2 February 2024

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

Issue 444
Of Eagle Eye Intelligence

Authors

Markus Weinzinger
Lauren Estrada
Sebastien Bragg

Associated Press Photos

2 February 2024

Issue 444
Of Eagle Eye Intelligence

In This Issue

MALI: Broken Peace Deal Will Likely Augment Internal Security Strategy

Summary: The dissolution of a peace deal will likely enhance Bamako's capabilities and influence against internal rebel groups.

Development: On 25 January, Bamako spokesperson Colonel Abdoulaye Maiga announced the termination of the 2015 peace deal with Tuareg rebel groups. Bamako based this decision on rebel violations of peace deal terms and Algiers's perceived hostility, according to AP News. Part of the peace deal allowed for more autonomy for the rebel groups in Mali, according to Deutsche Welle. This came about a month after Bamako summoned Algier's ambassador regarding allegations of interference in Bamako's internal affairs, according to Barron's. Algiers's Ministry of Foreign Affairs affirmed the breakdown but stated a "duty to provide information to our brother Malian people." On 26 January, Bamako outlined a new decree to establish a committee for organizing peace and reconciliation talks, according to Reuters.

Analysis: Bamako will likely escalate its actions to reacquire its northern territory with the dissolution of the peace treaty. The absent peace deal will most likely remove autonomy for the Tuareg groups and deter neighboring states from challenging the policy change. Despite Algiers's warm diplomatic stance, Bamako will likely pursue an exclusive campaign against the Tuaregs. The new decree will likely permit Bamako to gain more concessions in peace talks and secure more influence in its region of the Sahel.

[Markus Weinzinger]

CHINA: Malware Likely in Testing Phase Before Advancing Towards the West

Summary: An advanced persistent threat actor (APT) will likely continue advancing its malware in China, Japan, and the United Kingdom before targeting organizations and individuals in other Western nations.

Development: On 24 January, reports released information on a China-linked APT, named Blackwood, deploying the NSPX30 backdoor in system software updates. Threat actors utilize backdoors to traverse through cybersecurity measures to reach higher user access in the system. Investigations previously linked Blackwood to adversary-in-the-middle attacks to implement NSPX30 in replacement of software updates, according to Infosecurity Magazine. Every device updates its software, but more frequently in large network systems. When implemented, the backdoor can collect file information, take screenshots, log keystrokes, kill processes, and uninstall itself, according to *Ooda Loop*. Observations of the backdoor revealed it targeted Chinese and Japanese manufacturing and engineering facilities, according to The Hacker News.

Analysis: Blackwood's target history likely indicates a testing phase of the backdoor before advancing to larger organizations. Blackwood's methodology indicates it most likely will target commercial companies due to its ability to implement the backdoor through system software updates. Due to the West having a large population with modern technology and system software, Blackwood likely aims to target Western companies after it advances its backdoor with thorough attacks in other nations.

[Lauren Estrada]

NORTH KOREA: Cruise Missile Range Likely Limited by Poor Ship Detection Support

Summary: Pyongyang's most recent cruise missile tests likely show how Pyongyang intends to use multiple cruise missiles. These missiles integrate complex flight paths intended to compensate for a critical lack in ship detection equipment at the cost of range.

Background: On 30 January, Pyongyang launched a series of cruise missiles from the western Sinpo Port into the sea, making it the third cruise missile test of 2024. The Korean People's Army (KPA) fired several KN-01 and KN-19-class anti-ship cruise missiles. Both missiles launch from either the ground or the sea and occupy an estimated 150-mile range. The KN-01 uses an active radar seeker and an infrared homing system which track a target's radar or heat emissions respectively. The KN-01 further possesses the ability to pre-program coordinates into its flight plan to avoid obstacles like terrain and air defense systems. The KN-19, a more modern missile than the KN-01, features additional navigation systems such as a form of GPS tracking along with the same tracking systems as the KN-01.

Analysis: Pyongyang's recent cruise missile tests show that the KPA most likely lacks the support equipment required to detect hostile ships, limiting the effective range of its anti-ship cruise missiles. Both the KN-01 and KN-19 would need to rely on the ship's radar to detect incoming hostile ships, almost certainly limiting the effective range of the missiles to under 150 miles. Ground-based missile launchers almost certainly limit the effective range of the cruise missiles to visual range, with no viable naval detection systems to direct where to fire the missile beyond visual range. Pyongyang likely intends to combat the lack of detection equipment by launching multiple cruise missiles pre-programmed with extra maneuvers to increase the likelihood of finding hostile ships. The most recent missile tests possibly confirm this strategy. The extra maneuvers required to complete this search pattern almost certainly will limit the range of the cruise missiles due to a potential loss of energy when making additional turns.

[Sebastien Bragg]

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.

Sebastien Bragg, 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 444, 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