a reconnaissance and attack drone successfully underwent testing using a turboprop aircraft, an outcome officials said demonstrates the payload's future battlefield flexibility.

   The Multi-Function Electronic Warfare-Air Large, or MFEW-AL, is part of the Army's focus on sophisticated electronic warfare technologies after years of divestment. Lockheed Martin is handling development of the self-contained pod, which was initially meant to be slung beneath an MQ-1C Gray Eagle drone, made by General Atomics.

3. **[How the war in Ukraine is reshaping US Army modernization] (Next Gov, 11 OCT, Lauren C. Williams)**

   Electronic warfare's role in Russia's war on Ukraine has pushed the U.S. Army to tweak its modernization plans to keep pace with the ongoing threats, the leader of Army Futures Command said Monday.

   "We've got a moral responsibility to learn from this horrific war—to include the one they just started 72 hours ago—and I take that very seriously," Gen. James Rainey told reporters at the annual Association of the U.S. Army conference in Washington, D.C. "I haven't seen anything that tells me our current modernization efforts are off track," he said, adding that technological disruption seen in Ukraine has been unprecedented in speed and scale—with EW being a prime example.

5. **[Russia's electronic warriors are switching to 'much more subtle' operations around the frontlines in Ukraine] (Business Insider, 08 Oct, Stavros Atlamazoglou)**

   When Russia invaded Ukraine in February 2022, it hoped for a quick campaign. After

nearly 300,000 casualties and many humiliating defeats, the Russian military is still struggling to adjust to Ukraine's willingness and ability to fight.

Equipped with Western weapons, the Ukrainian military is now pushing hard in a counteroffensive it launched in the southern and eastern part of the country in June.

But while everyone is paying attention to the rumble of tanks and the buzz of drones, electronic-warfare troops on both sides are taking on more subtle and often risky operations around the frontlines.

6. **BREAKING NEWS: Ukraine troops destroy Russian Borisoglebsk-2 high value electronic warfare system (Army Recognition, 07 OCT)**

In a recent video released on October 3, 2023, by the Artillery and Missile troops of the Armed Forces of Ukraine via their official Facebook account, it has been revealed that the Ukrainian Armed Forces successfully targeted and destroyed a pivotal Russian RB-301B Borisoglebsk-2 electronic warfare system in the vicinity of Novopetrykivka, Donetsk region. Recognized as the cornerstone of electronic warfare within the Russian Army, the Borisoglebsk-2 boasts the capability to orchestrate four distinct jamming units from a singular command point.

7. **Space Force Conducts Its Biggest Electronic Warfare Exercise Ever (Air and Space Forces, 06 OCT, Unshin Lee Harpley)**

The Space Force wrapped up its largest-ever exercise focused on electromagnetic warfare, Black Skies 23-3, on Sept. 23, with more than 170 participants.

Back to Table of Contents

Introduced last year, Black Skies is an electronic warfare-focused evolution of the Space Flag exercises. Organized by Space Training and Readiness Command, it prepares participants to safeguard critical parts of the electromagnetic spectrum, such as those that can disrupt GPS and communication signals. The exercise also allows tactical units to grasp the complexities between operational planning and tasks.

8. **Electronic warfare training is headed to an Army school near you (C4ISR Net, 06 OCT, Todd South)**

Future Army ground unit commanders will have nearly instant, possibly deadly, feedback on whether they followed the right steps or if they revealed themselves on the electronic battlefield.

That’s the message the commandant of the Army’s Cyber School has for current and incoming maneuver unit leaders.

“If you remember nothing else, remember 8 minutes,” said Brig. Gen. Brian Vile at the recent Maneuver Warfighter Conference at Fort Moore, Georgia.

“What is 8 minutes? After you break squelch on your radio, you’re going to learn two things in 8 minutes — how good was your [emission control] and how good are your adversary’s [electromagnetic warfare] soldiers.”

Information Advantage

1. **X's Misinformation Problem Is Getting Worse (Forbes, 14 OCT, Peter Suciu)**

   Tech entrepreneur Elon Musk has touted how X—the platform formally known as Twitter—could replace traditional media with near real-time updates as news is breaking. Yet, in the past week, X has instead been largely overtaken by misinformation coming out of the Middle East.

   Since the start of the heaviest fighting seen in the region in nearly a decade, there has been a constant flow of fake photos, old videos, and in some cases even video game footage presented as coming from the region.

2. **Misinformation about the Israel-Hamas war is flooding social media. Here are the facts (AP News, 13 OCT)**

   In the days since Hamas militants stormed into Israel early Oct. 7, a flood of videos and photos purporting to show the conflict have filled social media, making it difficult for onlookers from around the world to sort fact from fiction.

   While plenty of real imagery and accounts of the ensuing carnage have emerged, they have been intermingled with users pushing false claims and misrepresenting videos from other events.

   Among the fabrications, users have shared false claims that a top Israeli commander had been kidnapped, circulated a doctored White House memo purporting to show President Joe Biden announcing billions in aid for Israel, and pushed old and unrelated videos of Russian President Vladimir Putin with inaccurate English captions.

3. **Hamas Network Spreads Dangerous Disinformation (FDD, 13 OCT)**

   The social threat intelligence company Cyabra said Hamas and its supporters are successfully spreading propaganda and disinformation online, The Jerusalem Post reported on October 12. The content is reaching as many as 500 million people on X (formerly Twitter), according to the company. With social media awash with fake videos and disinformation simultaneously glorifying and downplaying Hamas' brutality, Rafi Mendelsohn, Cyabra's vice president of marketing, concluded that Hamas and its supporters are demonstrating "a level of coordination [online] that goes beyond that of a terrorist group — it's more akin to a state level of organization."

4. **Social Media Platforms Were Not Ready for Hamas Misinformation (CSIC, 12 OCT, Caitlin Chin-Rothmann)**

   Millions of internet users flocked to X (formerly known as Twitter), Facebook, Instagram, and TikTok on October 7 to monitor real-time developments related to Hamas's attack on Israel. What they found—especially on X—looked noticeably different compared to previous global crises. One video, which claimed to depict a Hamas soldier shooting down an Israeli helicopter, was borrowed from the video game Arma 3. A second viral clip, which alleged to portray Israeli airstrikes in Gaza, more likely displayed a firework show following a soccer match in Algeria. Numerous accounts—some with pseudonyms, others posing as fake news agencies—misrepresented imagery from past months or inaccurate geographic locations as current portrayals of the violence in either Israel or Gaza. Falsified reports of U.S. policy actions—evacuating the U.S. embassy in Lebanon, allocating $8 billion to aid Israel's defense—circulated as well.

5. **[China's State Media Accused of Spreading Anti-Israel Disinformation] (Newsweek, 11 OCT, Micah McCartney)**

As Israeli strikes in the Gaza Strip continue after the attacks and kidnappings carried out by Hamas militants over the weekend, Chinese state-run media has spread the unverified rumor that Israeli forces are using white phosphorus bombs against civilians in a manner that contravenes international law.

More than 1,600 combined Israelis and Palestinians have reportedly been killed since Hamas launched attacks on Saturday, according to the Associated Press, and hundreds of others have been injured. Israel has been conducting airstrikes on the sealed-off and densely populated Gaza Strip after the deadliest Palestinian militant attack in its history. Hamas, which is funded and armed by Iran, is sworn to Israel's destruction.

6. **[Advancing AI governance in Japan] (Microsoft, 05 OCT, Brad Smith)**

"Don't ask what computers can do, ask what they should do."

That is the title of the chapter on AI and ethics in a book I coauthored with Carol Ann Browne in 2019. At the time, we wrote that "this may be one of the defining questions of our generation." Four years later, the question has seized center stage not just in the world's capitals, but around many dinner tables.

As people use or hear about the power of OpenAI's GPT-4 foundation model, they are often surprised or even astounded. Many are enthused or even excited. Some are concerned or even frightened. What has become clear to almost everyone is something we noted four years ago – we are the first generation in the history of humanity to create machines that can make decisions that previously could only be made by people.

Back to Table of Contents

7. **[US sending seized Iranian munitions to Ukraine] (Defense News, 04 OCT, Noah Robertson)**

More than one million Iranian rounds of munitions that were seized by the U.S. military late last year have been sent to Ukraine to assist the effort repel Russia's invasion, Central Command said.

The seizure occurred as Iran was sending weapons to Houthi rebels in Yemen. In July, the U.S. Department of Justice filed a motion to forfeit thousands of rifles, hundreds of machine guns and rocket launchers and around 700,000 rounds of ammunition that the U.S. intercepted from Iran on the same path. The motion allowed the U.S. to take control of the munitions now being sent to Ukraine, which had previously been stored in U.S. facilities around the Middle East.

The 1.1 million 7.62 mm rounds being sent to the Ukrainian military were seized by "Central Command naval forces from the transiting stateless dhow MARWAN" in December, it said. According to a Department of Defense fact sheet, the U.S. has sent Ukraine "more than 300,000,000 rounds of small arms ammunition and grenades" to date.

Signal

1. **To tackle cyberattacks, how about organisations adopting 'Zero Trust' policy? (Gulf News, 15 OCT, Mohamed Amin)**

   If trust is the true currency in today's competitive business environment, then 'Zero Trust' is the ultimate measure of an organization's cyber resilience posture.

   In an era dominated by rapidly evolving digital landscapes and relentless cyber threats, the need for a robust Zero Trust cybersecurity strategy has never been more critical. According to the World Economic Forum's Global Risk Report 2023, widespread cybercrime and cyber insecurity feature among the Top 10 risks facing economies within the next 10 years.

   For most businesses today, navigating security is like trying to make your way through a high-stakes labyrinth with many different, complicated passageways that make it hard to reach the destination. Zero Trust can help ease this journey.

2. **SpaceX's Starlink To Launch Satellite-Based SMS Services in 2024 (Hypebeast, 14 OCT, Arthur Parkhouse)**

   SpaceX's Starlink has revealed plans to launch a satellite-based SMS service, Direct-to-Cell, in 2024, as shown via its recent promotional website.

   Testing for the services, in partnership with T-Mobile, was first revealed earlier this year and while its 2024 launch is highly anticipated, it will be limited to SMS service, with voice, data and IoT features not expected to be added until 2025.

   Once it reaches its final form, Direct-to-Cell aims to offer an all-encompassing connectivity solution for texting, calling, and internet browsing across diverse terrains — enabling "ubiquitous access to texting, calling and browsing wherever you may be on land, lakes, or coastal waters," according to the site.

3. **Upcoming Air Force demos aim to connect commercial satcom with military platforms (Defense Scoop, 12 OCT, Mikayla Easley)**

   The Air Force Research Laboratory will conduct a set of demonstrations over the next few years that will seek to provide air- and ground-based military systems with ubiquitous connectivity using commercial satellite constellations.

   The demonstrations are part of AFRL's Defense Experimentation Using Commercial Space Internet (DEUSCI) program, which aims to leverage burgeoning commercial space internet services in order to establish resilient communications and data-sharing capabilities for warfighters. A notice on Sam.gov states the end goal is to establish "path agnostic communications" — or the ability to "reliably communicate to any location on the globe without explicitly specifying which nodes of a communication network to use."

   The program's mission ties directly into the Pentagon's vision for its new warfighting concept known as Joint All Domain Command and Control (JADC2). The effort seeks to connect systems that are currently siloed across the battlespace under a single network, enabling warfighters to quickly send and receive critical decision-making data.

4. **DRS RADA Technologies develops X-band radar sensor for US Army operations (Janes, 11 OCT, Michael Fabey)**

   DRS RADA Technologies has developed a wide-band, X-band radar sensor called the nMHR (Next-generation Multi-Mission Hemispheric Radar) for highly mobile ground-based air-defence operations, Charlene Caputo, Business Development vice-president,

told Janes.

"Traditionally DRS radars have operated in the S-band as this band offers an excellent balance of range and accuracy," Caputo told Janes on 5 October during a briefing in advance of the Association of the United States Army (AUSA) 2023 symposium, which started on 9 October in Washington, DC.

"However, this band is being considered for worldwide re-allocation to commercial communications in support of 5G networks," she said.

"DRS is proactively developing radars in diverse spectrums to mitigate the impact to training and operations, with our X-band radar being the first release," she said. "These newer radars will share the same characteristic of being software-defined, 4D active electronically scanned array (AESA) radars that can support a variety of operational missions."

5. **Ukraine rolls out secure radio to counter Russian electronic warfare (Euromaidan Press, 10 OCT, Iryna Voichuk)**

The HIMERA radio utilizes advanced Frequency Hopping Spread Spectrum (FHSS) technology to counter Russia's electronic warfare tactics effectively, creating a nearly undetectable communication system.

Ukraine's digital transformation minister Mykhailo Fedorov announced that Ukrainian developers have created a radio called Himera that can operate despite Russian electronic warfare jamming.

According to Fedorov, this "unique technology" can work despite Russian electronic warfare systems. The Russians cannot block or decrypt its signals. The radio can hold a charge for up to four days.

6. **Army combat advisors testing military version of Elon Musk's Starlink (Task & Purpose, 09 OCT, Jeff Schogol)**

The 5th Security Force Assistance Brigade, or SFAB, is experimenting with Starshield, the military version of Starlink communications network made by SpaceX, said Col. Brandon Teague, commander of 5th SFAB.

"We've done some testing with it at home station, and all of our systems worked flawlessly over the backbones that it provides," Teague told reporters on Monday.

SFABs are specialized units in which soldiers from the conventional forces train, advise, and assist foreign partners' conventional military forces. Unlike Special Forces, soldiers in SFABs do not train foreign special operations forces, nor do they conduct unconventional warfare and other special operations missions.

The 5th SFAB is focused on the Indo-Pacific region and it has a persistent presence in the Philippines, Thailand, Mongolia, Malaysia, and Indonesia, Teague said during the Association of the United States Army's annual conference in Washington, D.C.

7. **LightSpy iPhone Spyware Linked to Chinese APT41 Group (Info Security, 04 OCT, Kevin Poireault)**

Banking security firm ThreatFabric has found evidence that LightSpy, an iPhone spyware discovered in 2020, is more sophisticated than previously reported and could be linked to the infamous Chinese-sponsored threat group APT41.
During the investigation, ThreatFabric researchers discovered new features in the LightSpy malware. The spyware was first used in a watering hole attack against iOS users in Hong Kong in January 2020.

8. **[Data theft is now the biggest worry for IT admins](#) (Tech Radar, 02 OCT, Sead Fadilpašić)**

Forget about ransomware - data theft is the biggest concern these days.

For IT decision-makers, ransomware is no longer their number one concern - data theft is.

A survey from Integrity 360 found more than half (55%) saw data theft as their number one concern, followed by phishing (35%). Ransomware “only” came in third, with 29% saying they were most worried about this type of cybercrime.

8.

Back to Table of Contents

Items of Interest

1. Israel-Gaza Situation Report (Janes)

Israel–Gaza Situation Report, 12 October 2023
Israel–Gaza Situation Report, 10 October 2023

2. The Drive Israel-Gaza Update

Tit For Tat Escalation On The Israeli-Lebanese Border (Updated) – 15 OCT
The Perilous Tactical Realities Israel Will Face Fighting In Gaza – 13 OCT
Israel Poised To Attack After Warning To Immediately Evacuate Half Of Gaza – 13 OCT
Israel Strikes Syrian Airports, Hamas Calls For Armed West Bank Confrontations (Updated) – 12 OCT
This Is Heabollah's Arsenal Of Weapons It Could Rain on Israel – 12 OCT
Clashes With Hamas Are Still Occurring Inside Israel – 11 OCT
False Alarm Over Aerial Infiltration In Northern Israel Amid Hezbollah Fears – 11 OCT
Gaza Neighborhood Turned To Rubble, Rockets Rain On Tel Aviv (Updated) – 10 OCT
Israel Vows Gaza Siege, Hamas To Air Live Hostage Executions (Updated) – 09 OCT
Israel Strikes Inside Lebanon After Ground Incursion (Updated) – 09 OCT
Hamas Launches Unprecedented Surprise Attack On Israel – 07 OCT

Back to Table of Contents

3. Hybrid war comes to the Middle East. Cyberespionage. New DDoS techniques. Magecart innovation. (The Cyberwire, 14 OCT, CyberWire Staff)

At a glance.

- Disinformation in the war between Hamas and Israel.
- Hacktivism and state action in Hamas's campaign against Israel.
- International hacktivists join the cyber conflict.
- Novel DDoS attack: Rapid Reset.
- The current state of DPRK cyber operations.
- Storm-0062 exploits Atlassian 0-day.
- Grayling cyberespionage group active against Taiwan.
- Magecart campaign abuses 404 pages.
- CISA releases two new resources against ransomware.

Russia-Ukraine

1. **Russia-Ukraine Situation Report** (U.S. Army Asian Studies Detachment)

   Russia-Ukraine Situation Report, 12 October 2023
   Russia-Ukraine Situation Report, 11 October 2023
   Russia-Ukraine Situation Report, 04 October 2023
   Russia-Ukraine Situation Report, 03 October 2023

2. **The Drive/The Warzone Ukraine Situation Report:**

   Ukraine Situation Report: 'FrankenSAM' To Speed Delivery Of Air Defenses – 13 OCT
   Ukraine Situation Report: Signs Russia's Attempt To Encircle Avdiivka Is Stalling – 12 OCT
   Ukraine Situation Report: Kyiv Braced For Unprecedented Winter Drone War – 09 OCT
   Ukraine Situation Report: Are Kyiv's Special Operators Fighting Wagner In Africa? -06 OCT
   Ukraine Situation Report: Over 1M Seized Iranian Rounds Given To Kyiv – 04 OCT
   Ukraine Situation Report: Prigozhin's Son Has Eye On Wagner Reboot – 03 OCT
   Ukraine Situation Report: Long-Range Drones Now Targeting Sochi – 02 OCT
   Ukraine Situation Report: U.K. Considers Returning To Training Troops In Ukraine – 30 SEP

Back to Table of Contents

3. **Germany to send Ukraine $1B in air defense tech, plus more tanks (Defense News, 11 OCT, Rudy Ruitenberg)**

   Germany will send about €1 billion (U.S. $1.1 billion) worth of air defense systems to Ukraine as part of a second "winter package" for the embattled country, the German Defence Ministry said in a statement Tuesday.

   The support will include a Patriot air defense system and two IRIS-T surface-to-air systems, as well as 10 more Leopard 1 A5 main battle tanks, three Gepard anti-aircraft guns, armored trucks, and ambulances, in addition to more than €20 million in kit specifically for Ukraine's special forces.

   The latest support follows a €400 million package for Ukraine announced in September that included ammunition, mine-resistant combat vehicles and drones. After initial reluctance to provide Ukraine with military aid following Russia's invasion of the country, Germany has now overtaken the U.K. and Poland in terms of support, with only the U.S. providing more equipment.

4. **Ukraine conflict: Ukraine destroys key Russian EW system (Janes, 11 OCT, Olivia Savage & William Jardim)**

   A Russian R-330ZH Zhitel Automated Jamming Station has been destroyed in the Zaporizhzhia region in Ukraine.

   According to an announcement on 09OCT23 by the Special Operations Forces (SOF) of the Armed Forces of Ukraine, the attack was "completed by artillerymen" and supported by its SOF units.

   R-330ZH is a key component of Russia's electronic warfare (EW) arsenal, used to disrupt the communication command links between unmanned aerial vehicles (UAVs) and their operators. Specifically, it interferes with Inmarsat and Iridium satellite communication systems as well as the NAVSTAR (Global Positioning System [GPS]) radio navigation

system and the cellular communication solution (GSM-1800). It can also detect, analyze, and direction-find satellite- and cellular-based communication devices.

Back to Table of Contents