18 September 2026

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

Issue 500
Of Eagle Eye Intelligence

Authors

Armaan Needles
Cade Cunningham
Christina Muchow
Garrett Williams
McKenzie Koliba

18 September 2026

Issue 500
Of Eagle Eye Intelligence

In This Issue

AFRICA: Stronger Military Response Unlikely to Dampen Islamist Insurgencies 1

CHINA: Increased Vehicle Exports Likely Indicate Efforts to Reduce Economic 5
Stress

IRAN: War Dissatisfaction Almost Certainly Not Leading to Public Dissent 6

NORTH KOREA: Cyber Operations Will Likely Target Trusted South Korean 8

Systems

SUDAN: Foreign Support Will Likely Prolong War Between Military Groups 11

AFRICA: Stronger Military Response Unlikely to Dampen Islamist Insurgencies

Summary: Islamist insurgencies across Sub-Saharan Africa will likely continue to intensify and expand geographically over the next six months despite African governments' turn toward harder military responses and new security partnerships, because the governance failures and security-force abuses that drive recruitment remain largely unaddressed. Bamako's collapsing Russian-backed security arrangement to the Gulf of Guinea coast, where insurgents are opening entirely new fronts, likely demonstrates this pattern.

Background: The Global Terrorism Index 2026, published by the Institute for Economics and Peace, identifies Sub-Saharan Africa as the world's foremost center of terrorism, with six of the 10 most-affected countries worldwide located on the continent and the Sahel alone accounting for more than half of global terrorism deaths in 2025. Four distinct insurgencies drive this trend. In the Sahel, Jama'at Nusrat al-Islam wal-Muslimin (JNIM), al-Qaeda's regional affiliate, and the smaller Islamic State Sahel Province contest territory across Mali, Burkina Faso, and Niger. In the Lake Chad Basin, Boko Haram and its rival, Islamic State West Africa Province (ISWAP), continue a decade-long feud alongside their campaign against government forces in Nigeria, Chad, Cameroon, and Niger. In Somalia, al-Shabaab, al-Qaeda's largest and best-funded affiliate, wages a war of attrition against Mogadishu and allied African Union forces. In the Democratic Republic of the Congo (DRC) and Mozambique, the Islamic State Central Africa Province (ISCAP) runs two geographically separate but formally linked insurgencies. Despite differing affiliations, leadership, and terrain, each of these movements has expanded its reach or reversed government gains within the past year.

Security Partnerships Underdeliver: Bamako's experience with Russian security assistance almost certainly demonstrates that harder military partnerships have not translated into territorial control. Moscow's Wagner Group withdrew from Mali in June 2025 after declaring its mission accomplished, handing responsibility to the more centrally controlled Africa Corps. Eleven months later, on 25 April, JNIM and the Tuareg-led Azawad Liberation Front launched coordinated attacks against Bamako, Kati, Kidal, Gao, and Mopti in the largest offensive Mali has faced since 2012. A suicide car bombing killed Malian Defense Minister General Sadio Camara at his residence in Kati, and separatist forces seized Kidal, a town Russian-backed units had spent years recapturing. JNIM separately blockaded fuel shipments into Bamako earlier this

year, choking the capital's supply lines. This pattern recurs outside Russian-linked contexts. In the DRC, a joint offensive between Kampala and Kinshasa, Operation Shujaa, has pushed ISCAP out of several strongholds, yet the group adapted by relocating operations north to Haut-Uélé Province and striking a Chinese-owned mining site in March 2026, which likely demonstrates expanding reach rather than defeat. The recurrence of this dynamic across two unrelated security partnerships, one Russian and one regional African, indicates that battlefield pressure alone is not translating into durable territorial control, but rather that present military action is almost certainly insufficient to counter Islamist terrorism's spread.

Governance Failures Fuel Recruitment: Battlefield operations that fail to address governance failures are likely entrenching rather than diminishing these insurgencies. The Global Terrorism Index attributes this pattern to conditions on the ground: 71% of recruits across Sub-Saharan Africa cited abuses by state security forces, rather than ideology, as their reason for joining an extremist group, and roughly a quarter cited the complete absence of employment opportunities. Mali's experience illustrates the mechanism directly. Human Rights Watch's initial investigation found that Malian and Wagner Group forces summarily executed roughly 300 people over a five-day operation in the central town of Moura in March 2022. A subsequent investigation by the UN Human Rights Office concluded that Malian and Wagner Group forces had killed at least 500 people, and it documented dozens of cases of sexual violence against women and girls. Bamako has consistently denied these findings and refused investigators access to verify them independently. Somalia's experience offers a parallel case, built on a different failure. Mogadishu's 2022 counteroffensive succeeded initially by incentivizing clan militias, known as macawisley, to fight alongside government forces. The arrangement collapsed once al-Shabaab targeted the same communities for collective punishment, and the group's February 2025 counteroffensive erased nearly all of the government's territorial gains within months. Data from the Hiraal Institute shows al-Shabaab's targeting of civilians surged by 306% following the government's offensive, alongside a 1,764% rise in attacks on Somalia's elite Danab and Gorgor forces. In both cases, tactical military success did not produce lasting security, almost certainly because it did not resolve the governance failures driving local populations toward, or away from, cooperation with the state.

Insurgencies Spread Beyond Traditional Strongholds: The clearest evidence that containment is almost certainly failing is geographic: all four insurgencies have expanded into territory outside their historical strongholds within the past two years. JNIM has pushed south from the Sahel into northern Benin and Togo, territory that saw only isolated violence before 2021. Attacks recorded in northern Benin rose from 22 in 2021 to 176 in 2024, and deaths more than doubled from 52 to 131 over the same period, according to Armed Conflict Location and Event Data Project (ACLED) figures. JNIM claimed responsibility for killing 70 Beninese soldiers in a single raid on two military posts, its largest claimed death toll in over a decade of activity in the country. United States Africa Command's commander has separately described JNIM and its affiliated groups as actively “metastasizing” toward the borders of Côte d'Ivoire, Ghana, Togo, and Benin, countries that had not previously experienced sustained jihadist violence. The same dynamic is unfolding in Central Africa, where ISCAP has moved beyond its historical base in eastern DRC's North Kivu Province into Haut-Uélé Province and intermittently into Mozambique's Niassa Province, well outside Cabo Delgado, its original stronghold. Neither expansion likely reflects a coordinated continental strategy; rather, each group is likely exploiting the same conditions independently, to open new fronts as pressure mounts in their core territory: porous borders, thin state presence, and communities that have received little benefit from existing counterinsurgency campaigns.

Outlook and Implications: These four insurgencies will likely continue to expand geographically and resist military containment over the next six months, because none of the responses currently in place - Russian security partnerships, regional joint offensives, or government counteroffensives built on local militias - address the governance failures and security-force abuses that the Global Terrorism Index identifies as the primary recruitment driver across the continent. In the Sahel, Bamako will likely continue to lose ground to JNIM and allied separatist forces absent a fundamental change in Africa Corps' approach, since Moscow's security model has so far prioritized territorial recapture over the accountability measures that could reduce recruitment. Continued attacks on the capital's fuel supply raise the possibility of a more direct siege of Bamako itself. This trajectory will probably reinforce, rather than dispel, growing regional skepticism of Moscow's security-partnership model, potentially creating an opening for other external actors seeking influence in Mali, Burkina Faso, and Niger. In coastal West Africa, JNIM's push into Benin and Togo will likely continue over the same period,

probably prompting further military mobilization by the governments of Benin, Togo, Côte d'Ivoire, and Ghana and raising the risk that instability spreads to states whose economies depend heavily on regional trade and tourism along the Gulf of Guinea. Central Africa's multinational response has, however imperfectly, slowed ISCAP's spread; coastal West Africa has no comparable coordination at all. This absence of any regional response makes the Gulf of Guinea expansion more likely to continue unchecked in the near term.

An alternative explanation, that this apparent expansion partly reflects improved conflict-monitoring coverage rather than genuine operational growth, is less likely given the specificity of the evidence: the capture of a named town, the assassination of a sitting cabinet minister, and a claimed attack on a foreign-owned mine are discrete, verifiable events that a monitoring-coverage explanation alone cannot account for. Across all four theaters, continued reliance on military solutions without addressing the drivers the Global Terrorism Index identifies will almost certainly limit the durability of any territorial gains, regardless of which security partner or tactic a given government employs.

[Armaan Needles]

CHINA: Increased Vehicle Exports Likely Indicate Efforts to Reduce Economic Stress

Summary: Beijing's efforts to increase global vehicle exports during a slump in domestic sales likely indicate an effort by the Chinese Communist Party (CCP) to reduce domestic economic stress.

Development: As of 10 September, Beijing's vehicle exports so far this year have exceeded the total number exported last year, according to AP News. On 31 August, reports indicate that domestic sales fell by 25.6%. This occurred directly after Beijing experienced one of its weakest quarterly growth rates ever, according to the Guardian. This comes during a global boom for electric vehicle (EV) exports and technology as falling manufacturing prices, increasing infrastructure support, including charging and repair capabilities, and government incentives and regulations influence this boom. In 2025, global EV sales increased by 20%, according to the International Energy Agency.

Analysis: Beijing increasing global vehicle exports after experiencing weak domestic sales and low economic growth likely indicates an effort by the CCP to offset domestic economic stress by exporting domestic vehicles. By increasing exports, Beijing likely aims to maintain the profitability of the vehicle industry despite a weak domestic market. Beijing is also likely targeting the EV market during the current boom to ensure profitability. Additionally, Beijing likely wants to increase exports to allow domestic vehicle manufacturers to continue producing at the high rate the economy needs to sustain itself. These exports likely also open the door for additional foreign markets that would further stimulate Beijing's economy, making them critical to reducing future economic stress.

[Cade Cunningham]

IRAN: War Dissatisfaction Almost Certainly Not Leading to Public Dissent

Summary: Despite widespread economic hardship and large segments of the Iranian public's opposition to the regime, public dissent remains extremely limited. The economic and political consequences of the Iran War will almost certainly not lead to a serious threat to the regime's viability, and Tehran's fear of appearing vulnerable to its domestic and international opponents will likely motivate it to reject peace proposals despite the war's consequences.

Background: By about 18 January, a violent crackdown by Iranian security forces, coupled with an internet blackout, caused the end of several weeks of large-scale protests against the regime motivated in large part by economic concerns, according to ABC News. Security forces killed over 3,000 people and arrested nearly 25,000 during the crackdown. The US-Iran War has caused significant economic downturn within Iran, including significantly increased unemployment and 88% inflation, although Tehran's policies have limited the amount of data available, according to NPR and Trading Economics. However, since the start of the Iran War on 28 February, these large-scale protests have not resumed, nor have militant opposition groups such as Kurdish forces participated in the war, according to The Guardian and Al Jazeera.

Intimidation Against Dissidents: Despite relatively low opposition activity since the end of large-scale protests in January 2026, the regime has maintained significant pressure, making the reignition of widespread protests highly unlikely despite worsening economic and humanitarian conditions. Tehran has maintained its crackdown, executing at least 532 people in 2026 in connection with the protests, arresting more than 6,000 people, and seizing at least 240 people's assets, according to Euronews. Furthermore, the regime deployed Basij and Law Enforcement Command units across the country on 7 September, coinciding with a gas price increase, according to the Institute for the Study of War (ISW). Islamic Revolutionary Guard Corps (IRGC) special operations units that have participated in previous protest crackdowns also conducted recent trainings publicized by the regime-linked Fars News on 10 September, according to the Institute for the Study of War. The magnitude of the regime's ongoing repression is almost certainly acting as a significant barrier to anti-regime protest activity, despite economic conditions. The security forces' mobilization and willingness to utilize deadly force will almost certainly continue to preempt meaningful attempts to force reforms.

Limited Official Dissent: High-ranking members of the Iranian government have consistently expressed commitment to continuing the war, even amidst acknowledgement of its economic costs, likely indicating that regime hardliners maintain full control over the government. On 11 September, Iranian President Masoud Pezeshkian stated, "I am not in favor of continuing the war, but we must strengthen the country's resilience in the face of upcoming developments," to avoid having to negotiate from a "position of weakness," according to Anadolu Agency. Iranian Parliamentary Speaker Mohammad Bagher Ghalibaf similarly vowed to resist economic pressure despite acknowledging significant hardships. Ghalibaf and Pezeshkian have both called for negotiations and an end to the war, but they likely exercise almost no control over Iranian military policy. Rather, regime hardliners, especially those within the IRGC, almost certainly exercise full control over military and diplomatic decision-making. The limited nature of Pezeshkian and Ghalibaf's statements likely indicates the extent of allowed dissent by elected officials within the regime and demonstrates the control exercised by the anti-concessions camp.

Outlook and Implications: Given Tehran's extensive ongoing crackdown against dissidents and hardline consolidation of control over the government since the start of the Iran War, discontent over the war and its economic and social impacts will almost certainly not lead to regime change or meaningful reform. Regime hardliners almost certainly control all aspects of Tehran's foreign and domestic policies and will likely not accept a negotiated peace despite the economic hardship facing the country out of fear of appearing vulnerable to its domestic opponents. Tehran's fear of appearing vulnerable and facing a renewed existential threat in the form of large-scale internal opposition will almost certainly drive it to maintain its crackdown for the duration of the war and its associated economic consequences. Given the risk of detection, persecution, and death, protests are highly unlikely to reignite while the security forces remain deployed.

[Christina Muchow]

NORTH KOREA: Cyber Operations Will Likely Target Trusted South Korean Systems

Summary: North Korean-linked cyber groups will likely continue to target South Korean government and civilian organizations by exploiting software, websites, and authentication systems that users already trust. In 2026, activity connected to the Lazarus Group and Kimsuky affected hospitals, media outlets, companies and other institutions. Hackers used software vulnerabilities, malware, compromised websites, phishing and credential theft to gain access to systems. The growing overlap between state-linked hacking and ransomware will likely make future attacks harder to identify and contain. Hackers will likely continue targeting commonly used technology because a single compromise can provide access to multiple organizations.

Background: On 20 August, South Korean police reported that a hacking campaign believed to be connected to the Lazarus Group affected over 101 South Korean institutions, including hospitals, pharmaceutical companies, news organizations and a server management firm. Investigators linked the activity to North Korea because malware recovered during the attacks resembled code previously associated with Lazarus, according to Seoul Economic Daily. However, police stated that final attribution will require further investigation. Hackers also breached a private certification authority in February and stole personal information belonging to important South Koreans, including information belonging to at least one senior Presidential Office official. Police said the hackers did not directly compromise the Presidential Office's internal server. Investigators believe the hackers used watering hole attacks, which infect websites frequently visited by intended targets and then attempt to compromise visitors. South Korea also reported 1,236 cyber intrusions during the first half of 2026, a 19.5% increase from the same period in 2025.

Growing Link Between Ransomware Groups: On 30 July, four South Korean security and intelligence agencies warned that cyberattack tools and infrastructure associated with Lazarus appeared alongside the Gunra ransomware operation, likely indicating a growing link between ransomware groups According to The Record, AhnLab researchers found that Lazarus and Gunra exploited the same vulnerabilities in Korean financial security software that banks and government services commonly require. Lazarus-linked hackers used the access to install espionage backdoors in at least 72 organizations during 2026, including government agencies, cryptocurrency exchanges and information technology service providers. Gunra used similar

access to encrypt files, steal information and demand ransom payments. The similarities went beyond the initial vulnerabilities. AhnLab found identical malware filenames, execution commands, privilege escalation tools and more. Researchers assessed a high likelihood of technical linkage, but they did not determine whether Lazarus and Gunra were directly cooperating. The overlap could also have resulted from shared infrastructure or one group providing access to another. An organization compromised through the same vulnerability could face different consequences, depending on which attacker controls the access. Lazarus is likely seeking long-term intelligence collection, while ransomware groups more often focus on stealing information and disrupting operations for payment.

Cyber Attacks Targeting Various Websites: North Korean cyber operators will likely continue compromising legitimate websites because users are less likely to suspect websites they regularly visit. Attackers compromised 15 legitimate Korean websites across several industries and used them for watering hole attacks, according to The Record. Attackers redirected selected visitors to infrastructure that exploited vulnerable security software and injected malicious code into legitimate computer processes. Researchers also discovered that the same Korean website development company managed several of the affected websites. AhnLab assessed that hackers may have compromised a management system and then expanded into client websites rather than attacking every website separately. This approach gives hackers an opportunity to reach multiple victims through one successful compromise. It also creates risks for organizations not specifically selected as targets because employees may encounter infected websites during normal activity. The campaigns did not rely only on compromised websites. Attackers also conducted spearphishing operations, including a campaign against a South Korean defense company. Using several methods at once gives North Korean operators more options if defenders block one path into a network, almost certainly increasing the hacker's likelihood of success.

Government Authentication Remains a Major Target: North Korean-linked hackers will likely continue targeting authentication systems because stolen credentials can provide access without repeatedly exploiting a network. On 14 May, Kaspersky reported that Kimsuky was developing malicious software targeting South Korea's government electronic authentication system. Researchers connected the HelloDoor backdoor to Kimsuky and found that the group's AppleSeed malware was primarily used to extract information from the authentication system

used on government servers, according to Yonhap News Agency. Kaspersky warned that stolen authentication information could allow hackers to hijack accounts and enter internal government systems. Kimsuky has also changed how it establishes remote access. Kaspersky reported that the group began using Visual Studio Code Remote Tunneling instead of relying on traditional malware to connect to victim computers. Researchers also found signs that artificial intelligence may have assisted in HelloDoor's development, including code comments and debugging information that appeared to have been produced by a large language model. These developments could help Kimsuky adjust its tools while still maintaining its focus on South Korean government organizations. More importantly, stolen authentication information could remain useful even after defenders remove malware from an infected computer if compromised accounts are not identified and secured.

Outlook and Implications: North Korea-linked hackers will likely continue combining software exploitation, compromised websites, phishing, malware and credential theft to target South Korea. North Korean hackers will likely continue exploiting widely used security software because vulnerabilities in one product can expose numerous organizations and individual users. Hackers will almost certainly continue to target hospitals, news organizations, technology companies, pharmaceutical companies, service providers, government authentication systems, and financial security software that can hold valuable information or provide a path into other networks. The use of common financial security software and trusted websites increases the number of organizations that could become exposed through a small number of initial compromises. The overlap between Lazarus-linked activity and Gunra ransomware operations will also likely complicate future investigations, as the same vulnerabilities and infrastructure can support espionage or ransomware, making an attacker's purpose unclear during the early stages of an intrusion. North Korea will likely continue targeting trusted technology and third-party services because these systems give its hackers opportunities to reach more victims while also reducing the need to attack every organization directly.

[Garrett Williams]

SUDAN: Foreign Support Will Likely Prolong War Between Military Groups

Summary: As foreign support continues providing weapons and personnel to the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF), the war will likely continue without a ceasefire. Both sides likely have the resources to continue causing destruction in hope of retaining power. Drone attacks have destroyed cities, homes, schools, that have displaced millions of citizens and causing a humanitarian issue in Sudan. The conflict will likely remain unstable, and the war will likely continue to displace citizens.

Background: On 3 September, the United Nations Independence Fact-Finding Mission released a report discussing how foreign aid is fueling the conflict between the SAF and RSF, according to Jurist News. Foreign actors have contributed to supplying drones and weapons, which have added to civilian fatalities in the Sudan War. On 15 April 2023, the civil war broke out due to a power struggle between the army, SAF, and paramilitary group RSF, according to the BBC. SAF leader Gen Abdel Fattah al-Burhar and RSF leader Gen Mohamed Hamdan Dagalo had worked together in a joint military-civilian government to help remove President Omar al-Bashir of Sudan in 2019. After the removal of President Bashir, the leaders of the SAF and RSF initially agreed to merge into one military group before leadership conflicts ignited. Now, the country has faced drone attacks that have displaced over 14 million people and left two-thirds of the citizens in need of humanitarian support, according to International Rescue Committee.

Foreign Support Strengthens Both Sides: The war will likely continue if foreign support does not cease. Investigations have documented Colombian military contractors deploying to operate drones and advance weapons to help the RSF, according to Al Jazeera. Additionally, reports surfaced of Abu Dhabi supplying weapons to the RSF via Chad, Libya, and Somalia. Though the SAF has also secured support from Egypt, Saudi Arabia and many national militias have helped build Burhar's manpower. Furthermore, the usage of advanced weapons will most likely increase the fatality count and prolong both the RSF and SAF operations by providing weapons of destruction. As both sides have assembled more personnel and weaponry, the country will likely remain divided.

Foreign Supplies Increase Civilian Suffering: SAF and the RSF have acquired more supplies from allies that will likely increase civilian harm. Recently drone use has taken the war to new levels of conflict, damaging electricity, fuel, water, and transport systems, along with health care

and schools, according to Jurist News. RSF launched multiple drone attacks in Kalogi, South Kordofan, reportedly killed 114 people, as well as attacks in Ad-Da'ein, East Darfur, demolishing a hospital. Around 150,000 people have died, and many women and girls have suffered sexual violence due to both military groups, according to International Rescue Committee. Both sides have drones available to them, which most likely gives them more ground to cover, putting more civilians at risk. In addition, much of this war has destroyed homes, schools, and hospitals, and many women and children have fled to surrounding countries. This war has devastated communities all over Sudan and will almost certainly continue to do so if more weapons become available.

Outlook and Implications: The Sudanese war will likely not resolve until foreign support decreases, as such support has helped expand the SAF and RSF weapon capabilities. The increase of drones in the war has likely provided both sides significantly increased capabilities. Given the military benefits associated with drone use, the prevalence of drone will likely increase. Both factions will almost certainly continue to commit war crimes, and the cost to the civilian populace will likely continue to increase. Neither faction in the war is likely to accept a compromise while they maintain the ability to fight, as both leaders almost certainly seek to maintain and expand their power.

[McKenzie Koliba]

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.

Christina Muchow, a Senior 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 500, a publication created by students at Embry-Riddle Aeronautical University in Prescott, Arizona.

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