Cyber Center of Excellence

Unclassified Threat Read Book

15 - 31 JUL 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

Russia-Ukraine

1. Russia-Ukraine Situation Report
2. The WARZONE Ukraine Situation Report
3. Deutsche Welle (DW) Ukraine updates
4. Crimea Attack Provokes Dangerous Escalation! Russia, For The 1st Time, Strikes At NATO's Doorstep; Hits Ukraine's Reni Port - 26 JUN
5. Ukraine Strikes Back With Drone Attacks On Moscow, Crimea - 24 JUL
6. Trench Warfare In Ukraine Casts Old School Army Training In Different Light - 21 JUL
7. A Sobering Analysis Of Ukraine's Counteroffensive From The Front - 20 JUL
8. Russia Directly Targets Ukrainian Grain In Reprisal Airstrikes - 19 JUL
9. Captured Russian Weapons Being Studied By UK - 18 JUL
10. Russia's Kerch Strait Bridge Has Been Badly Damaged - 17 JUL

Cyber

1. **Army officially creates new offensive cyber and space program office (Defense Scoop, 28 JUL, Mark Pomerleau)**

   Christopher Green assumed the role for project management for cyber and space within the program executive office for intelligence, electronic warfare and sensors.

   The Army has officially created an offensive cyber and space program office to manage the portfolio of capabilities it provides for soldiers as well as the joint force.

   In a ceremony on July 25, Christopher Green assumed the role for project management for cyber and space within the program executive office for intelligence, electronic warfare and sensors.

2. **Industrial Organizations in Eastern Europe Targeted by Chinese Cyberspies (Security Week, 24 JUL, Eduard Kovacs)**

   A China-linked cyberspy group appears to be behind a campaign targeting industrial organizations in Eastern Europe, cybersecurity firm Kaspersky reported last week.

   The attacks have been linked to APT31, a group believed to be sponsored by the Chinese government that is also known as Zirconium, Judgement Panda, Bronze Vinewood and Red Keres. The threat actor has focused on operations whose goal is to steal valuable intellectual property from victims.

3. **MOVEit Hack Could Earn Cybercriminals $100M as Number of Confirmed Victims Grows (Security Week, 24 Jul, Eduard Kovacs)**

   Experts believe the Cl0p ransomware gang could earn as much as $100 million from the MOVEit hack, with the number of confirmed victims approaching 400.

   Ransomware recovery company Coveware believes the Cl0p ransomware gang could earn as much as $100 million from the MOVEit hack, which has impacted hundreds of organizations.

   In a ransomware monetization report published on Friday, Coveware said the percentage of victims that paid a ransom in the second quarter of 2023 fell to a record low of 34%.

4. **Top cybersecurity exec talks targeted hacks on U.S. diplomats (CNBC, 21 JUL)**

   Rupal Hollenbeck, Check Point Software president, joins 'TechCheck' to talk the state of U.S. cybersecurity after targeted China-linked hacks impact U.S. diplomats.

5. **Microsoft Cloud Hack Exposed More Than Exchange, Outlook Emails (Security Week, 21 JUL, Ryan Naraine)**

   Cloud security researcher warns that stolen Microsoft signing key was more powerful and not limited to Outlook.com and Exchange Online.

   Researchers at cloud security startup Wiz have an urgent warning for organizations running Microsoft's M365 platform: That stolen Microsoft Azure AD enterprise signing key gave Chinese hackers access to data beyond Exchange Online and Outlook.com.

6. **In Other News: Military Emails Leaked, Google Restricts Internet Access, Chinese Spyware (Security Week, 17 JUL)**

   Weekly cybersecurity news roundup that provides a summary of noteworthy stories

that might have slipped under the radar for the week of July 17, 2023.

Electronic Warfare

1. **Electronic Warfare: Is The U.S. Military Falling Behind? (1945, 31 JUL, Kris Osborn)**

   Some of the newest EW systems use what is referred to as narrowly configured "pencil beams" designed to emit a more precise, yet smaller and less detectable signature.

   Years ago, former Chief of Naval Operations Adm. Jonathan Greenert famously made the statement, "Whoever dominates the electromagnetic spectrum" will prevail in future conflict. Certainly, the ability to control, monitor, or jam enemy communications, radar, weapons guidance systems and drone datalinks, and RF signals could prove decisive in any modern warfare engagement.

2. **Strategic Command officially creates Joint Electromagnetic Spectrum Operations Center (Defense Scoop, 25 JUL, Mark Pomerleau)**

   The JEC will aim to provide the joint force metrics on readiness within the electromagnetic spectrum.

   U.S. Strategic Command will official establish the Joint Electromagnetic Spectrum Operations Center in a ceremony Wednesday, serving as a key piece of the Pentagon's implementation plan for its spectrum superiority strategy to gain an advantage over adversaries.

   The JEC, as it is known, will aim to raise the readiness of the joint force within the electromagnetic spectrum, serving as the heart of the Defense Department's EMSO, according to a spokesperson. It will work to restructure accounts for force management, planning, situation monitoring, decision-making and force direction while focusing on training and education with capability assessments.

3. **US' 'Cutting-Edge' Switchblade-600 Drone "Downed" By Russian Electronic Warfare; Viral Videos Show Near-Intact Munition (The EurAsian Times, 25 JUL, Parth Satam)**

   Seven months after it first arrived in Ukraine, a US-made Switchblade-600 loitering munition has possibly fallen into Russian hands after it was downed over Donetsk, according to multiple videos on social media.

   A viral clip posted by many Twitter and Telegram accounts showed a nearly intact unit that has sustained superficial damage, with speculations that Russian engineers will now study the technology behind the advanced drone.

   This is the second time the Switchblade-600 had fallen into Russian hands, with the first instance in late April, when another video showed Russian soldiers examining the rear part of the UAV with the engine, with the front portion reportedly missing after a strike.

4. **NATO's Exercise Ramstein Guard strengthens electronic warfare capabilities (Aero Time, 20 Jul, Clement Charpentreau)**

   Allied forces in Lithuania are currently participating in Exercise Ramstein Guard, an electronic warfare exercise aimed at enhancing the capabilities of the NATO

Integrated Air and Missile Defence System or NATINAMDS units.

The exercise, taking place simultaneously in Lithuania and Latvia from July 17 to 21, 2023, consists of Electronic Warfare (EW) drills under the command and control of NATO's Combined Air Operations Centre in Uedem, Germany.

5. **Dearth of jamming gear follows years of 'autopilot,' says Rep. Bacon (C4ISR Net, 19 JUL, Colin Demarest)**

The U.S. military is failing to speedily develop and deploy electronic warfare equipment amid a global competition for electromagnetic spectrum supremacy, according to a congressman who served in the Air Force for more than two decades.

After years of putting electronic warfare on "autopilot," troops' ability to now jam and spoof and spy from afar has "withered," said Rep. Don Bacon, a Nebraska Republican and former director of intelligence, surveillance and reconnaissance strategy, plans, doctrine and force development.

6. **The Evolution of Digital Radio Frequency Memory (DRFM) (Anyuak Media, 15 JUL)**

Digital Radio Frequency Memory (DRFM) has revolutionized the field of electronic warfare, providing advanced capabilities for military forces around the world. This technology has come a long way since its inception, evolving and adapting to meet the changing needs of modern warfare.

Information Advantage

1. **FBI warns of broad AI threats facing tech companies and the public (Cyber Scoop, 28 JUL, AJ Vicens)**

The bureau warned that hackers will target tech companies, researchers and academics working on artificial intelligence advancements.

Executives, researchers and engineers at big tech companies and startups alike working on artificial intelligence face a growing threat from criminal and nation-state hackers looking to pilfer intellectual property or data that underlies powerful chatbots, the FBI warned on Friday.

The growing risk coincides with increasing availability of AI tools and services to the general public in the form of products such as OpenAI's ChatGPT, or Google's Bard, for instance, as well as the increasing ease and ability for many companies to develop AI language models.

2. **BRI - Belt and Road Initiative - Highlights, 26 July 2023 (U.S. Army Asian Studies Detachment, 27 Jul)**

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

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

ASD is publishing BRI-related reports on PiX, the Protected Internet eXchange Portal, which can be viewed at the following URL:

hxxps://pixtoday.net/article/article/220079.

3. **China allegedly turns to transnational criminals to spread disinformation in Australia (The Record, 25 JUL, Daryna Antoniuk)**

Australian researchers have found evidence that China is using fake social media accounts linked to transnational criminal groups to spread online propaganda and disinformation.

According to a report that the Australian Strategic Policy Institute (ASPI) released this week, certain fake accounts used by China for its influence operations are linked to a network of Twitter accounts that promote Warner International Casino, an online gambling platform operating in Southeast Asia.

4. **Russia using 'disinformation' to exaggerate 'small' military gains in Ukraine, says UK (Evening Standard, 24 JUL, Sami Quadri)**

Russia has only achieved "marginal gains" during its assault along the north of the frontline in Luhansk and Kharkiv oblasts, British defence chiefs have said.

The UK's Ministry of Defence (MoD) says Russia is using "disinformation" to exaggerate these small military gains in Ukraine.

5. **AI being used for hacking and misinformation: top Canadian cyber official (Reuters, 20 JUL, Raphael Satter)**

Hackers and propagandists are wielding artificial intelligence (AI) to create malicious software, draft convincing phishing emails and spread disinformation online, Canada's top cybersecurity official told Reuters, early evidence that the technological revolution sweeping Silicon Valley has also been adopted by cybercriminals.

In an interview this week, Canadian Centre for Cyber Security Head Sami Khoury said that his agency had seen AI being used "in phishing emails, or crafting emails in a more focused way, in malicious code (and) in misinformation and disinformation."

6. **Google Creates Red Team to Test Attacks Against AI Systems (Security Week, 21 JUL, Eduard Kovacs)**

Google has created a red team that focuses on artificial intelligence (AI) systems and it has published a report providing an overview of common types of attacks and the lessons learned.
The company announced its AI Red Team just weeks after introducing Secure AI Framework (SAIF), which is designed to provide a security framework for the development, use and protection of AI systems.
Google's new report highlights the importance of red teaming for AI systems, the types of AI attacks that can be simulated by red teams, and lessons for other organizations that might consider launching their own team.

7. **Misinformation – the dark side of generative AI (Verdict, 19 JUL)**

The growing number of media sources makes the battle against misinformation more challenging.

Misinformation is among the main challenges facing the media industry today.

It encompasses a broad spectrum of cases where the purpose is either malicious (so-called disinformation) or simply due to inaccuracy or honest mistakes. Whatever

the purpose, information sources need to ensure that the content they spread is accurate if they want to remain reliable in the eyes of their audience and prevent any unnecessary harm to society.

8. **Real-time deepfake detection: How Intel Labs uses AI to fight misinformation (ZD Net, 16 JUL, Dan Patterson)**

   Intel's Ilke Demir explains how deepfake tech works, and why it's essential for AI researchers to collaborate with anthropologists, social scientists, and academic researchers.

   A few years ago, deepfakes seemed like a novel technology whose makers relied on serious computing power. Today, deepfakes are ubiquitous and have the potential to be misused for misinformation, hacking, and other nefarious purposes.

9. **Fact check: Deepfakes and disinformation in the Ukraine war (DW, 18 JUL, Rachel Baig)**

   Deepfake videos make it hard to distinguish fact from fiction, especially in a war that is also unfolding online and is full of mis- and disinformation. Experts have worried for years that fakes like deepfakes will play a major role in disinformation and propaganda campaigns.

Signal

1. **How China's satellite navigation technology is challenging U.S. GPS (CNBC, 29 JUL, Magdalena Petrova, Jeniece Pettitt & Christina Locopo)**

   For decades, the United States has been a leader in satellite navigation technology thanks to GPS. But in 2020, China launched the last satellite needed to complete its own global system called Beidou. Since then, the influence of Beidou has grown, with an estimated 1.1 billion people now using the system. Experts say Beidou underpins not only China's military ambitions, but is also spurring economic growth in the country and increasing its diplomatic leverage.

2. **Senator urges US agencies to hold Microsoft accountable for email hack (Verdict, 28 JUL, Alice Nunwick)**

   Senator Ron Wyden has called for Microsoft's "negligent cybersecurity practises" in the recent Outlook hack to be examined.

   In a letter released yesterday 27 July 27, Senator Ron Wyden urged the FTC, CISA and DOJ to "hold Microsoft responsible for negligent cybersecurity practices" that "enabled" a successful Chinese hack against the US government.

   The letter, addressed to the heads of each organisation, describes that the hack happened after the hackers stole an encryption key Microsoft itself had generated for Outlook's identity service.

3. **How 5G and mobile computing-at-the-edge are revolutionizing DOD's future (Defense Scoop, 26 JUL, Lamont Copeland)**

   The DOD's principal director of FutureG articulates better than most the real value 5G and MEC bring to enterprises like the Defense Department, says a Verizon executive.

Breakthrough technology developments often have a knack for catapulting onto the world stage only after years of research, testing and commercial piloting. That's probably never been more apparent than with the recent eruption of generative AI. However, the pattern is familiar to those of us who watched the emergence of cloud computing, mobile smartphones, GPS, the Internet and many other technology developments.

What often gets lost in the spotlight is the hard but essential work of integrating these breakthrough developments into the fabric of existing technologies — and reimagining entirely new ways of creating and delivering value for the federal government and businesses.

4. **US Army Tests Pilot Visual Navigation Tech for GPS-Denied Environments (The Defense Post, 20 JUL, Joe Saballa)**

   The US Army has announced the successful trial of a new visual navigation technology to help military pilots navigate in global positioning system (GPS)-denied environments.

   The test, conducted by the Combat Capabilities Development Command Aviation & Missile Center (AvMC), aimed to evaluate if the tech can provide precise location information in the absence of GPS.

   During the activity, a high-performance camera was attached to the base of an experimental Black Hawk helicopter to capture terrain images.

Items of Interest

1. **Travis King: How the US negotiates with North Korea (BBC News, 26 JUL, Chelsea Bailey)**

   A country with closed borders and few diplomatic channels... talking to North Korea is tricky at the best of times. Now the stakes are even higher with a young American soldier in their hands. How is the US going about securing his release?

   The fate of Travis King, a US soldier who crossed into North Korea, remains unknown and experts say the US is at a critical stage to try and negotiate his return home.

   The key challenge is America has never had an official diplomatic relationship with North Korea.

   As a result, the US relies on a network of backchannels to negotiate the return of citizens detained in the country.

2. **North Korea: China and Russia in first post-pandemic visits (BBC News, 26 JUL, Derek Cai)**

   A Russian delegation led by Defence Minister Sergei Shoigu has arrived in North Korea, to be joined by a Chinese delegation later on Wednesday.A

   They will attend Pyongyang's celebrations of the 70th anniversary of the end of the Korean War, marked typically by massive military parades.

   The visits are the first of their kind to the North since it shut its borders to try to keep out the pandemic.

   It is unclear if this signals a change in Pyongyang's border policies.

3. **96 Years Of PLA: Low On Morale & Training, China's People's Liberation Army A Deadweight On Xi Jinping (The EurAsian Times, 25 JUL, NC Bipindra)**

   August 1 marks the 96th anniversary of the People's Liberation Army (PLA). The world's largest military, the PLA, comprises over two million military personnel with an annual budget of $224.8 billion.
   However, despite the numbers and the resources, newfound aggressive strategy, and growing territorial ambitions, especially in the Indian Ocean Region (IOR) and South China Sea (SCS), is the PLA battle ready?
   The modernization project of the People's Liberation Army (PLA), incepted in 2015, has seen some huge investment in its efforts for the development of cutting-edge military hardware, further aimed to modernize its weapons, sensors, and military platforms.
   However, as per PLA Daily, the issue that continues to haunt the PLA is the shortage of skilled manpower with respect to Beijing's military modernization ambitions, and this remains a cause of concern.

4. **Air Force Nominee to Lead NSA and CYBERCOM Says They Should Keep Sharing One Leader (Air and Space Forces, 20 Jul, Chris Gordon)**

   Testifying before the Senate on July 20, the Air Force general nominated to head both the National Security Agency and U.S. Cyber Command offered a full-throated endorsement of the "dual-hat" arrangement in which the same official leads both organizations.

   "The signals intelligence and the cyber environments are overlapping," said Air Force Lt. Gen. Timothy Haugh, who has been tapped to pin a fourth star and become the first Airman to lead CYBERCOM since its establishment in 2010.

5. **U.S. Service Member In North Korea After "Willfully" Crossing Border (Updated) (The Drive/The War Zone, 18 JUL, Joseph Trevithick)**

   An American has crossed over into the North as Navy nuclear ballistic missile submarine is visiting the south for the first time in decades.

   Amember of the U.S. armed forces is believed to be in detention in North Korea. That individual crossed the inter-Korean Military Demarcation Line at the Joint Security Area in Panmunjom and did so deliberately, though their exact motivations remain unclear. This comes amid a surge in geopolitical friction on the Korean Peninsula, punctuated by the arrival today of the first U.S. Navy Ohio class nuclear ballistic missile submarine to visit the South in four decades.

Russia -Ukraine Conflict

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, 25 July 2023
Russia-Ukraine Situation Report, 24 July 2023
Russia-Ukraine Situation Report, 18 July 2023

2. The WARZONE Ukraine Situation Report (Howard Altman)

Ukraine Situation Report: Key Crimean Railway Bridge Targeted In Missile Strike – 31 JUL

Ukraine Situation Report: The Curious Case Of Kyiv's North Korean Rockets – 29 JUL

Ukraine Situation Report: S-200 Missile Slams Into Russian Town – 28 JUL

Ukraine Situation Report: Key Donetsk City Liberated – 27 JUL

Ukraine Situation Report: Main Thrust Of Counteroffensive Has Begun, Report States – 26 JUL

Ukraine Situation Report: Kyiv's Noose Around Bakhmut Tightens – 25 JUL

Ukraine Situation Report: Fighting Flares Around The Oskil River – 24 JUL

Ukraine Situation Report: Huge Explosions Rock Crimean Ammo Depot – 22 JUL

Ukraine Situation Report: U.S. Now Pushing To Deliver F-16s "As Fast As Possible" – 21 JUL

Ukraine Situation Report: U.S. Cluster Munitions Hit The Battlefield – 20 JUL

Ukraine Situation Report: Pentagon Promises More Bradleys, Strykers – 18 JUL

Ukraine Situation Report: Kyiv Claims Massive Russian Buildup Near Kharkiv – 17 JUL

Ukraine Situation Report: Kyiv's Growing Counter-Battery Advantage -15 JUL

3. Deutsche Welle (DW) Ukraine updates

Ukraine updates: NATO meeting to focus on Black Sea – 26 JUL
Ukraine updates: IAEA confirms mines near Zaporizhzhia plant – 25 JUL
Ukraine updates: Russian attack destroys Odesa grain depot – 24 JUL
More cracks appear in Russia's military – 24 JUL
Russia accuses Ukraine of drone attack in Moscow – 24 JUL
Ukraine updates: Russian missile attack targets Odesa – 23 JUL
Russian men keep fleeing abroad to avoid fighting in Ukraine – 18 JUL
Russia pulls out of Ukraine grain deal: What's next? – 17 JUL
Russia: From convict to hero via Ukraine? – 15 JUL

4. After Latest Moscow Strike, Zelensky Warns Drone War Is Coming To Russia (The Drive/The Warzone, 31 JUL, Thomas Newdick)

Long-range drone strikes on Moscow are increasing in frequency and Ukraine's leadership is talking more openly about them.

Ukrainian President Volodymyr Zelensky responded to the latest drone strike to hit targets in Moscow with a warning of further attacks on Russian territory, including military infrastructure. Zelensky refrained from accepting full responsibility for yesterday's drone attack on the Russian capital, but Ukrainian officials are

increasingly referring more explicitly to these events, which have stepped up notably in recent weeks, with four waves having struck the capital region this month.

5. **Crimea Attack Provokes Dangerous Escalation! Russia, For The 1st Time, Strikes At NATO's Doorstep; Hits Ukraine's Reni Port (The EurAsian Times, 26 JUN, Shweta Sengar)**

Inexorably, aerial warfare in Ukraine is escalating to a level where a NATO-Russia conflict appears inevitable. The dueling adversaries crossed two red lines in the past week, likely resulting in dangerous escalation.

On July 19, 2023, Ukraine crossed a red line when for the first time, it struck Crimea with the long-range UK-supplied Storm Shadow cruise missile.

In retaliation, on July 24, 2023, Russia crossed a red line when it struck Ukraine's Reni port on the Danube, close to Romania, a NATO state.

6. **Ukraine Strikes Back With Drone Attacks On Moscow, Crimea (The Drive/The War Zone, 24 JUL Thomas Newdick)**

Russia claimed two drones were brought down over Moscow, while Ukraine also launched a barrage of drones against targets in Crimea.

Russia has responded with predictable outrage after the latest Ukrainian drone strike on Moscow, with Kyiv promising more such attacks to come. As well as the Russian capital, Russian-occupied Crimea was the target of multiple drone strikes overnight. While Ukraine has prosecuted targets in Crimea and inside Russia before using drones, the latest wave of attacks is unusual in that President Volodymyr Zelensky had promised what he called "a retaliation to Russian terrorists for Odesa," after the Kremlin's forces struck the Ukrainian port city repeatedly in recent days.

7. **Trench Warfare In Ukraine Casts Old School Army Training In Different Light (The Drive/The War Zone, 21 JUL, Joseph Trevithick)**

The Army's trench warfare training may have seemed archaic in the past, but the war in Ukraine is serving as the latest reminder otherwise.

Combat engineers from the Georgia Army National Guard recently built a trench line to help train new recruits. Though the U.S. Army uses trenches in training evolutions and exercises, at first glance doing so may look like a throwback to time gone by. Sadly, that is not the case. In fact, their significance can be viewed with chilling clarity given the very active use currently of fortifications like this by both sides of the conflict in Ukraine.

8. **A Sobering Analysis Of Ukraine's Counteroffensive From The Front (The Drive/The War Zone, 20 JUL, Howard Altman)**

A military analyst just returned from touring the Ukraine front and has offered his blunt take on how the counteroffensive is really going.

Agroup of military analysts recently traveled to the front lines for a closer view of Europe's most brutal land war in several generations. Spending time with troops who've fought through massive Russian artillery barrages, helicopter and tank assaults, drone strikes and mine fields, one of them came back with a blunt assessment about why the counteroffensive is progressing slower than some anticipated.

Franz-Stefan Gady, a senior fellow with the Institute for International Strategic Studies and the Center for New American Security, says after his visit to Ukraine it's

clear the country is struggling with how to employ its forces. Once in the fight, they sometimes display poor tactics and a lack of coordination between units. All while having to cope with a still deeply entrenched bureaucracy, infighting and a continued reliance on “Soviet-style thinking.” Then there are the Russians, who are “putting up stiff resistance.”

9. **Russia Directly Targets Ukrainian Grain In Reprisal Airstrikes (The Drive/The War Zone, 19 JUL Howard Altman)**

The port city of Odesa was struck by another missile and drone barrage as Russia now threatens Black Sea shipping.

Ukrainian officials say 60,000 tons of grain was destroyed in the latest wave of Russian missile and drone attacks on and around the Black Sea port city of Odesa. The attack was tied to Russia's withdrawal from the Black Sea Grain Initiative, according to Ukrainian officials. That followed Ukraine's attack on the Kerch Bridge just days ago. The Kremlin has denied a connection and the Russian Defense Ministry (MoD) said it is hitting military targets.

10. **Captured Russian Weapons Being Studied By UK (The Drive/The War Zone, 18 JUL, Thomas Newdick)**

Disclosures about U.K. foreign materiel exploitation come as the government announces its future priorities for the armed forces.

Russian military equipment captured in Ukraine is being analyzed in the United Kingdom to help develop new weapons and tactics, the U.K. Ministry of Defense has confirmed. Russian armored vehicles are a particular focus of study, while new concepts developed in response to the war in Ukraine include a high-mobility vehicle armed with Brimstone anti-armor missiles, as well as infantry riding into battle on e-bikes while carrying recoilless rifles.

11. **Russia’s Kerch Strait Bridge Has Been Badly Damaged (Updated) (The Drive/The War Zone, 17 JUL, Howard Altman)**

The Kerch Bridge that connects Russia to Crimea was abruptly shutdown with claims of Ukrainian attack quickly following.

The Kerch Bridge, connecting Russia and the Crimean Peninsula has been closed after an incident in which portions of the bridge were damaged, according to Russian officials. Those officials are not saying what caused the damage, but Russian Telegram channels say the bridge was attacked by Ukraine.