20 November 2026

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

Issue 509
Of Eagle Eye Intelligence

Authors

Christina Muchow
Hunter Varin
Isabella Cantwell



20 November 2026

Issue 509
Of Eagle Eye Intelligence

In This Issue

AFGHANISTAN: Beijing Very Unlikely to Expand Relations Amid Instability 1

RUSSIA: Cyber Operations Against European Allies Will Likely Undermine 2

Security

RUSSIA: Likely Seeking Sustainability for Current and Future Military Ambitions .. 3

AFGHANISTAN: Beijing Very Unlikely to Expand Relations Amid Instability

Summary: Despite Kabul's almost certain interest, Beijing remains very unlikely to expand the two countries' trade relations due to security risks and a lack of economic or political incentives.

Development: On 4 October, Kabul commemorated the opening of a road through the Wakhjir Pass leading to the closed Afghanistan-China border, according to *Al Jazeera.* The new road comes amid the near-total closure of the Afghanistan-Pakistan border and clashes between the two countries, including clashes on 5 November, according to the Long War Journal and Voice of America. Islamabad claims that Kabul is harboring Islamist militants conducting attacks in Pakistan, according to the Long War Journal. This follows multiple militant crossings from Afghanistan into Tajikistan in December 2025, as well as targeted attacks on Chinese nationals in Afghanistan in January, according to the Jamestown Foundation and the BBC.

Analysis: Despite Kabul's almost certain interest, Beijing will very likely not expand its trade relations with the country due to the large security risks and low probability of significant economic gains or expanded regional influence. Kabul's recent actions reflect that it almost certainly desires a genuine expansion in its trade relations with other partners, including Beijing, to improve its economic condition amid the ongoing clashes and closure of the Afghanistan-Pakistan border. Beijing will very likely not significantly expand its economic or political ties given high security risks. This almost certainly includes both the security risks within Afghanistan as well as the risk of Afghan-based militant crossings and attacks into Chinese territory if the borders are loosened, as has occurred in Pakistan and Tajikistan. Beijing would likely not gain significant economic advantages if it expanded trade, compared to other potential partners with greater security and political stability, although it would provide Beijing with an alternative route to reach Iran. Beijing would almost certainly not gain significant geopolitical advantage from expanding its trade relations with Kabul prior to security consolidation, as Kabul largely remains a pariah state, limiting its broader international and regional influence considerably, and Kabul would likely not significantly alter its policy to Beijing's interests given the likelihood of backlash from the hardline Islamists within the country. This lack of economic or political benefit, coupled with significant security risks, makes it highly unlikely that Beijing will respond to Kabul's overtures.

[Christina Muchow]

RUSSIA: Cyber Operations Against European Allies Will Likely Undermine Security

Summary: Moscow will likely continue targeting European government institutions, defense organizations, and critical infrastructure through cyber operations. Russian state actors will likely prioritize government networks, research institutions, and NATO organizations to collect intelligence and undermine support for Kyiv. These operations will likely threaten sensitive information, essential services, and economic security. However, stronger cybersecurity cooperation and intelligence sharing will likely limit Moscow's operational effectiveness.

Background: Moscow has a history of conducting cyber operations against European governments and organizations, using espionage, disruption, and network exploitation to advance its strategic objectives. Hours before the 24 February 2022 invasion, Moscow launched a cyberattack on the KA-SAT satellite communications network, disrupting Ukrainian military and civilian communications. Alongside the satellite attack, Russian actors conducted website defacements and deployed IsaacWiper, a destructive malware designed to erase data by overwriting hard drives, against Ukrainian government, energy, and financial portals, according to the European Union. More recently, cyber operations have incorporated information warfare tactics, such as SMS intimidation campaigns, deepfakes, and persistent distributed denial-of-service (DDoS) attacks, intended to undermine public confidence and civilian morale, according to EclecticIQ. These activities demonstrate how cyber operations can complement conventional military action as part of broader hybrid campaigns.

The sustained pressure on Ukraine has prompted substantial assistance from European allies, including the European Union (EU), Berlin, and London. Since the beginning of the invasion, the EU and its 27 member states have mobilized approximately $226 billion in military assistance, financial support, humanitarian aid, and support for Ukrainian refugees, according to the European External Action Service. Additional assistance has included emergency energy supplies, electricity generators, and funding for the restoration of damaged infrastructure, according to the European Commission. European countries supporting Kyiv have also faced Russian cyber activity, with Russian threat actors targeting government organizations and other sectors across the region.

Russian Cyber Operations Target European Government and Defense Organizations: Russian-linked cyber actors have increasingly targeted European government institutions,

defense organizations, and private-sector entities to collect intelligence and will likely disrupt continued support for Kyiv. Microsoft's 2025 Digital Defense Report identifies the United Kingdom as the second most targeted country by Russian nation-state actors, accounting for 12% of reported targeting. Germany follows at 6%, Belgium at 5%, and Italy, Estonia, France, the Netherlands, and Poland each account for 3%. Microsoft also reports that all ten countries most affected by Russian cyber activity outside Ukraine belong to NATO, representing a 25% increase compared with the previous year. These findings demonstrate the geographic reach of Russian cyber operations and the exposure of European countries supporting Kyiv. This pattern suggests that will likely continue using cyber operations to collect intelligence on NATO governments and defense organizations, particularly as European support for Kyiv persists. Although Ukraine remains the primary focus of Russian state actors, Moscow's expanded targeting of NATO members provides additional opportunities to collect intelligence on European governments, defense organizations, and their support for Kyiv.

Critical Infrastructure and Essential Services Remain Potential Targets: European energy, transportation, and telecommunications infrastructure remains susceptible to cyber operations that will likely disrupt essential services and impose economic costs on affected countries. Microsoft's 2025 Digital Defense Report identifies government organizations as the most frequently targeted sector, accounting for 25% of Russian nation-state targeting. Research and academia and think tanks/NGOs each account for 13%, while IT organizations account for 10%. Energy accounts for 5%, followed by defense industry, manufacturing, and transportation at 3% each. These findings demonstrate that Russian state actors target organizations across sectors that support government operations, economic activity, and national security. Given this broad targeting pattern, Russian-aligned actors will likely continue probing sectors that support essential services, creating opportunities for disruption even when not primarily targeting infrastructure. Separately, the European Union identified Russian-linked cyber groups responsible for attacks against critical infrastructure, including a December 2024 attack against a Danish water utility by the pro-Russian group Z-Pentest. The EU also attributed sustained DDoS campaigns against government agencies, financial institutions, media organizations, and critical infrastructure to the Cyber Army of Russia Reborn (CARR), which it links to the Russian military intelligence agency GRU. These incidents almost certainly demonstrate that Russian-

aligned actors can disrupt essential services and impose costs on European countries without directly engaging their military forces.

European Cybersecurity Cooperation May Limit Russian Operations: European cybersecurity cooperation and intelligence sharing will likely constrain some Russian cyber operations by improving threat detection, incident response, and collective defense capabilities. NATO and the EU have strengthened cooperation to identify, attribute, and respond to Russian cyber operations targeting European governments and critical infrastructure. In July 2025, NATO publicly attributed malicious cyber activity targeting several allied countries and Ukraine to the Russian military intelligence service, the GRU. NATO also reaffirmed its commitment to supporting Ukraine through the Tallinn Mechanism and the IT Capability Coalition, which provide cybersecurity assistance and strengthen Ukraine's ability to defend its networks. In July 2026, the EU imposed sanctions on nine Russian individuals and four entities involved in carrying out, enabling, or facilitating cyberattacks against EU member states and international partners. These actions demonstrate how European governments and NATO allies use intelligence sharing, public attribution, sanctions, and coordinated cyber defense to respond to Russian operations. However, differences in national cybersecurity capabilities and Moscow's reliance on state-aligned groups and cybercriminal infrastructure will likely complicate attribution and allow some operations to continue.

Outlook and Implications: Moscow will likely continue targeting European government institutions, defense organizations, and critical infrastructure while European countries maintain military and financial support for Kyiv. Moscow will likely expand its use of smaller businesses as entry points into larger government and defense networks while relying on state-aligned groups and cybercriminal infrastructure to complicate attribution. Continued Russian cyber operations will likely expose sensitive information, compromise defense networks, disrupt essential services, and increase economic costs across Europe. Although these operations will not likely end European support for Kyiv on their own, sustained activity could force governments to divert resources toward cybersecurity and infrastructure protection. NATO and EU cooperation will likely limit these effects, but Moscow's continued cyber activity will likely require governments to balance support for Ukraine with protecting their own national security interests.

[Hunter Varin]

RUSSIA: Likely Seeking Sustainability for Current and Future Military Ambitions

Summary: Moscow is likely strengthening relationships with allies such as Beijing and Tehran to strengthen its economy and reduce military vulnerability, likely aiming to sustain its war with Kyiv and possibly start new military campaigns in the Baltic Region. Moscow's economic partnership with Beijing increases Moscow's access to trade and new technologies, while Moscow's cooperation with Tehran allows access to weapons capabilities. These bilateral relations will likely support Moscow's economy and military in the long term.

Background: Since Moscow's military invasion of Kyiv in February 2022, NATO allies and Western governments have put sanctions and export restrictions in place in an effort to weaken Moscow's economic ability to fund its military invasion. In response, Moscow has strengthened bilateral ties with Beijing and Tehran, according to The Center for Strategic and International Studies (CSIS). Moscow's allies have responded cooperatively and maintained economic, diplomatic, and military cooperation, according to CSIS. In doing so, Moscow, Beijing and Tehran, have relied less on the West while achieving mutual benefit, according to CSIS.

Allied support economically and militarily: Moscow's partnership with Beijing and Tehran likely provides Moscow with the military and economic support needed for Moscow to maintain the war in Kyiv and possibly carry on another military campaign in the Baltic region. Moscow has been providing Tehran with satellite intelligence on Western military assets, according to *Defense News*. Furthermore, arms supplies remain a mutual exchange, according to *Al Jazeera*. Tehran has been providing drones with limited capabilities to Moscow, according to *Al Jazeera*. In exchange, Moscow has sent the same model of drones back to Tehran with enhanced capabilities, according *to Al Jazeera*. Beijing's role as an economic partner for Moscow extends to major industries. Russian Prime Minister Mikhail Mishustin said that Moscow and Beijing's cooperation in the energy sector includes oil, gas, coal, and nuclear energy, according to Reuters. Additionally, Moscow is planning the construction of Russian-designed nuclear power plants in China, according to the Kremlin. Trade is increasingly strengthening economic partnership. Trade exceeded $200 billion and nearly reached $250 billion in 2025, according to the Kremlin.

Implications for Baltic Regional Security: These international partnerships can likely help Moscow sustain its current war in Kyiv. They could also supply the economic and military capabilities needed to pursue another military campaign in the Baltic region. The Baltic region,

particularly Tallinn, has expressed security concerns about current military aggression in Kyiv and its implications on their soil. On 25 September, Estonian Defense Readiness Department Head Gert Kaju stated that due to Moscow's war of aggression in Kyiv, more drones and cruise missiles have entered neighboring countries, according to ERR News. Kaju also stated that Estonian forces have shot down drones in Tallinn, according to ERR News. President Vladimir Putin has responded to these concerns about a potential Russian attack with claims that Russian minorities are being mistreated in the Baltic region, according to the Kremlin.

Outlook and Implications: If Moscow continues to foster its efforts and cooperation with its allies, it will likely secure the necessary military, economic, and allied support to continue the current war in Kyiv and possibly conduct another military operation in the Baltic region. While Moscow's expanding economic and military partnerships with its allies does not necessarily indicate another military campaign, they could give Moscow long-term economic and military assistance to continue the war in Kyiv. Concerning the Baltic region, the threat of military aggression will most likely remain present. NATO will most likely remain a major deterrent for Moscow due to NATO's mutual defense pact. Moscow will likely cautiously test with military aggression, given that Tallinn, Riga, and Vilnius are members of NATO. NATO's influence within the Baltic Region and response to Moscow will play a major role in Moscow's decisions within the Baltic Region.

[Isabella Cantwell]

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 pregleye@erau.edu or Professor Avery at 928.777.4708. If you use material from this publication, you should attribute: Eagle Eye Intelligence Edition 509, a publication created by students at Embry-Riddle Aeronautical University in Prescott, Arizona.

© 2020 by Eagle Eye Intelligence. All rights reserved.

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