

China and Russia's Competition for Central Asia

From Insikt Group®

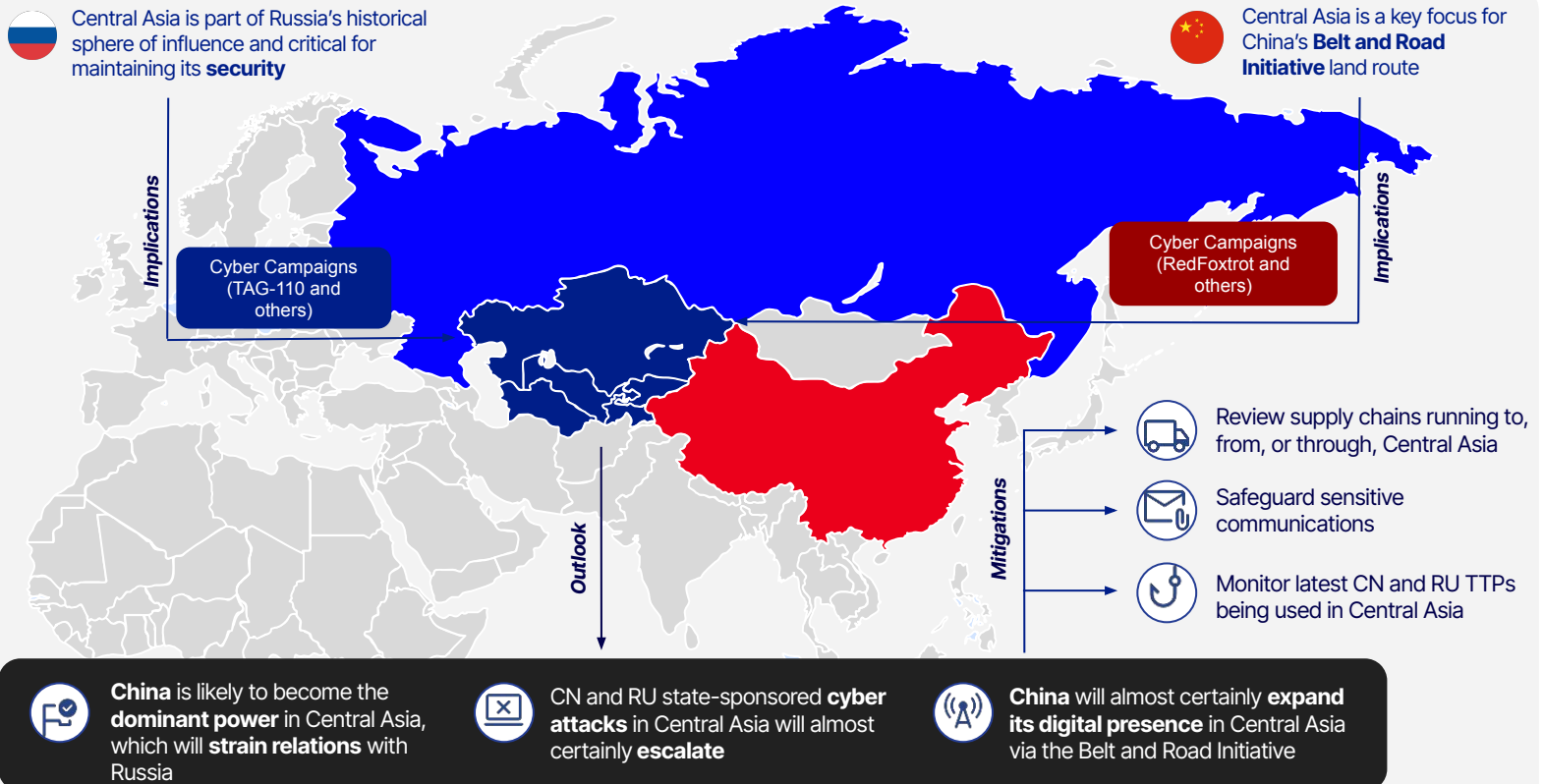
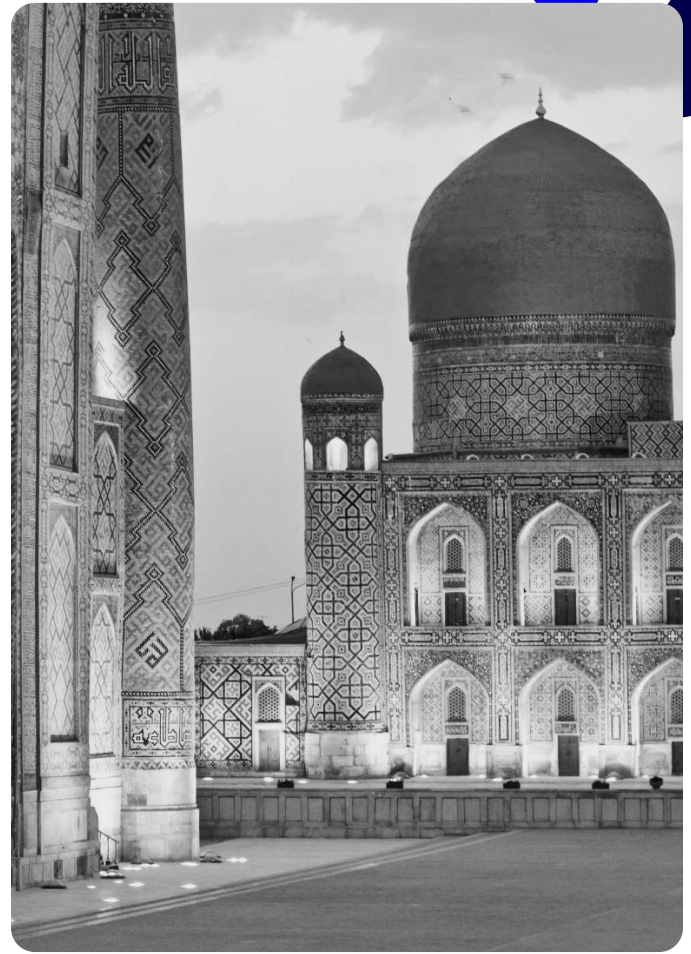
Summary

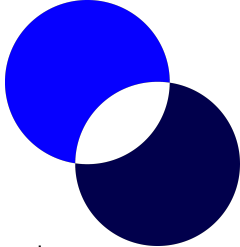
China and Russia have deepened their strategic partnership to counter Western influence, but mutual distrust remains at the lower bureaucratic levels. Their interests overlap in Central Asia, where cooperation and competition are in constant tension.

Recorded Future's Insikt Group has tracked both Chinese and Russian state-sponsored cyber-espionage campaigns targeting many of the same Central Asian organizations, a trend that reflects rising geopolitical competition.

China is likely to emerge as the dominant power in Central Asia by the 2030s as Russia's influence wanes following its invasion of Ukraine. Cyber espionage from both states is expected to intensify as this geopolitical shift occurs, with Beijing also expanding its digital presence through initiatives such as the Belt and Road and the Digital Silk Road.

Organizations operating in Central Asia should be extra vigilant against state-sponsored spearphishing campaigns, assess supply-chain risks, and safeguard sensitive communications given espionage threats.





Analysis

Both China and Russia have deepened their involvement in Central Asia. Over the last decade, China has invested heavily in infrastructure and economic development projects, while Russia continues to strengthen its longstanding political influence and security guarantees, which date back to the Soviet period.

Despite China and Russia having a strong strategic partnership, likely anchored by a mutual desire to push back against US global hegemony, mutual distrust persists, particularly in Russian and Chinese intelligence services. In June 2025, a [leaked document](#) by the FSB's Department of Counterintelligence Operations (DKRO) [described](#) China as a significant intelligence threat to the Russian Federation. Competition for influence in Central Asia — which includes Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan — has emerged as an area where Chinese and Russian interests are likely to conflict.

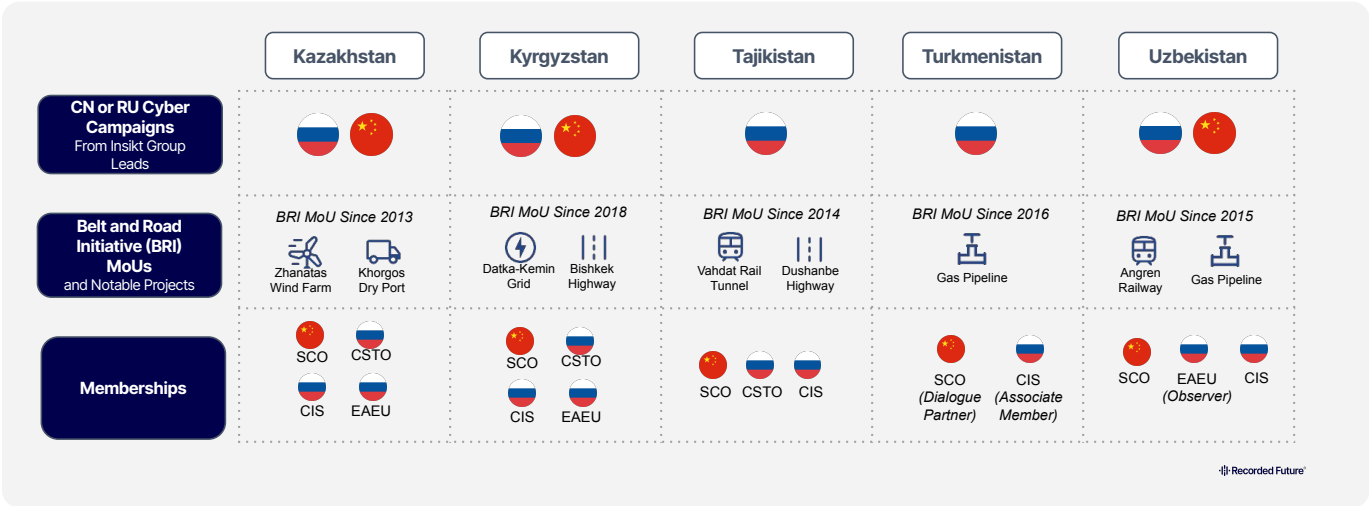


Figure 1: Summary of geopolitical alignment, cyber campaigns Insikt has observed, BRI projects, and memberships in Central Asia (Source: Recorded Future)

China [views](#) Central Asia as an essential component of its Belt and Road Initiative (BRI), a sweeping infrastructure and investment program aimed at enhancing China's global trade routes and economic influence. Central Asia serves as the land-based gateway to Europe, granting China access to critical resources, energy supplies, and markets. China has invested heavily in regional infrastructure, building highways, rail links, and dry ports to facilitate these trade flows.

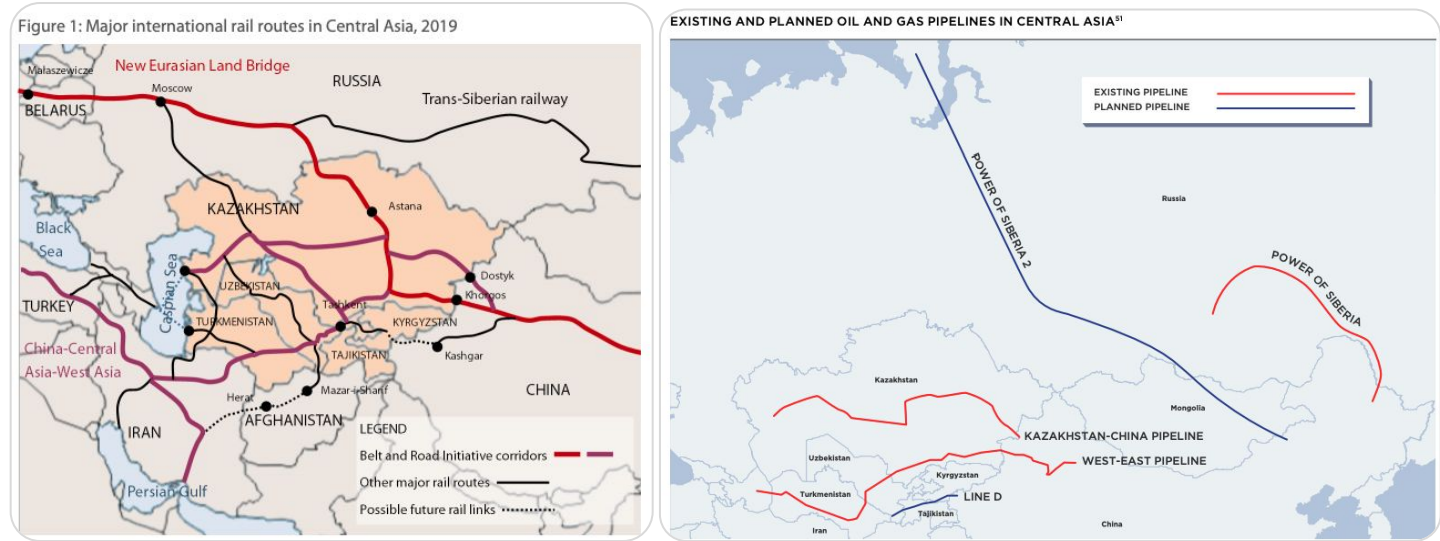


Figure 2: [Map](#) of China's Belt and Road routes through Central Asia (left); [map](#) of existing and planned gas pipelines to China through Central Asia (right)

To help [protect](#) this vital corridor, China has expanded engagement with Central Asian countries via the Shanghai Cooperation Organization (SCO), promoting political, economic, security, and cultural cooperation among its member states.

For Russia, Central Asia [remains](#) part of its historical sphere of influence, critical for maintaining regional hegemony. Moscow seeks to preserve its geopolitical dominance, military presence, and economic leverage through organizations like the Eurasian Economic Union (EAEU), the Commonwealth of Independent States (CIS), and the Collective Security Treaty Organization (CSTO). Russia demonstrated its readiness to uphold Central Asian governments in January 2022 when unrest in Kazakhstan left hundreds [reportedly](#) dead and thousands arrested. Under the CSTO framework, Russia [deployed](#) thousands of paratroopers to put down the nationwide uprising, reflecting its intention to act as the region's primary security guarantor. Russia also continues to [export](#) System for Operative Investigative Activities (SORM) surveillance systems to Central Asia, empowering state monitoring and repression.



Figure 3: [Images](#) of security forces arresting protestors in Almaty, Kazakhstan (left); Russian troops (part of CSTO mission) arriving in Ivanovo to put down protests across Kazakhstan in January 2022 (right)

China has become the undisputed economic [leader](#) in Central Asia, with trade and investment rising even amid its own slowdown. Meanwhile, Russia remains the region's main political partner, but its authority has [weakened](#) significantly. Both countries are also [coordinating efforts](#) to limit the influence of rival governments and foreign enterprises.

For Central Asian nations themselves, the Sino-Russian presence presents both opportunities and challenges. These countries [welcome](#) Chinese investments and infrastructure projects to drive economic growth, but remain wary of overreliance on Beijing.

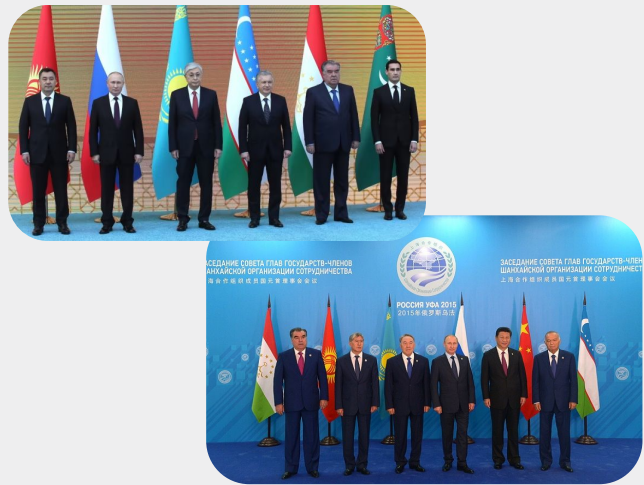


Figure 4: [Image](#) of Xi Jinping, the general secretary of the Chinese Communist Party (CCP), alongside leaders of Central Asian countries (left); [image](#) of Vladimir Putin, the president of Russia, also alongside leaders of Central Asian countries (right)

There is a clear correlation between geopolitical developments in Central Asia and state-sponsored cyber activity. Despite their strong strategic partnership, Russia and China are vying for regional dominance, using cyber operations as strategic tools to advance their own interests. Recorded Future's [Intelligence Graph](#), [network traffic analysis](#), [malware sandbox](#), and other tools have helped identify multiple instances of Chinese and Russian threat groups targeting Central Asia over the last five years.

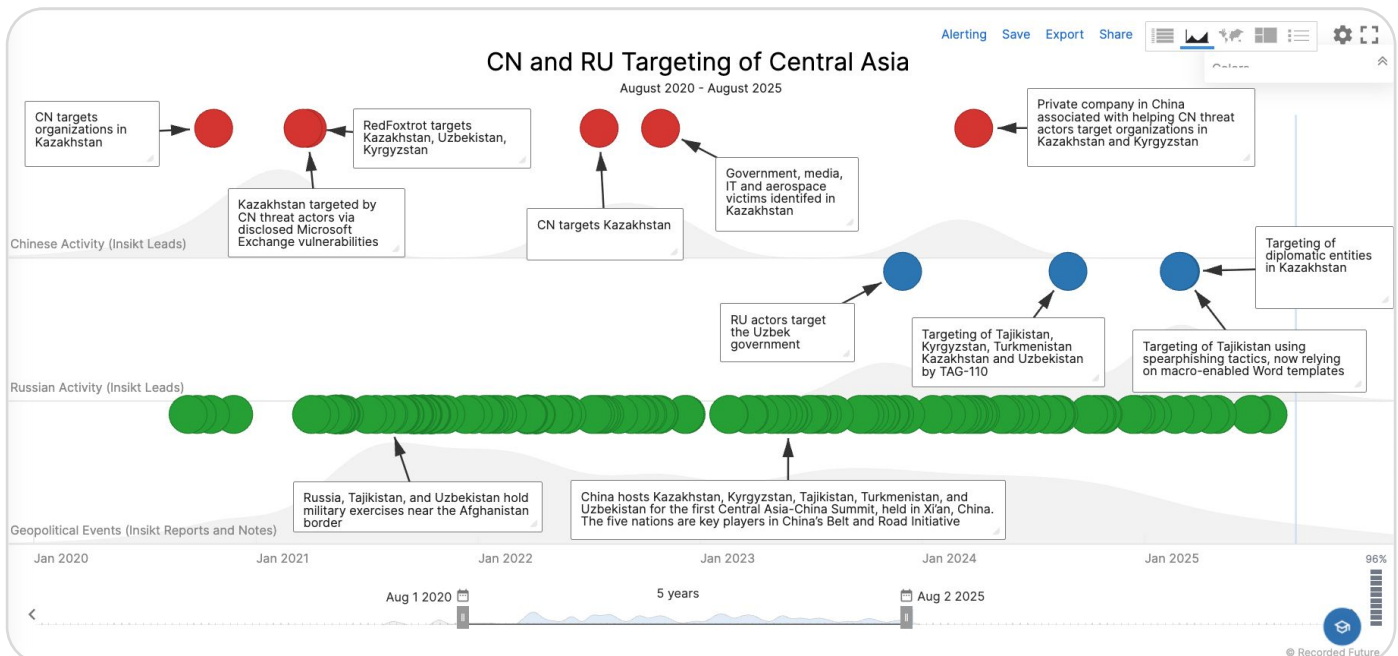
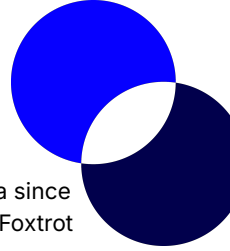


Figure 5: Timeline showing cyber campaigns Insikt Group observed targeting Central Asia (Source: Recorded Future)



Insikt Group [uncovered](#) RedFoxtro targeting government, defense, and telecommunications sectors across Central Asia since at least 2014. Operational security lapses, procurement records, and the use of specific malware families have tied RedFoxtro to PLA Unit 69010, which is under the PLA's Western Theatre Command, with its headquarters in Ürümqi, Xinjiang.

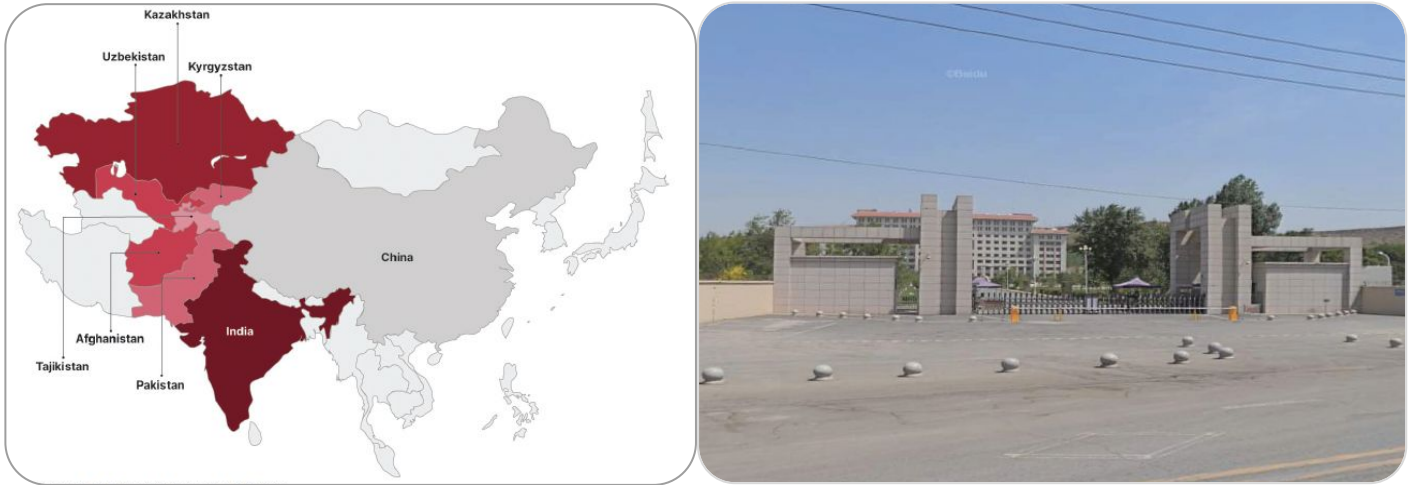


Figure 6: Diagram showing targeting of Central Asia (left); image of suspected Unit 69010 compound targeting these countries located in Ürümqi, from RedFoxtro [report](#) (right) (Source: Recorded Future)

Insikt Group also [identified](#) an ongoing Russia-linked cyber-espionage campaign targeting Central Asian human rights organizations, private security firms, government, and educational institutions. Victims were primarily located in Tajikistan, Kyrgyzstan, Turkmenistan, and Kazakhstan. Targets were infected with custom malware such as Hatvibe and Cherryspy, delivered through malicious Microsoft Word attachments and the exploitation of vulnerable web services.

The activity was attributed to TAG-110, a threat actor assessed with medium confidence to have overlaps with the Russian cyber-espionage group APT28, which is associated with Russia's military intelligence agency (GRU). TAG-110's operations were [assessed](#) to support Russia's military goals to gather intelligence on geopolitical dynamics in neighboring Central Asian states, particularly as Moscow's regional relationships deteriorated after its invasion of Ukraine.

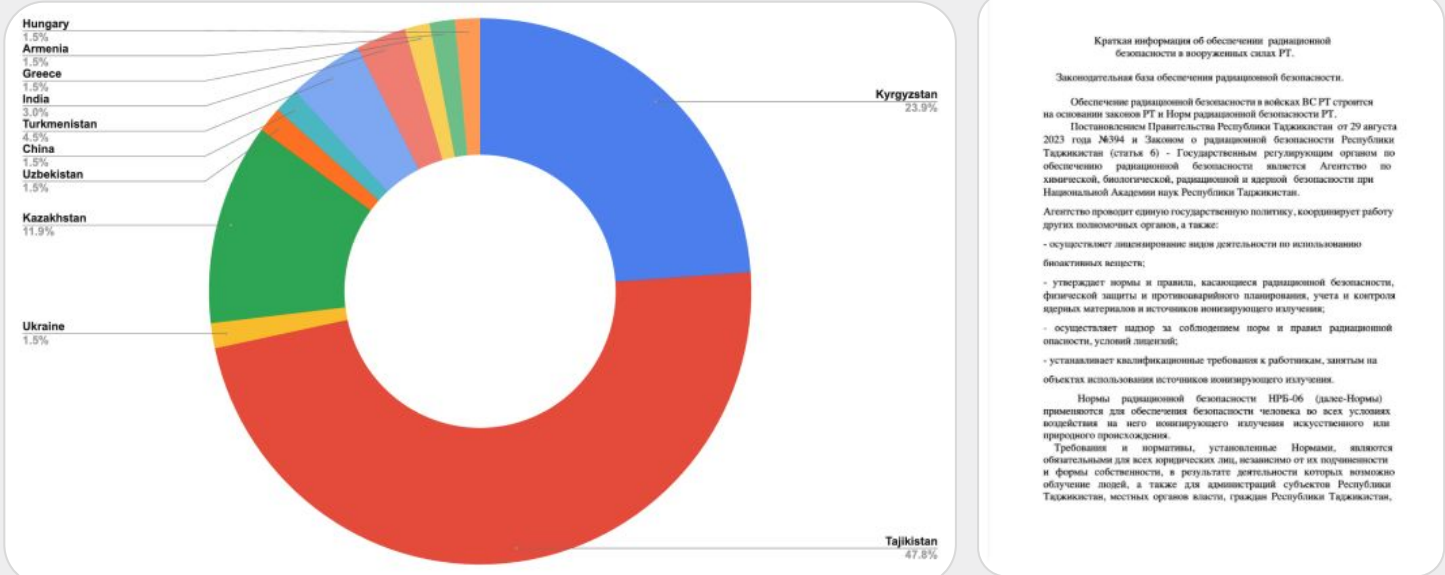
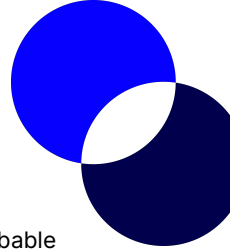


Figure 7: Chart from [report](#) showing heavy targeting of Central Asian states by TAG-110 (left); image from [report](#) showing phishing document used to target victims in Tajikistan (right) (Source: Recorded Future)



Using Recorded Future's Malicious Traffic Analysis, we observed victims in Kazakhstan communicating with highly probable Chinese state-sponsored infrastructure. Notably, there were spikes in traffic when high-profile political meetings were being held between Kazakh and Russian officials or when BRI infrastructure projects were being negotiated.

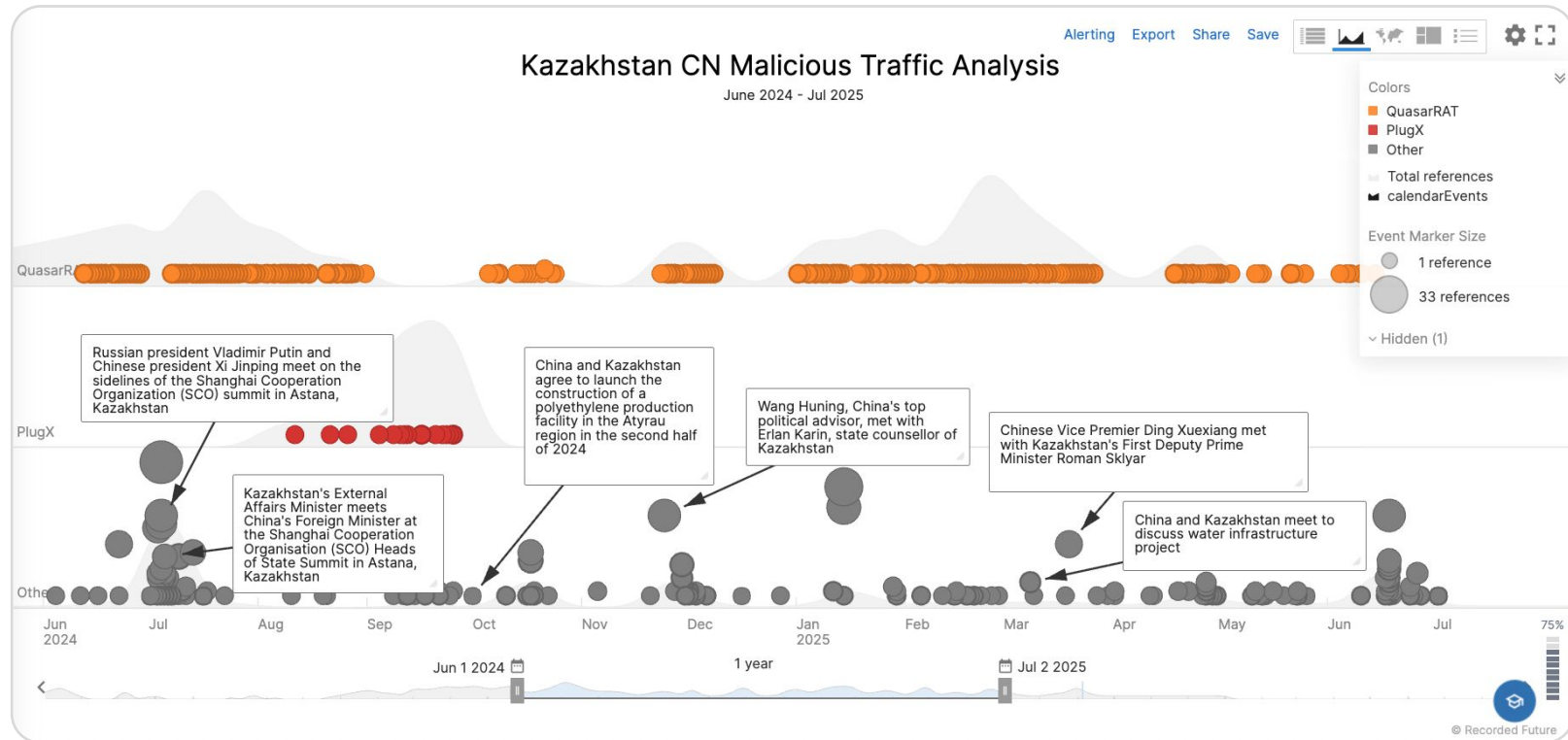


Figure 8: IP addresses in Kazakhstan communicating with QuasarRAT and PlugX C2s, in particular when major meetings are being held on security and infrastructure projects (Source: Recorded Future)

Moscow's traditional influence in the region continues to decline. Meanwhile, China's economic influence continues to grow, with initiatives like the Belt and Road Initiative offering an alternative development model. This evolving power dynamic will continue to fuel mutual distrust and cyber espionage.

Organizations operating in Central Asia should factor these geopolitical and cyber risks into their security planning and risk assessments.

Outlook

China is likely to become the dominant power in Central Asia by the 2030s: Since Russia’s 2022 invasion of Ukraine, Russia has increasingly [relied](#) on China to compensate for revenue losses due to Western sanctions. Furthermore, the ongoing conflict has [weakened](#) Russia’s ability to support allied regimes, as observed in Syria. While Russia has been able to maintain a significant amount of influence in Central Asia, this is gradually declining and is likely to decline further. Nonetheless, Central Asian states are likely to still seek positive relations with Russia, given their geographic proximity to Russia and membership in Russia-led regional organizations such as the CSTO.

Developments in Central Asia may strain Russia-China relations but are unlikely to threaten their strong strategic partnership: While Russia and China share many objectives, chief among them being the erosion of US and Western influence globally, distrust remains, particularly in their respective security services.

China and Russia’s adversaries are very likely to capitalize on tensions over Central Asia: President Donald Trump is [reportedly](#) planning a visit to Uzbekistan to commemorate the ten-year anniversary of the [“C5+1” regional diplomatic platform](#), marking the first time a US president has visited the region. The US and Uzbekistan have a [long history](#) of security cooperation in the region, while in May 2025, the two countries signed [multiple agreements](#) on US access to critical minerals.

Cyber attacks against Central Asian countries by Russian and Chinese state-sponsored threat actors will almost certainly escalate: China’s digital infrastructure projects and Russia’s security networks create more high-value targets. State-sponsored threat actors continue to conduct espionage campaigns on behalf of Moscow and Beijing, with many important enterprises and government departments having data exfiltrated. This almost certainly enables both Russia and China to stay one step ahead of each other in the region.

China will almost certainly expand its digital presence in Central Asia via the Belt and Road Initiative: As Beijing’s infrastructure projects expand in Central Asia, so does the “Digital Silk Road,” as previously [reported](#) on by Insikt Group. Technology and telecommunications companies like Huawei are becoming increasingly [active](#) in the region, leading to [increased espionage risks](#).

Mitigations

Prepare your defenders and staff for targeted spearphishing attachment campaigns ([T1566.001](#)): If you are operating in Central Asia, ensure your blue teams are aware of active spearphishing attachment campaigns; this has been a common TTP used by Russian threat actors. Consider exploring options for Emulated File Analysis ([D3-EFA](#)). Recorded Future’s [Secops](#) Intelligence and [Enterprise Sandbox](#) can help support these efforts.

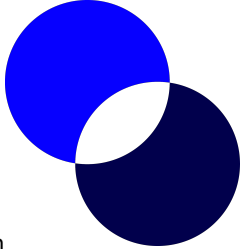
Review any supply chains running through Central Asia: Russia and China are increasing their grip on Central Asia despite those countries’ attempts to diversify their relationships. Ensure you have reviewed the risks that any suppliers in Central Asia pose to your organization. Also, consider running a business impact assessment should governments in Central Asia destabilize as a result of ongoing geopolitical changes. Recorded Future’s [Third-Party Intelligence](#) can help support these efforts.

Be cautious with what you send to entities in Central Asia: If your organization is communicating with strategic organizations or governments in Central Asia, assume those communications might be intercepted or exfiltrated by Chinese or Russian cyber threat actors. Ensure you are not sharing information that could lead to brand impairment, legal or compliance failure, or competitive disadvantage.

Monitor surveillance digital infrastructure projects: Chinese telecommunications and technology companies are increasingly active in Central Asia. These companies, which are alleged to have ties to the Chinese government, are increasingly operating state networks. Russia has also exported its surveillance capabilities to Central Asian countries. Incorporate this into your risk management approach for regional operations. Recorded Future’s [Geopolitical Intelligence](#) can help support these efforts.

Further Reading

SOURCE	TITLE
Insikt Group	Threat Activity Group RedFoxtrot Linked to China’s PLA Unit 69010; Targets Bordering Asian Countries
Insikt Group	Russia-Aligned TAG-110 Targets Asia and Europe with HATVIBE and CHERRYSPY
Insikt Group	Russia-Aligned TAG-110 Targets Tajikistan with Macro-Enabled Word Documents
Insikt Group	Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America
Insikt Group	China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road



Risk Scenario

Scenario: “Import Export International,” headquartered in Northern Europe, has won a lucrative deal with two Central Asian countries, edging out Chinese and Russian competitors. The deal was backed by the government of that Northern European country.

First-order Implications

Threat

Heightened cyber-reconnaissance: Russian and Chinese state-aligned threat actors are likely to probe Import Export International’s networks (and those of its government partners) to collect deal details and negotiate positions.

Risk

Operational disruption may occur if adversaries use network probing to identify vulnerabilities, exposing system architectures and security gaps that enable intrusions or denial-of-service attacks. These attacks could potentially halt critical services, interrupt operations, or degrade mission-essential systems.

Wave of spearphishing and watering-hole campaigns: Russian and Chinese cyber threat actors target executives, bid teams, and key Central-Asian third-party suppliers to steal negotiating documents and credentials.

Brand impairment caused by reports of targeted phishing against senior leadership and partners undermines confidence in Import Export International’s cybersecurity posture, prompting customers and governments to question its ability to protect sensitive negotiations.

Second-order Implications

Threat

Deepfake-enabled disinformation campaigns launched: Politically motivated deepfake videos of executives and government officials spread on regional media, alleging corruption and triggering shareholder queries. Coordinated social media narratives question the ethics of both the firm and its home country government, accusing them of siphoning funds for personal enrichment.

Risk

Widespread circulation of fabricated videos and coordinated narratives erodes trust among customers, partners, and local stakeholders, damaging the firm’s reputation for integrity and leading to **brand impairment**. Furthermore, content falsely portraying executives and members of their home-country government involved in corrupt dealings could trigger investigations from opportunistic rival politicians, resulting in **legal or compliance failures**.

Third-order Implications

Threat

Wiper malware disrupts critical shipping operations: As a result of an employee falling victim to a phishing email, the threat actor gains access to the network and deploys wiper malware disguised as ransomware to create plausible deniability. This attack occurs in the context of escalating geopolitical tensions between Russia and NATO.

Risk

Critical systems destructively wiped under the guise of ransom demands can cripple essential IT infrastructure, halting trading operations, logistics coordination, and real-time transaction processing, leading to **operational disruption**. Stakeholders may perceive the company’s inability to distinguish and mitigate advanced attacks as a severe security shortfall, eroding trust among customers, partners, and regulators, which results in **brand impairment**.

Key:

- Legal or compliance failure:** Breach of laws, regulations, or industry standards resulting in liability or sanctions.
- Operational disruption:** Interruption to normal business processes affecting productivity or service delivery.
- Brand impairment:** Damage to reputation that reduces customer trust and market value.
- Financial fraud:** Unauthorized manipulation or theft of financial assets for personal or organizational gain.
- Competitive disadvantage:** Loss of market position due to inferior capabilities, intelligence, or innovation.

References:
[The Risk Business: Second Edition](#)
[Intelligence to Risk](#)
[The Intelligence Handbook](#)