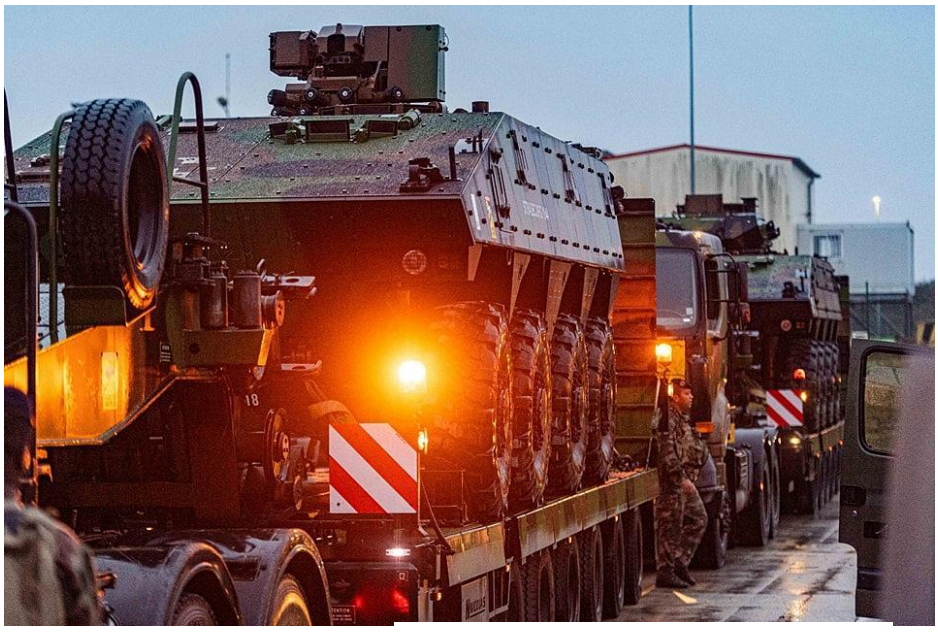
4 November 2022

An Analytic Intelligence Wire Prepared by The Students of Embry-Riddle Aeronautical University

Issue 416
Of Eagle Eye Intelligence

Authors

Jake S. Solomovici
Hayden Sapp
Brandon Hammer
Katie Larson
Jerome Lacaden
Haley Childress
Mason Meinzinger



Romania Insider

4 November 2022

Issue 416
Of Eagle Eye Intelligence

In This Issue

ROMANIA: Deployment of NATO Soldiers in Bucharest Likely to Deter Moscow

Summary: The North Atlantic Treaty Organization (NATO) allied forces, currently comprised of Paris, Ottawa, Brussels, Amsterdam, and other allied forces, stationed soldiers in Bucharest, which will likely deter Moscow's war efforts.

Development: On 26 October, NATO Secretary General Jens Stoltenberg stated, "Romania represents a valuable part of the Alliance, and NATO can defend the country if necessary." The Russia-Ukraine conflict turned the Black Sea into a warzone, implying the importance of Bucharest which borders the Sea and acts as a key location for NATO's ballistic missile site. In preparation for the battlegroup, Bucharest will host a formal meeting of foreign ministers from NATO member countries and other allies for the first time ever in a month. Bucharest also acquired fighter crafts from other countries like Paris and Madrid and considered purchasing the Jerusalem Iron Dome missile defense system. Bucharest will also host and train close to two hundred Ukrainian paramedics as part of a NATO program meant to bring relief to the war-torn country.

Analysis: The stationing of soldiers and military vessels will likely deter war efforts with Kyiv and Bucharest from Moscow. As a key point for NATO, Bucharest will likely act as a forward operating base for NATO operations. The statement of Stoltenberg will likely spark the start of a defensive allied war for the defense of Kyiv and Bucharest. If Moscow continues its forward assault and pushes to the Black Sea and Kyiv, NATO will likely begin to push Moscow's forces back, resulting in a turning point in the war. However, NATO will most likely not advance into Moscow until winter ends so as to not repeat past mistakes.

[Jake S. Solomovici]

INDIA: SQLite Patch Likely to Decrease Ransomware Attacks

Summary: The Hive ransomware group is exploiting a vulnerability in SQLite, exposing worldwide corporations to the threat of ransomware. News surrounding the attacks will likely increase awareness of the newest SQLite patch, decreasing attacks that exploit this vulnerability.

Development: On 26 October, the Hive ransomware group leaked data from Tata Power after it failed to pay ransom. The Russian-based ransomware group exploited vulnerabilities in SQLite, a lightweight database engine used commonly in websites, smartphones, and form-based applications. The group gained access to Tata's application by overflowing user input, causing the software to crash. The Hive ransomware group breached the data of Bell Canada, the German Mediamarkt, and Trinidad-based Massy Stores just this week by utilizing the CVE-2022-35737 vulnerability. Experts report that keeping packages utilizing SQLite up to date remains the best remedy for this vulnerability, as the latest patch disallows inputs larger than two gigabytes.

Analysis: The number of victims from the Hive ransomware group will likely decrease. The media presence, in conjunction with the patch for CVE-2022-35737, will likely reach enough system administrators, causing an increase in patched versions of SQLite. The Hive ransomware group will likely continue attacks on systems that don't have the SQLite patch installed.

[Hayden Sapp]

PAKISTAN: Backdoor Attack by Indian Hackers May Cause Increased Tensions

Summary: The Indian state-sponsored advanced persistent threat actor SideWinder, used a new backdoor attack through a malware named WarHawk to attack military entities in Pakistan. These attacks on military entities will likely cause a rise in tensions between the two countries.

Development: On 24 October, world news sources reported on a group of hackers called SideWinder committing backdoor attacks on Pakistani military entities. In the past, SideWinder has used various methods to attack businesses and military entities throughout Asia, focusing specifically on Pakistan. SideWinder typically uses a backdoor, or some other entrance point, to gain access into computers in its target organizations. SideWinder used this attack on Pakistani military entities as a way for New Delhi to figure out their future attack plans. Since the major Indo-Pakistani wars, New Delhi and Islamabad have maintained fragile relations. Starting in 2003, the two countries entered a cease-fire that has remained yet another point of conflict for the nations, with both sides regularly firing across the contested border and claiming that the other country fired first. Tensions between the countries continue to rise with increasingly deadly attacks such as airstrikes and terroristic attacks on the ground and an increase in cyber-attacks and espionage. The recently released reports on the use of backdoor attacks on Islamabad, using the WarHawk, further develop the seriousness of the conflict between India and Pakistan in both the physical and cyber realm.

Analysis: Cyber-attacks on Pakistani military entities by the Indian state-sponsored persistent threat actor SideWinder, will most likely cause a rise in tension and conflicts between the two countries. Cyber-attacks on Islamabad will almost certainly lead to retaliation against New Delhi. New Delhi will likely use the stolen information to plan attacks on the border between India and Pakistan.

[Brandon Hammer]

RUSSIA: Economic Partnership with Tehran Could Increase Economic Instability

Summary: Moscow and Tehran seek to strengthen energy cooperation ties through Tehran's promise of 40 turbines to aid Moscow's energy sector. Despite the strengthened relationship, Moscow's economy may suffer more as a result.

Development: On 23 October, Tehran announced it would export Moscow 40 turbines. This action acts as a continuation of the deal between Moscow's PJSC Gazprom and Tehran's National Iranian Oil Company, promising energy cooperation considering the Western-imposed sanctions. Moscow and Iran make up two of the largest gas reserves in the world; however, conflict in Ukraine pushed Western nations into undermining Moscow's position in the energy market. Moscow and Tehran view energy cooperation as a vital necessity for their countries' economies and hope to form a long-term relationship. Tehran and Moscow have already begun trading military arms, drones, and weaponry in addition to the 40 turbines.

Analysis: Moscow's economy potentially could lose more than it gains through a partnership with Tehran. Moscow will probably seek to strengthen its military sector alongside its energy sector, which could mean an increase in military spending and an increase in the duration of the Ukrainian conflict. The economic implications of this include a less stable economy as military spending would continue to draw resources away from other areas of the Russian economy. Additionally, longer conflict with Ukraine would further strain the Russian economy due to Western sanctions and the prolonging of martial law in Russia.

[Kate Larson]

RUSSIA: Nuclear Power Plant a Likely Target Following Battle for Kherson

Summary: Moscow will likely destroy the Zaporizhzhia Nuclear Power Plant in Kherson, which could provide Moscow the opportunity to blame Kyiv for utilizing a nuclear deterrent in the conflict.

Development: On 23 October, Moscow accused Kyiv of planning to detonate a radioactive dirty bomb within the Russian-controlled Zaporizhzhia Nuclear Power Plant while pinning the blame on Moscow. In response to the accusations, Kyiv also accused Moscow of planning the same nuclear threat through a false flag operation, according to *Aljazeera*. Previously, Moscow made nuclear threats to Ukraine and its allies in early October, citing Western involvement as a direct interference. Following the evacuation of civilians along the Dnipro River, Russian forces fortified defensive positions in preparation for a large-scale battle in Kherson. The Russian-controlled Zaporizhzhia Nuclear Plant remains a prime target for both sides. Russian President Vladimir Putin claims nuclear weapons remain unnecessary despite the allegations made by Kyiv and its allies. Moscow also stated the power supply situation will improve for Ukraine only if Kyiv concedes to Moscow's demands, according *TASS*.

Analysis: Upon losing Kherson to Ukrainian forces, Moscow will likely retaliate by destroying the Zaporizhzhia Nuclear Plant using explosives. Moscow likely does not wish to start an all-out nuclear war with the West and may blame the destruction of the plant on Kyiv. Moscow could use the destruction of the nuclear plant to cripple Ukrainian energy infrastructure and place doubt on Ukrainian leadership. Moscow's attack strategy likely revolves around targeting Ukrainian energy resources. These attacks will certainly continue as winter approaches. Moscow likely falsified the dirty bomb accusations to link Kyiv's involvement to any future damages caused to the nuclear plant. The destruction of the Zaporizhzhia plant would render the area uninhabitable by both forces indicating Moscow will likely destroy it if Ukrainian forces succeed in driving out its forces. Moscow probably views the upcoming battle for Kherson as a last-ditch effort and will do anything to ensure it does not fall back into Kyiv's control.

[Jerome Lacaden]

PAKISTAN: Shooting of Journalist Likely a Deliberate Attack

Summary: The shooting of a Pakistani journalist likely acted as a strategic killing to punish him for his anti-military and anti-government messages.

Development: On 23 October, Pakistani journalist Arshad Sharif died after getting shot in Kenya. Nairobi claims that the shooting happened as a case of mistaken identity, according to *Indian Express.* Sharif's body returned home on 26 October after Pakistan Prime Minister Shehbaz Sharif promised to fast-track the process. Sharif fled to Kenya in August amidst death threats and court cases following controversial anti-military and anti-government reporting.

Analysis: Sharif's death likely occurred as a targeted attack. Islamabad may have asked Nairobi to deal with Sharif for it because of his controversial reporting and his fleeing the country. The death likely will bring more attention to Islamabad journalists in the future. The international attention that Sharif's death brought likely will lead to Islamabad journalists being safer in the future. Islamabad and Nairobi relations may improve because of Nairobi's willingness to send Sharif's body home.

[Haley Childress]

IRAN: Rhetoric On Baku Border Aggression Likely to Encourage Armed Conflict

Summary: Political opposition to the Turkic-Azerbaijani commerce route blocking Tehran's commerce into Armenia will likely enflame tensions in the region due to competing economic and political interests with Ankara for control of the Caucasus region

Development: On 22 October, Iranian Foreign Minister Hossein Amir-Abdollahian said that Tehran will not agree with any sort of territorial changes to nations within the Caucasus region. The border between Iran and Azerbaijan follows the Aras River where the Islamic Republic of Iran Armed Forces practiced river crossings and combined arms assaults in military exercises a couple days earlier. The phrase 'one nation, two states' accurately reflects Ankara and Baku's relationship, according to *Hurriyet Daily News*. The proposed commerce route between Azerbaijan and Turkey would block Iranian commerce into Armenia and beyond. Poor relations exist between Ankara and Tehran due to the proxy wars that pit their respective interests against each other in both Libya and Syria. Tehran targets $3 billion in trade with Yerevan, according to *Tasnim News Agency*. Tehran continually invests in Armenian energy infrastructure and delivery systems between the two nations. The ferocity of citizens protesting Tehran increases as demonstrated in the killing of two officers in the Islamic Revolutionary Guard Corps, according to *Iran International*.

Analysis: Tehran's domestic protests will likely increase in size and seek to uproot Tehran's system of power. This will likely push Tehran to engage in combat with Baku to protect its influence in the area from Ankara and divert the domestic population's attention away from the protests by tapping into the nationalism of Iranians. Tehran will likely defend its investments in Armenia by force as it will likely want to invest more funding in Armenia.

[Mason Meinzinger]

About GSIS

Embry-Riddle Aeronautical University's (ERAU) Bachelor of Science in Global Security & Intelligence Studies (GSIS) degree program at our Prescott Campus blends both academic and professional studies to equip students with the knowledge and skills necessary to become future leaders in intelligence, security, and law enforcement. The program provides students with a sound foundation in the liberal arts, including international relations, foreign languages and cultures, international law, foreign policy, political and military history, and other essential topics.

About EE

Eagle Eye Intelligence (EE) is an intelligence and research organization led by the students of the GSIS program at ERAU in Prescott, Arizona.

Dr. Philip E. Jones founded EE and Embry-Riddle's GSIS program in 2002, following a career with the Central Intelligence Agency and consulting work in international development and global security. Currently, Professor Dale R. Avery, a former career intelligence analyst, serves as EE's faculty advisor.

EE strives to provide actionable intelligence and analysis to its customers during the academic year. We are driven by a number of goals – continuous development, nonpartisanship, interdisciplinary studies, global awareness, and professionalism.

EE does not cite sources in the final publication; however, we log every source we use in our research and are happy to share them upon request. The official EE Source Database is available on our website's resources page for a general overview of our sourcing methods.

The views expressed in this publication are those of the authors, and do not represent the position Embry-Riddle Aeronautical University or the College of Business, Security, and Intelligence.

Savannah Gallop, a junior in the GSIS program, currently serves as EE's Editor in Chief. For questions or comments, contact the team at editorsee@gmail.com or Professor Avery at 928.777.4708. If you use material from this publication, you should attribute: Eagle Eye Intelligence Edition 416, a publication created by students at Embry-Riddle Aeronautical University in Prescott, Arizona.

Eagle Eye Intelligence
3700 Willow Creek Rd.
Prescott, AZ 86301
eagleeyeintel.com