Cyber Center of Excellence

Unclassified Threat Read Book

16-31 March 2023

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

POC: Threat Management Office, jeffrey.t.hardimon.civ@army.mil or
kevin.m.bird.civ@army.mil 706-849-9259

Table of Content

Cyber

Electronic Warfare

Information Advantage

Signal

1. Space Force seeking more narrowband communication satellites – 31 MAR
2. Govt launches ‘quantum communication’ network with a dare: Rs 10L for ethical hackers who can break encryption – 27 MAR
3. Passwords vs Passwordless: A Debate on Online Security – 27 MAR
4. Why Zero Trust Is Necessary In The Fight Against Ransomware – 23 MAR
5. Elon Musk's Starlink is aiding criminal mining efforts in Brazil's Amazon – 17 M
6. US Army consolidates network modernization efforts into single office – 17 MAR
7. DoD seeking seamless military-commercial satellite communications – 16 MAR
8. No, AI did not break post-quantum cryptography – 16 MAR
9. NSA Shares Guidance on Maturing ICAM Capabilities for Zero Trust – 15 MAR

Items of Interest

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. Foreign Reflections on U.S. Exercises and Operations, 30 March 2023 – 30 MAR
4. Foreign Reflections on U.S. Exercises and Operations, 27 March 2023 – 30 MAR
5. Balloon Intercepted By U.S. Air Force Over Texas – 25 MAR
6. Russia Removing T-54 Tanks from 1295th Central Tank Repair and Storage Base – 22 MAR
7. Russia’s most elite troops use Soviet-era paper maps – 21 MAR
8. Former US Marine may have been 'lured' from China before arrest, lawyer says – 20 MAR
9. China's Xi arrives in Russia to meet Putin over Ukraine war – 20 MAR
10. What Vladimir Putin was doing on his first trip to Mariupol since its annexation – 19 MAR
11. Russian defense minister decorates pilots for downing U.S. drone – 17 MAR
12. Foreign Reflections on U.S. Exercises and Operations - 16 MAR
13. Wagner’s convicts tell of horrors of Ukraine war and loyalty to their leader – 16 MAR
14. US Army chief wants three multidomain task force units in the Pacific – 15 MAR

Cyber

1. **Hackers probing contractors for path to Pentagon, DISA chief says (Federal Times, 30 MAR, Colin Demarest)**

   Foreign hackers are targeting contractors to the U.S. government not only for their intellectual property and non-public information, but also to find furtive avenues into Pentagon networks, according to the director of the Defense Information Systems Agency.

   Lt. Gen. Robert Skinner on March 29 told Congress that hackers backed by China, Russia and other adversaries are applying “very high” levels of effort to digitally infiltrate, surveil and make off with plans or intelligence closely held by suppliers to the Department of Defense

2. **Report: Chinese state-sponsored hacking group highly active (AP News, 30 MAR, David Rising)**

   A Chinese hacking group that is likely state-sponsored and has been linked previously to attacks on U.S. state government computers is still “highly active” and is focusing on a broad range of targets that may be of strategic interest to China’s government and security services, a private American cybersecurity firm said in a new report Thursday.

   The hacking group, which the report calls RedGolf, shares such close overlap with groups tracked by other security companies under the names APT41 and BARIUM that it is thought they are either the same or very closely affiliated, said Jon Condra, director of strategic and persistent threats for Insikt Group, the threat research division of Massachusetts-based cybersecurity company Recorded Future.

3. **TikTok represents 'strategic' challenge, says top US cyber official (Reuters, 28 MAR, Stephen Nellis)**

   The head of the U.S. National Security Agency's cybersecurity directorate on Monday said TikTok represents a "strategic issue" rather than an immediate "tactical" threat to the United States.

   Speaking at a policy conference in Northern California, Rob Joyce, director of cybersecurity for the spy agency, reiterated the agency's earlier position that the Chinese-owned social networking app is akin to a "loaded gun" that the Chinese government could use to influence what information Americans see.

4. **How could a TikTok ban be enforced? (The Hill, 27 MAR, Rebecca Klar)**

   Bipartisan support to ban TikTok in the U.S is mounting, but carrying out the action will likely be trickier than gaining the political power to enact it.

   Any action the U.S. takes to try to block TikTok, the video sharing app owned by Chinese-based parent company ByteDance, will still have loopholes for users to access through workarounds and is almost certain to be challenged by free speech groups.

5. **Why does US see Chinese-owned TikTok as a security threat? (AP News, 24 MAR, Joe McDonald and Zen Soo)**

   U.S. lawmakers have grilled TikTok CEO Shou Zi Chew about data security and harmful content, with some pushing to ban the popular short-video app nationwide.

   Chew, a native of Singapore, told the lawmakers that TikTok prioritizes user safety as he

sought to avert a U.S. ban on the app by downplaying its ties to China.

Both Republican and Democratic representatives aggressively questioned Chew on topics including TikTok's content moderation practices, its data security plans, and past spying on journalists.

6. Why TikTok's security risks keep raising fears (AP News, 23 MAR, Kelvin Chan & Haleluya Hadero)

The battle between the U.S. and China over TikTok came into full view on Thursday when the social media platform's CEO testified before Congressional lawmakers.
Shou Zi Chew's hearing in front of the House Committee on Energy and Commerce is happening at what he's called a "pivotal moment" for the hugely popular short video sharing app. TikTok is owned by parent company ByteDance, which has offices in Beijing. The platform has 150 million American users but it's been dogged by persistent claims that it threatens national security and user privacy, or could be used to promote pro-Beijing propaganda and misinformation.

7. Here are the countries that have bans on TikTok (AP NEWS, 23 MAR, Kelvin Chan)

A growing number of countries in North America, Europe and Asia-Pacific have banned the popular video-sharing app TikTok from government devices as privacy and cybersecurity concerns increase. A handful have prohibited the app altogether.

The company's CEO faced a grilling Thursday from U.S. lawmakers. TikTok, which is owned by the Chinese technology company Bytedance, has long maintained that it does not share data with the Chinese government.

The company points to a project its carrying out to store U.S. user data in the U.S., which it says will put it out China's reach. It also disputes accusations it collects more user data than other social media companies, and insists that it is run independently by its own management.

8. US sent 'hunt-forward' team to Albania in wake of Iranian cyberattacks (C4ISR Net, 23 MAR, Colin Demarest)

U.S. cyber specialists spent three months in Albania working alongside forces there to identify network weaknesses and hacking tools following Iranian cyberattacks on government systems.

The so-called hunt-forward operation, a defensive measure taken at the invitation of foreign officials, was the first conducted in Albania, a smaller NATO ally. U.S. Cyber Command revealed the operation, handled by its Cyber National Mission Force, or CNMF, on March 23.

9. Pulling the Plug on TikTok Will Be Harder Than It Looks (The New York Times, 21 MAR, David E. Sanger, David McCabe and Sapna Maheshwari)

The tensions over the Chinese-owned social media app will come to a head on Thursday, when the company's chief executive testifies on Capitol Hill.

In the summer of 2020, in full re-election mode and looking for new ways to punish China, President Donald J. Trump threatened to cut off TikTok from the phones of millions of Americans unless its parent company agreed to sell all of its U.S. operations to American owners. The effort collapsed.

10. **If You Think AI Is Hot, Wait Until It Meets Quantum Computing (Forbes, 21 MAR, Susan Galer)**

The resurgence of AI has industry leaders counting the days until quantum computers go mainstream. There's been considerable progress on the quantum computing front since I blogged last year about how The European Quantum Industry Consortium (QuIC) was developing its Quantum Strategic Industry Roadmap. For an update, I reached out to Laure Le Bars, research project director at SAP and also president of QuIC. Le Bars was a recent guest on the Future of ERP Podcast from SAP, hosted by Richard Howells, vice president for thought leadership at SAP, and Oyku Ilgar, marketing director for SAP Supply Chain.

11. **What Is a Domain Fronting Attack and How Can You Prevent One? (Make Use Of It, 18 MAR, Chris Odogwu)**

The domain accessing your network may not be what it seems. Domain fronting allows an attacker to sneak in from what seems to be a legitimate source.

They say all is fair in war. Cybercriminals are going all out to win the cyberwar by implementing any means possible to attack unsuspecting victims for their data. They deploy the biggest deceptions to mask their identity and take you by surprise with techniques like domain-fronting attacks.

That seemingly legitimate domain accessing your network may not be legitimate after all. For all you know, an attacker could be fronting it to put you in a tight corner. This is what's known as a domain fronting attack. Is there anything you can do about it?

12. **Threat actors using images, Google translate links, and special characters to launch phishing attacks (The Hindu, 17 MAR,)**

Cybercriminals are using three novel tactics to bypass scrutiny by security measures and launch phishing attacks. These include using Google Translate service, images, and special characters in text to hide malicious URLs.

While the overall volume of attacks using these tactics is currently low, with each tactic making up less than 1% of attempted phishing attacks, they are widespread, with between 11% and 15% of organisations affected, often with multiple attacks, a research report from Barracuda said.

13. **Ransomware attacks are increasing, so you better be 'cyber ready' (The Scotsman, 17 MAR, Laura Gillespie)**

Ransomware attacks are increasing in volume, and threat actors are increasingly aggressive and sophisticated in the nature of such attacks.

While guidance has been introduced to help businesses understand what measures they should take to address ransomware risk, there are increasingly complex challenges to be navigated when engaging with those behind ransomware attacks and deciding whether to make a payment to recover access to systems and data.

14. **GPT-4 vs. ChatGPT: just how much better is the latest version? (Digital Trends, 17 MAR, Jon Martindale)**

GPT-4 is the latest language model for the ChatGPT AI chatbot, and despite just being released, it's already making waves. The new model is smarter in a number of exciting ways, most notably its ability to understand images, and it can also process over eight times as many words as its predecessor. It's a lot harder to fool now as well.

15. **KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks (Microsoft, 17 MAR, Azure Network Security Team)**

In the last year, geopolitical tension has led to an uptick of reported cybercrime events fueled by hacktivist groups. The US Cybersecurity and Infrastructure Security Agency (CISA) published an advisory to warn organizations about these attacks and teamed with the FBI on a distributed denial-of-service (DDoS) response strategy guide. KillNet, a group that the US Department of Health and Human Services (DHHS) has called pro-Russia hacktivists, has been launching waves of attacks against western countries, targeting governments and companies with focus on the healthcare sector. DHHS published an analyst note on KillNet's threat to the health sector, mentioning that the group compromised a US healthcare organization that supports members of the US military.

16. **Russian Hackers Preparing New Cyber Assault Against Ukraine: Report (News 18, 16 MAR, Majid Alam)**

Russian hackers appear to be preparing a renewed wave of cyber attacks against Ukraine, including a "ransomware-style" threat to organizations serving Ukraine's supply lines, a research report by Microsoft said on Wednesday.

The report, authored by the tech giant's cyber security research and analysis team, outlines a series of new discoveries about how Russian hackers have operated during the Ukraine conflict and what may come next.

17. **New security platform to fight AI-based cyber attacks (Data Centre & Network News, 16 MAR, Beatrice)**

OryxAlign has launched securyXDR, a fully managed extended detection and response (XDR) platform. An advanced form of antivirus and malware management, the system is part of a solution that will address the expected rise in sophisticated AI-phishing attacks. It will be valuable for SMEs, or those with a hybrid and remote workforce, across sectors including financial services, recruitment, legal and more.

18. **Microsoft adds AI tools to office apps like Outlook, Word (AP News, 16 MAR, Haleluya Hadero)**

Microsoft is infusing artificial intelligence tools into its suite of office software, including Word, Excel and Outlook emails.

The company said Thursday the new feature, named Copilot, is a processing engine that will allow users to do things like summarize long emails, draft stories in Word and animate slides in PowerPoint.

Microsoft 365 General Manager Colette Stallbaumer said the new features are currently only available for 20 enterprise customers. It will roll it out for more enterprise customers over the coming months.

19. **A year of Russian hybrid warfare in Ukraine (Microsoft, 15 MAR)**

Prior to Russia's full-scale invasion of Ukraine on February 24, 2022, many observers expected that a Russian-led hybrid war, like that observed when Russia invaded Donbas and illegally annexed Crimea in 2014, would involve marrying cyber weapons, influence operations, and military force to swiftly overrun Ukrainian defenses. Now, one year after its full-scale invasion, Russia's military has indeed wrought physical devastation in Ukraine but has not achieved its objectives—in part because Moscow's parallel cyber and influence operations have largely failed.

20. **Is Russia regrouping for renewed cyberwar? (Microsoft, 15 MAR, Clint Watts)**

As the second year of the Russian war in Ukraine commences, a detailed survey of the cyberattacks used during the first year of the war, and especially new developments we have observed in recent months, provide hints of what the future of this hybrid war may hold.

Since the start of the war, Russia has deployed at least nine new wiper families and two types of ransomware against more than 100 government and private sector Ukrainian organizations. Strong cyber defense partnerships between the public and private sector, and Ukrainian preparedness and resilience, has successfully defended against most of these attacks, but Russian activity continues.

21. **Russian Cyberspies Abuse EU Information Exchange Systems in Government Attacks (Security Week, 15 MAR, Ionut Arghire)**

Russia-linked APT29 was seen abusing the legitimate information exchange systems used by European countries in attacks aimed at governments.

Russia-linked cyberespionage group APT29 has been observed abusing two legitimate information exchange systems used by European countries, BlackBerry reports.

APT29 is a Russian advanced persistent threat (APT) actor mainly focused on cyberespionage. The group, believed to be sponsored by the Russian Foreign Intelligence Service (SVR), is also tracked as Cozy Bear, the Dukes, Nobelium, and Yttrium.

As part of a recently observed campaign aimed at EU governments, the group was seen sending phishing emails with a malicious document attached, using the Polish Foreign Minister's recent visit to the US as a lure.

22. **What can ChatGPT maker's new AI model GPT-4 do? (AP News, 15 MAR, Kelvin Chan)**

The company behind the ChatGPT chatbot has rolled out its latest artificial intelligence model, GPT-4, in the next step for a technology that's caught the world's attention.

The new system can figure out tax deductions and answer questions like a Shakespearan pirate, for example, but it still "hallucinates" facts and makes reasoning errors.

Electronic Warfare

1. **An Impenetrable Dome From Drones: How the Russian "Pole-21" Electronic Warfare System Protects the Sky from High-Precision Weapons and UAVs (Army Europe Open Source Intelligence Center, 29 MAR)**

   According to the RF Ministry of Defense, a Ukrainian attack attempt was made on Sunday, March 26 by an unmanned aerial vehicle of the Strizh type (Tu-141) in a shock performance in the Tula region, and a latest Russian electronic warfare system "Pole [Field]-21" lowered down the Ukrainian drone. The characteristics of the "Pole-21" system are classified. It is known that "Pole21" is primarily designed to combat high-precision weapons and unmanned aerial vehicles. The system is able to create an impenetrable dome of interference and thereby suppress the equipment for binding to global satellite and radio navigation systems. The system can control the airspace within a radius of over 50 km. It allows to put up to a hundred radio interference posts in the area of responsibility. The system is capable of not only jamming signals, but also introducing distortions into them forming false coordinates. As soon as a drone flew into the "Pole-21" coverage area, it lost control and fell.

2. **Success of Russian Electronic Warfare Should Not be Overstated, and Here is Why (Defense Express, 21 MAR)**

   Recently, Defense Express noticed many comments about Russians constantly accumulating their EW systems in Ukraine frontlines in order to jam unmanned vehicles piloted by the Ukrainian army with utmost effectiveness. That may make an impression of total Russian superiority in the EW field.

   However, that would be an overstatement. Sometimes, Russian EW systems cannot do anything about a drone, somewhere they simply lack these systems, and in some particular cases, it is Ukrainian EW specialists who achieve significant success. We can see that from some of the openly available videos from the frontlines we'd like to discuss below.

3. **What is 'deep sensing' and why is the US Army so focused on it? (C4ISR Net, 17 MAR, Colin Demarest)**

   The Army is seeking ways to identify, monitor, target and strike opponents from farther distances and with greater precision amid the U.S. military's pivot to the Indo-Pacific.

   To do so, the service is pursuing what officials, including Secretary Christine Wormuth and Chief of Staff Gen. James McConville, dub "deep sensing."

4. **Cyber plays both sides of the spectrum with both offensive bullets and defensive shields (Breaking Defense, 16 MAR)**

   Just demonstrated on a live range at Pax River, an airborne SIGINT platform injected cyber effects, neutralizing an integrated air defense system and clearing the airspace for US assets to execute a strike.

Information Advantage

1. **TikTok propaganda labels fall flat in 'huge win' for Russia (AP, 30 MAR, David Klepper)**

   A year ago, following Russia's invasion of Ukraine, TikTok started labeling accounts operated by Russian state propaganda agencies as a way to tell users they were being exposed to Kremlin disinformation.

   An analysis a year later shows the policy has been applied inconsistently. It ignores dozens of accounts with millions of followers. Even when used, labels have little impact on Russia's ability to exploit TikTok's powerful algorithms as part of its effort to shape public opinion about the war.

2. **Musk, scientists call for halt to AI race sparked by ChatGPT (AP News, 30 MAR, Matt O'Brien)**

   Are tech companies moving too fast in rolling out powerful artificial intelligence technology that could one day outsmart humans?

   That's the conclusion of a group of prominent computer scientists and other tech industry notables such as Elon Musk and Apple co-founder Steve Wozniak who are calling for a 6-month pause to consider the risks.

   Their petition published Wednesday is a response to San Francisco startup OpenAI's recent release of GPT-4, a more advanced successor to its widely-used AI chatbot ChatGPT that helped spark a race among tech giants Microsoft and Google to unveil similar applications.

3. **TikTok updates content rulebook as pressure from West builds – (AP News, 21 MAR)**

   TikTok on Tuesday rolled out updated rules and standards for content and users as it faces increasing pressure from Western authorities over concerns that material on the popular Chinese-owned video-sharing app could be used to push false information.

   The company released a reorganized set of community guidelines that include eight principles to guide content moderation decisions.

   "These principles are based on our commitment to uphold human rights and aligned with international legal frameworks," said Julie de Bailliencourt, TikTok's global head of product policy.

   She said TikTok strives to be fair, protect human dignity and balance freedom of expression with preventing harm.

4. **AI-powered tools, deepfakes pose challenge of misinformation before Internet users (The Week, 20 MAR,**

   The battle against misinformation has become more difficult

   Artificial intelligence, deepfakes and social media little understood by laypersons, the combo of three poses a mystifying hurdle for millions of Internet users caught in the everyday battle of trying to filter the real from the fake.

   The battle against misinformation was always challenging and has become much more so since developments in AI-powered tools have made detecting deepfakes on multiple

social media platforms more difficult. The unintended ability of AI to create fake news faster than stopping it has worrying consequences.

5. **Pro-Moscow voices tried to steer Ohio train disaster debate (AP News, 18 MAR, David Klepper)**

   Soon after a train derailed and spilled toxic chemicals in Ohio last month, anonymous pro-Russian accounts started spreading misleading claims and anti-American propaganda about it on Twitter, using Elon Musk's new verification system to expand their reach while creating the illusion of credibility.

   The accounts, which parroted Kremlin talking points on myriad topics, claimed without evidence that authorities in Ohio were lying about the true impact of the chemical spill. The accounts spread fearmongering posts that preyed on legitimate concerns about pollution and health effects and compared the response to the derailment with America's support for Ukraine following its invasion by Russia.

6. **Explainer: What is Generative AI, the technology behind OpenAI's ChatGPT? (Reuters, 17 MAR,**

   Generative artificial intelligence has become a buzzword this year, capturing the public's fancy and sparking a rush among Microsoft (MSFT.O) and Alphabet (GOOGL.O) to launch products with technology they believe will change the nature of work.

   Here is everything you need to know about this technology.

7. **Factbox: TikTok's Chinese ownership, security concerns spark bans across nations (Reuters, 17 MAR, Yuvraj Malik)**

   The Biden administration has demanded that TikTok's Chinese owners divest their stakes in the popular video app or face a possible U.S. ban, the company told Reuters this week.

   The move follows the introduction of a new U.S. legislation that would allow the White House to ban TikTok or other foreign-based technologies if they pose a national security risk.

   Other countries and entities have also elected to ban the app.

8. **Why TikTok's security risks keep raising fears (AP News, 17 MAR, Haleluya Hadero)**

   TikTok is once again fending off claims that its Chinese parent company, ByteDance, would share user data from its popular video-sharing app with the Chinese government, or push propaganda and misinformation on its behalf.

   China's Foreign Ministry on Wednesday accused the United States itself of spreading disinformation about TikTok's potential security risks following a report in the Wall Street Journal that the Committee on Foreign Investment in the U.S. — part of the Treasury Department — was threatening a U.S. ban on the app unless its Chinese owners divest their stake.

Signal

1. **Space Force seeking more narrowband communication satellites (C4ISRNet, 31 MAR, Courtney Albon)**

   The U.S. Space Force is moving forward with plans to buy two more Mobile User Objective System satellites, which provide secure narrowband communication for military users.

   A March 24 solicitation kicks off the first phase of the effort, which is focused on early design and risk reduction work. The service plans to award a 12-to-18-month contract to as many as two companies in September. By fiscal year 2025, the Space Force will select a single company to deliver the satellites, the first of which it wants to launch before the end of FY30.

2. **Govt launches 'quantum communication' network with a dare: Rs 10L for ethical hackers who can break encryption (The Print, 27 MAR, Yuthika Bhargava)**

   Quantum communication refers to communication channels that take advantage of laws of quantum physics to protect data & in theory, is much more secure than traditional systems.

   New Delhi: The government Monday announced that the first quantum communication network is operational in the country and challenged ethical hackers to break the encryption on the network — offering them a reward of Rs 10 lakh per break.

3. **Passwords vs Passwordless: A Debate on Online Security (ghacks.net, 27 MAR, Russell Kidson)**

   Passwords can be a source of frustration for many individuals in the digital age, often viewed as an inconvenient necessity. While they are an essential element of online security, research indicates that people frequently fail to use them correctly. Fortunately, the introduction of password managers has alleviated the burden of having to remember and create numerous strong and distinctive passwords. However, these tools are not without flaws, and some individuals still find them troublesome to use for various reasons, resulting in a reluctance to adopt them.

4. **Why Zero Trust Is Necessary In The Fight Against Ransomware (Forbes, 23 MAR, Michelle Drolet)**

   The rising number and increasing severity of ransomware attacks are sufficient to prove that current cybersecurity strategies are simply not working. The fact is, today's security approaches are far too focused on the network perimeter and too lenient when it comes to internal traffic. And since most users, devices and cloud-based applications operate outside of the corporate perimeter, the traditional approach of considering network location as the prime component of the security posture has now become obsolete.

   What's more, the perimeter-based approach is also insufficient from the perspective that if an attacker breaches the perimeter, it is extremely difficult to block or halt their lateral movement. Given this scenario, organizations are in dire need of a new security approach that is not just solely focused on network location. Enter zero trust.

5. **Elon Musk's Starlink is aiding criminal mining efforts in Brazil's Amazon (Business Insider, 17 MAR, Grace Mayer)**

   When Elon Musk launched Starlink, SpaceX's satellite internet service, in 2020, he

envisioned connecting people and businesses around the world — particularly in remote areas.

In Brazil, Starlink internet terminals have done just that. But, according to an investigation by the Associated Press, some of those terminals are assisting illegal mining efforts in parts of the Amazon, where such activities have contaminated waterways and caused disease and famine to spread.

In the last five weeks, seven Starlink terminals were found and seized at illegal mining sites in Yanomami land, Brazil's largest Indigenous region, the Brazilian environment agency Ibama told the AP.

6. **US Army consolidates network modernization efforts into single office (Defense News, 17 MAR, Colin Demarest)**

A U.S. Army hub for battlefield communications development will soon oversee a larger portfolio.

The Program Executive Office for Command, Control and Communications-Tactical, or PEO C3T, will by Oct. 1 absorb the network-heavy assignments of the Program Executive Office for Enterprise Information Systems, or PEO EIS.

7. **DoD seeking seamless military-commercial satellite communications (Space News, 16 MAR, Sandra Erwin)**

DoD satcom chief Mike Dean: 'We try to not make distinction between commercial and military or even international partner services'

Among the many new products unveiled this week at the Satellite 2023 convention were mobile communications terminals capable of talking to military and commercial satellites.

Intellian Technologies rolled out a new terminal it developed with the U.S. Navy that provides simultaneous connectivity with commercial Ka-band satellites and with the military Wideband Global Satcom (WGS) constellation used by the U.S. and several allied nations.

8. **No, AI did not break post-quantum cryptography (Cloudflare, 16 MAR, Bas Westerbaan. Lejla Batina, & Stjepan Picek)**

News coverage of a recent paper caused a bit of a stir with this headline: "AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm". The news article claimed that Kyber, the encryption algorithm in question, which we have deployed world-wide, had been "broken." Even more dramatically, the news article claimed that "the revolutionary aspect of the research was to apply deep learning analysis to side-channel differential analysis", which seems aimed to scare the reader into wondering what will Artificial Intelligence (AI) break next?

Reporting on the paper has been wildly inaccurate: Kyber is not broken and AI has been used for more than a decade now to aid side-channel attacks. To be crystal clear: our concern is with the news reporting around the paper, not the quality of the paper itself. In this blog post, we will explain how AI is actually helpful in cryptanalysis and dive into the paper by Dubrova, Ngo, and Gärtner (DNG), that has been misrepresented by the news coverage. We're honored to have Prof. Dr. Lejla Batina and Dr. Stjepan Picek, world-renowned experts in the field of applying AI to side-channel attacks, join us on this blog.

9. NSA Shares Guidance on Maturing ICAM Capabilities for Zero Trust (Security Week, 15 MAR, Ionut Arghire)

The National Security Agency (NSA) this week published guidance to help system operators mature identity, credential, and access management (ICAM) capabilities to improve their cyberthreat protections.

Immature ICAM capabilities pose a risk to critical infrastructure, national security, and defense industrial base (DIB) systems, but improvements can be made by integrating zero trust principles and designs into enterprise networks.

Part of the national cybersecurity strategy, the adoption of zero trust is mandated by the president's executive order on improving the nation's cybersecurity (EO 14028) and National Security Memorandum 8 (NSM-8), which applies to federal civilian executive branch (FCEB) agencies and national security system (NSS) owners and operators.

Items of Interest

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

These reports are a compilation of articles from Russia, Ukraine, and other nations regarding the current tensions between Russia and Ukraine. Topics covered in this report include the following:

- Foreign Observations and Reactions
- Social Media Highlights
- Russian Eastern Military District Movements
- Other Topics

Russia-Ukraine Situation Report, 30 March 2023

Russia-Ukraine Situation Report, 29 March 2023

Russia-Ukraine Situation Report, 28 March 2023

Russia-Ukraine Situation Report, 27 March 2023

Russia-Ukraine Situation Report, 24 March 2023

Russia-Ukraine Situation Report, 23 March 2023

Russia-Ukraine Situation Report, 22 March 2023

Russia-Ukraine Situation Report, 21 March 2023

Russia-Ukraine Situation Report, 20 March 2023

Russia-Ukraine Situation Report, 17 March 2023

Russia-Ukraine Situation Report, 16 March 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Patriot Missile System's Arrival Draws Near - 30 MAR
Wagner Has Up To 36,000 Troops In Bakhmut Says Top U.S. General - 29 MAR
France Denies It's Looking To Buy Back UAE's Mirage Jets For Kyiv - 28 MAR
Challenger Tanks, Stryker Armored Vehicles Arrive In Country - 27 MAR
Russian Nukes Ready To Deploy To Belarus This Summer - 25 MAR
Ukraine Situation Report: Sevastopol Attacked By Drones From Sea And Air - 22 MAR
Patriot Air Defenses To Arrive Sooner Than Anticipated - 21 MAR
Explosions Rock Russian-Occupied Crimea - 20 MAR
Armored Personnel Carriers Make A Charge In Bakhmut - 18 MAR
Arrest Warrant For Putin Issued Over War Crimes Allegations - 17 MAR
Delivery Of Polish MiG-29s Imminent - 16 MAR

3. Foreign Reflections on U.S. Exercises and Operations, 30 March 2023 (U.S. Army Asian Studies Detachment, 30 Mar)

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 23 to 29 March 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC,

Japan, the Philippines, North Korea, South Korea, and Taiwan.

4. **Foreign Reflections on U.S. Exercises and Operations, 27 March 2023 (U.S. Army Asian Studies Detachment, 27 MAR)**

   This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from16 to 22 March 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, North Korea, the Philippines, Singapore, and South Korea.

5. **Balloon Intercepted By U.S. Air Force Over Texas (The Drive, 25 MAR, Howard Altman & Tyler Rogoway)**

   North American Aerospace Defense Command has confirmed that it scrambled aircraft to investigate a suspicious target of interest over Texas.

   North American Aerospace Defense Command sent fighters, a supporting KC-135 tanker, and an E-3 Sentry Airborne Warning And Control aircraft after a suspicious radar track over southern Texas that was approaching the Gulf Of Mexico.

   We started getting word of an intercept operation occurring when radio enthusiasts reported the odd operation underway. The E-3 and the fighter-supporting KC-135 tanker were subsequently spotted on radar tracking software ADSBExchange.com flying orbits in the area in question.

6. **Russia Removing T-54 Tanks from 1295th Central Tank Repair and Storage Base (Army Europe Open Source Intelligence Center, 22 MAR)**

   A website reported about a video showing a trainload of T-54/55 tanks has recently departed from the town of Arsenyev, Primorsky region, where the 1295th Central Tank Repair and Storage Base is located.

7. **Russia's most elite troops use Soviet-era paper maps (Defense-Blog, 21 MAR, Dylan Malyasov)**

   Russia's all-out invasion of Ukraine confirmed that, despite the propaganda, Russian troops were poorly trained and equipped.

   Ill-equipped Russian soldiers have relied on decades-old paper maps, often getting lost on the battlefield and ambushed by Ukrainian troops.

   A noticeable example is the battle between the elite Russian Airborne Troops, or VDV, and the Ukrainian BMP-2 fighting vehicles near Girske, Luhansk Region, in May 2022. The Dead District blog brought to attention drone footage showing a Russian BMD-4M airborne infantry fighting vehicle of the 31st Air Assault Brigade of the Russian VDV lost its way and was ambushed by two BMP-2s of the Ukrainian 24th Brigade.

8. **Former US Marine may have been 'lured' from China before arrest, lawyer says (Reuters, 20 MAR, Kirsty Needham)**

   A former U.S. Marine Corps pilot may have been "lured" from China to Australia by security agencies before his arrest, his lawyer said outside court on Monday after an extradition hearing in Sydney.

   Daniel Duggan, 54, is facing extradition to the United States on charges of breaking U.S. law by training Chinese military pilots to land on aircraft carriers.

   He was arrested by Australian federal police in a rural town in New South Wales state in

October, shortly after returning from China, where he had lived since 2014.

9. **China's Xi arrives in Russia to meet Putin over Ukraine war (Reuters, 20 MAR, Michael Perry & Philippa Fletcher)**

Chinese President Xi Jinping flew into Moscow on Monday where he was expected to press Beijing's role as a potential peacemaker in the Ukraine conflict while Russian President Vladimir Putin hoped for support against Western pressure.

Xi will be the first national leader to shake Putin's hand since the International Criminal Court (ICC) issued an arrest warrant for him on Friday over the deportation of Ukrainian children to Russia since its invasion.

10. **What Vladimir Putin was doing on his first trip to Mariupol since its annexation (Australian Broadcasting Coperation News, 19 MAR,)**

Russian President Vladimir Putin has visited the occupied port city of Mariupol, his first trip to Ukrainian territory Moscow illegally annexed in September.

State television showed footage of him being shown around the city on Saturday night, meeting rehoused residents and being briefed on reconstruction efforts by Deputy Prime Minister Marat Khusnullin.

So what inspired the president to make the trip and what exactly was he doing there?

11. **Russian defence minister decorates pilots for downing U.S. drone (Reuters, 17 MAR, Mark Trevelyan)**

Russian Defence Minister Sergei Shoigu has presented awards to the pilots of two Su-27 fighter planes that intercepted a U.S. drone near the airspace around Russia's military campaign in Ukraine, his ministry said on Friday.

The drone crashed into the Black Sea on Tuesday after being intercepted by Russian jets, in the first known direct military encounter between Russia and the United States since Russia invaded Ukraine a year ago.

12. **Foreign Reflections on U.S. Exercises and Operations, 16 March 2023 (U.S. Army Asian Studies Detachment, 16 MAR)**

This week's report contains reporting of foreign observations on U.S. and Bilateral exercises from 10 to 15 March 2023. Each section also contains the respective ASD report number for the original report (if available) and covers reporting from the PRC, Japan, the Philippines, Russia, and South Korea.

13. **Wagner's convicts tell of horrors of Ukraine war and loyalty to their leader (Reuters, 16 MAR, Filipp Lebedev & Felix Light)**

In October last year, a Russian news site published a short video of Yevgeny Prigozhin, founder of the Wagner Group, the Russian mercenary army, sitting with four men on a rooftop terrace in the resort town of Gelendzhik, on Russia's Black Sea coast. Two are missing parts of a leg. A third has lost an arm. They are identified as pardoned former convicts, returned from the front in Ukraine after joining Wagner from prison.

14. **US Army chief wants three multidomain task force units in the Pacific (C4ISR Net, 15 MAR, Jen Judson)**

The U.S. Army chief would like to see three multidomain task force units in the Pacific region, he said Wednesday at the McAleese & Associates conference.

“I can see three in the Pacific and then one other one. We have one in Europe and then one probably in a contingency-type place where it can go wherever it needs. So I think that’s how those five are going to play out,” Gen. James McConville said.