1 April 2024

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

Issue 450
Of Eagle Eye Intelligence

Authors

Reina Girouard
Brandon Greenaway
Christina Muchow

1 April 2024

Issue 450
Of Eagle Eye Intelligence

In This Issue

CHINA: Poor Working Conditions Will Not Likely Impact Cyber Operations

Summary: A recent data leak revealed frustrations over working conditions within a Chinese state-sponsored private hacking company I-Soon. Hackers across the state will likely share these conditions and views. Despite Beijing's increased cyberspace emphasis, the working conditions of its cybersecurity specialists remain lacking. The working conditions will likely not decrease the company's strength in the cyber domain.

Background: On 16 February, an unknown actor uploaded a variety of data related to Chinese cybersecurity company I-Soon onto GitHub. The data leak revealed data on state-sponsored hacking operations, as well as employee chats revealing dynamics within the company. This leak exposed many details on the inner workings of Chinese state-sponsored hacking companies. I-Soon offered a variety of services, including hacking and social engineering operations. Some of the leaked files contained information relating to I-Soon's marketing of its company and services, according to *The New York Times*. The company struggles with a lack of experience and often leaves clients displeased, according to *The New York Times* and *The Washington Post*. It repeatedly failed on assignments to gather information from foreign government agencies. It also had many services "under maintenance," according to *The New York Times*. I-Soon employees also complained about poor pay, long hours, malpractice, and sexism within the workplace. The actor who posted on GitHub presented their intentions as wishing to expose bad working conditions and incompetencies within I-Soon, according to The Washington Post. Over the last couple of months, I-Soon significantly increased cyber-attacks and initiatives from Beijing. Regardless of the accusations, Beijing continues to deny responsibility for any cyber-attacks. Beijing uses private cybersecurity firms to conduct its offensive cyber operations. This allows it to deny responsibility for such operations. On 26 February, Beijing expanded its cyber defensive agenda through a new industrial cybersecurity plan.

Working Conditions and Expectations: The working conditions described at I-Soon likely translates across other cybersecurity firms and industry in general in China. I-Soon demonstrated technical incompetencies, the frustrations from employees with poor pay, excessive workloads, and working conditions likely appear in other companies. The data leak not only revealed dissatisfaction with the environment at I-Soon, but also tensions between other firms as well, according to *The Washington Post*. These tensions and frustrations likely emerge out of the heightened competition for government contracts. Beijing's digital economy accounts for about

30% of its GDP, according to the *China-Britain Business Council*. The lack of demand compared to the supply of cybersecurity companies most likely caused a highly competitive market. The larger working culture in China likely shares standards of the working conditions described at I-Soon, particularly the excessive workloads and long working hours. Employees across the country commonly practice the 996-work schedule, where they work from 9am to 9pm, six days a week, according to the BBC. Companies in the technology sector often have employees working long hours without consistent pay, according to the BBC. As a result of the increased competition, most firms likely reduced wages and working conditions to try and gain a competitive advantage. Beijing prohibits working conditions like these, with little changes. Over the last 10 years, several protesters have gathered against poor pay and the 996-work culture. China's youth also show less desire to participate in the intense work culture, preferring reasonable and flexible working hours instead, according to BBC. This, along with a slowing growth in population, will result in a shrinking labor force, according to BBC and *The Economist*.

Increased Cyber Efforts: Beijing's cyber capabilities will likely continue to progress supported by Beijing's continued monetized support. As shown by the new cybersecurity plan released in February, this support extends to both offensive and defensive cyber operations. Earlier in the decade, Beijing focused on cyber espionage and used simpler techniques, such as email phishing, but these tactics evolved over time. Before 2018, Beijing began shifting from using military resources for cyber operations to outsourcing contracts to the private sector, according to The New York Times. This includes private companies and universities. The recent, frequent reporting of hacking organizations like Volt Typhoon and Double Dragon, also referred to as APT 41, highlights this transition. Since this shift, Beijing's cyber capabilities have increased significantly. At the Munich Security Conference in February, officials from both Japan and the US discussed the rising threat of Chinese state-sponsored hacking, according to The Record. Taipei, Manila, and other governments in East Asia raised concern about the prevalence and danger of Chinese cyber-attacks. The success of Beijing's use of the private sector for cyber operations means that it will most likely continue using this tactic. With the rising tensions between other countries, Beijing will not likely decrease cyber funding and will likely continue to create new defensive cyber initiatives. With the success of and need for strong cyber operations in recent years, Beijing will likely continue to develop competitive cyber capabilities.

Outlook and Implications: The low-quality working conditions prevalent in China's cyber systems will not likely decrease its power in the cyber domain. The working culture and expectations in China likely accept working long hours with excessive workloads to achieve a company's goal. This means that the poor working conditions at I-Soon and other cybersecurity firms will not likely raise much concern. As a result, Beijing and these firms will likely do little to change these conditions in the next few years. However, these conditions will also not likely affect efficiency because the labor force learned to accept and manage these poor work conditions. The increased state support and funding for cyber operations will likely continue to increase the competition between firms. This will most likely advance the efficiency and effectiveness of Beijing's cyber operations. It will also likely cause more strain on the individual hackers at private firms.

[Reina Girouard]

MOLDOVA: Expulsion of Russian Diplomat Likely to Escalate Tensions

Summary: The potential for civil conflict between Chișinău and Moscow will likely increase due to authorities expelling a Russian diplomat after opening polling stations for its presidential election in the Transnistria region. Moscow will most likely utilize the civil conflict between Chișinău and Transnistria to decrease government support for Chișinău, destabilizing the country and increasing support for Moscow.

Background: On 19 March, authorities in Chișinău declared a Russian embassy worker *persona non grata* after opening polling stations for Moscow's presidential elections in the region of Transnistria. The embassy worker opened six polling stations in the region, despite initial agreements to open only one polling station in the Russian embassy building in Chișinău, according to AP News. The move prompted foreign embassy authorities to summon Russian ambassador Oleg Vasnetsov, informing him of the diplomat's involvement and their expulsion from the country, according to The Bangkok Post. Vasnetsov later described the expulsion as an "unfriendly act," and stated that Moscow will act against Chișinău, according to TASS. In a press conference, Moldovan President Maia Sandu spoke against the incident, calling it a disrespectful move against the country's sovereignty, according to Reuters.

Civil Conflict in Breakaway Region: The use of polling stations will likely increase tensions and civil conflict between Chișinău and local authorities in the Transnistrian region. Transnistria, a Moscow-aligned breakaway state, claimed independence from Chișinău since its founding in the 1990s, but the United Nations members do not recognize Transnistria's independence, according to *Al Jazeera*. On 1 January, officials in Chișinău established new taxes and customs duties on Transnistrian imports and exports, resulting in several protests and Transnistrian leadership accusing Chișinău of starting an "economic blockade," according to Balkan Insight. On 28 February, Transnistrian officials appealed to Moscow for protection, claiming Chișinău's policies seek to destroy Transnistria's economic potential and create poor living conditions for its citizens, according to AP News. Civil conflict will likely continue between Chișinău and Transnistria, which will likely result in increased hostility and create further division between the two. However, it remains extremely unlikely that Transnistria would succeed in a breakaway from Chișinău due to international countries refusing the region's independence. Furthermore, Moscow will most likely not reason with Transnistrian appeals because Moscow never

recognized the region's independence or acknowledged other Transnistrian appeals, according to *The Kyiv Post*. Moscow still maintains a military presence in the region to guard Soviet-era weapons and ammunition stockpiles, according to *Al Jazeera*. As a result, Moscow will likely maintain involvement in the region to protect its military interests and maintain pro-Moscow influence.

Moscow's Increased Interference: The expulsion will likely increase Moscow's attempts to destabilize support and sabotage the policy objectives of Chișinău officials. Since February 2022, Chișinău condemned the neighboring Russo-Ukranian war, resulting in strained relations between Chișinău and Moscow, according to Reuters. On 15 December 2023, Chișinău opened accession negotiations with the European Union (EU), beginning the process for EU membership, according to AP News. This has resulted in Moscow conducting "hybrid warfare" against Chișinău to pressure government officials to returning to Kremlin influence, according to *Al Jazeera*. On 5 November 2023, Chișinău accused Moscow in meddling in local elections after intelligence officials found that the pro-Kremlin Chance political party received $53 million from Moscow to bribe voters, according to AP News. On 5 March, reports from intelligence officials stated that Moscow planned to conduct several misinformation campaigns through various social networking platform to encourage anti-government sentiment and protests, as well as back pro-Kremlin political figures, according to AP News.

Outlook and Implications: Because of the diplomat's expulsion, Moscow will most likely retaliate by increasing interference efforts against Chișinău. Due to ongoing civil conflict between Chișinău and Transnistria, Moscow will likely utilize Transnistria as a proxy to conduct interference and other destabilization efforts against Chișinău. As a result, Moscow will likely increase collaboration with Transnistrian officials to undermine Chișinău's support. However, despite having Transnistrian support, it is highly unlikely that Moscow would consider an annexation of the region due to its lack of engagement towards Transnistrian referendums, as well as its ongoing involvement in the Russo-Ukranian war. As a result, efforts against Chișinău seem unlikely to lead to direct war, but Moscow will still hope to destabilize the country through passive methods.

[Brandon Greenaway]

RUSSIA: Mobilization Efforts to Ukraine Will Likely Increase

Summary: Moscow will likely expand its mobilization efforts for the Russo-Ukrainian War and pressure allies to expand their counterterrorism efforts.

Development: On 22 March, four men attacked the Crocus City Hall concert venue in Moscow with firearms and incendiary devices. The men opened fire on the concertgoers, started a fire, then fled. On 24 March, the death toll stood at 133, although Russian officials expected it to rise. Eleven suspects, including the four attackers and seven others, are currently in custody and charged with committing an act of terrorism. At least one of the attackers is believed to be a Tajik national. Tajikistan is a member of the Russia-led Collective Security Treaty Organization (CSTO), which contributes to terrorism in Islamic states. Islamic State – Khorasan (ISIS-K) claimed responsibility for the attack, which several Western governments confirmed. Russian President Vladimir Putin did not comment on ISIS-K's claim in his public statements but claimed that the suspects attempted to flee to Ukraine. Russian Foreign Ministry Spokeswoman Maria Zakharova claimed that Kyiv, with Western support, was responsible for the attack rather than ISIS-K, according to state-sponsored newspaper *Komsomolskaya Pravda*.

Analysis: Moscow will likely claim Kyiv organized and aided the attackers. Moscow will probably acknowledge the attackers' ISIS-K ties but claim that Kyiv, and the governments that support it, are primarily responsible for the attack. Moscow will likely use the attack as justification to expand mobilization efforts in Ukraine. Moscow is unlikely to expand ongoing counterterrorism efforts in Syria and Africa. Moscow will likely use the current forces in Syria and Africa for the Ruso-Ukrainian War. Moscow is unlikely to increase military aid to Damascus due to supply shortages in the Russo-Ukraine war. Moscow will likely apply diplomatic pressure to convince fellow CSTO members, especially Dushanbe, to increase their counterterrorism efforts.

[Christina Muchow]

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 449, 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