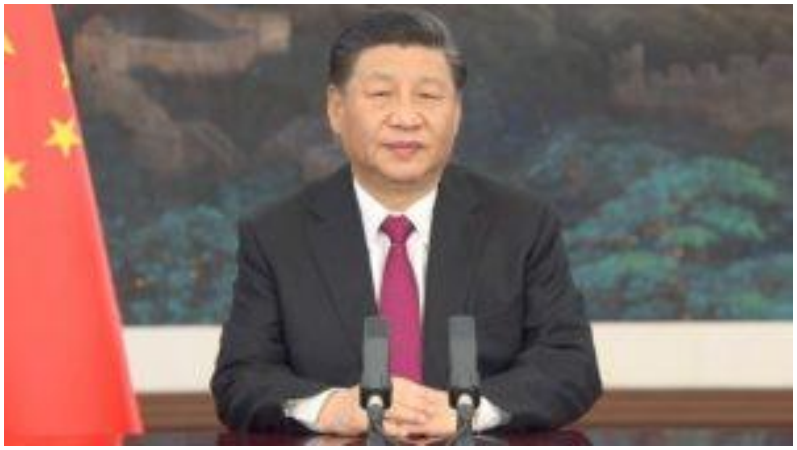
28 April 2023

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

Issue 431
Of Eagle Eye Intelligence

Authors

Isabella Whalen
Amanda Franklin
Bobby Roe
Julia Rieth
Mason Meinzinger



The Diplomat

28 April 2023

Issue 431
Of Eagle Eye Intelligence

In This Issue

RUSSIA: Killnet Cyber Attacks Likely to Remain a Rising Threat for Targeted Entities

Summary: Since early January 2022, officials have identified the Moscow-aligned hacker group Killnet launching distributed denial of service (DDoS) attacks against multiple governments and political organizations across Europe and the United States. Its current attacks shed light on a new aggression towards current public-facing services by organizations non-affiliated with Moscow and Killnet motives. These resulting disruptions and threats will likely cause an increase in relation tensions between Moscow and NATO countries.

Background: Officials have identified the Moscow-aligned hacker group Killnet as a pro-Kremlin hacker group known for targeting European governments and infrastructure through disinformation campaigns. Lesser-known groups who sympathize with Moscow's operations compose Killnet. Since last March, the Killnet group launched DDoS attacks against Kyiv and Warsaw, claiming all attacks responded to countries outwardly stating its non-support of Moscow, according to AVERTIUM. The group remains active in European and United States organizations and expanded its activity since the invasion of Russian and Ukraine to target NATO countries and its allies. The targeting appears consistent with previous activity seen across the threat across the landscape, showing an interest in causing disruptions to critical infrastructure and using social platforms regarding attacks for Moscow propaganda. The Killnet group attack tools remain DDoS and brute-force credentials with no tools identified as developed or custom. However, the Killnet group continues to have persistent capabilities in its way of conducting reconnaissance and credential harvesting. Allowing its unique attack methods to thrive on publicity and misinformation, permitting the group to influence and achieve its goal of disruption.

A Likely Platform to Increase Tension: The Moscow-linked hacker group Killnet will likely continue attacking NATO countries and allies due to the increased tension within its support of Kyiv during the current Moscow and Kyiv war operations. Killnet's and Moscow's other organizations' recent operations since February 2022, play a key role in escalating the Russo-Ukrainian War such as:

- The Killnet hacker group consistently targets supporters of Ukraine, including NATO countries and its allies since February 2022, with the most recent activity involving lures to coincide with the Russian invasion of Ukraine.

- In October 2022, Killnet claimed responsibility for the digital disruption of state government websites in the United States following Russia's invasion of Ukraine. Later that month it claimed responsibility for taking down several United States airport websites in a DDoS attack.
- In November 2022, hours after lawmakers passed a resolution labeling Russia a state that sponsors terrorism, Killnet claimed responsibility for a DDoS attack on the European Parliament's websites.
- In February 2023, Killnet carried out a series of DDoS attacks against NATO, causing temporary disruption to some of the military alliance's public-facing websites. Later that month, Killnet claimed responsibility for a DDoS attack on German airports.

With its previous attacks increasing and aimed at NATO countries and connected allies, the Killnet hacker group remains likely to continue launching its attack chains at organizations and entities unaligned with its views in the wake of current tensions regarding war operations and resolution between the Moscow and Kyiv dispute.

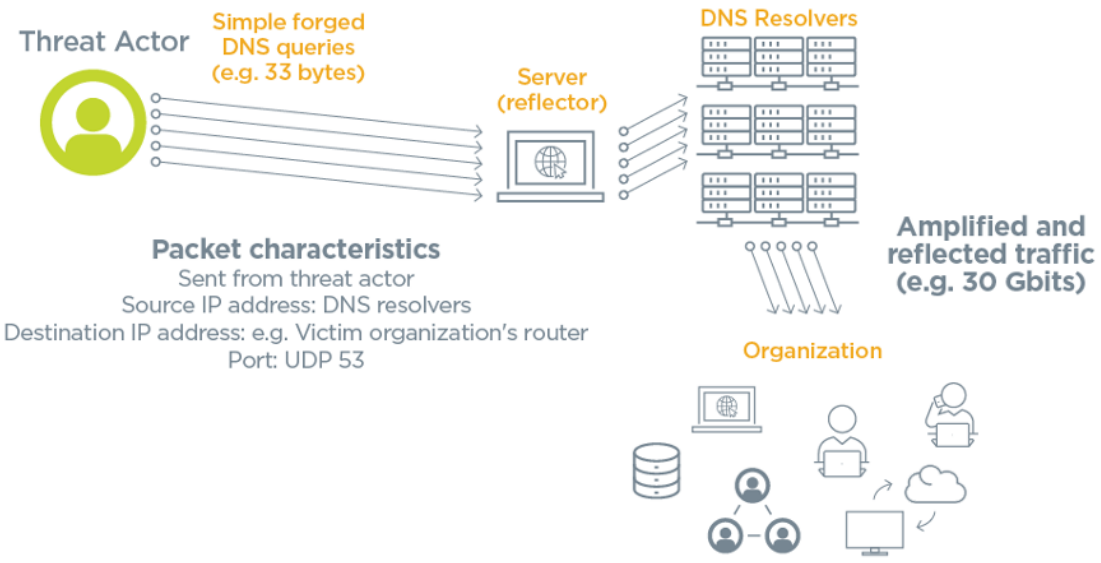


Figure 1: Behavior of Preferred DDoS Attack Method

Attention and Power: Killnet probably will continue conducting these forms of consistent disrupting attacks against critical infrastructure to increase its campaign of political rhetoric and misinformation. With this possibility, also leading to Killnet furthering threats against any opposition and attacks performed against any Moscow-aligned organizations or groups with

shared viewpoints. As current escalating tensions between Moscow and Kyiv operations will likely continue to increase the risk of conflict between NATO countries and affiliated allies regarding its relations moving forward.

Outlook and Implications: Killnet's progressing development within its aggressive attacks and strategies in compromising its target will likely lead to an increase in attacks targeting infrastructure in increased quantities but, with a specific emphasis on government disruption. As its efforts to sustain and further its attacks on NATO nations and aligned allies almost certainly remain a platform to escalate conflict between targets and create support for Moscow's war operations. Its efforts and support of these operations will probably only increase the opposition of targeted governments and affiliated organizations. This will likely lead Killnet to conduct new tactics that may lead to more conflict and relation tensions as governments respond with opposition.

[Isabella Whalen]

CHINA: Lithium Likely to Remain a Key Driver in Newest Economic Strategy

Summary: Beijing will likely use the lithium energy industry to propel its official "dare to struggle" economic and diplomatic narrative due to the amount they could gain, most likely focusing on lithium-heavy countries in Latin America and Africa as their next major focus. While Beijing already holds strong ties to lithium-producing areas, the market flux around lithium prices will probably not stop further development and incorporation of lithium and lithium-rich areas into bilateral agreements with the People's Republic of China (PRC).

Background: Since 2000, Beijing worked to incorporate lithium-producing nations and areas into trade agreements and further diplomatic relationships, especially if they can gain further trade or better access from doing so. Beijing openly promoted relationships with lithium-rich countries such as Argentina, Bolivia, Chile, and Peru, which contain 67 percent of proven lithium reserves and produce about half of the global supply, according to the U.S. Geological Survey. Coming up to 2023, the lithium markets slow down with speculation as to what Beijing will do. On 16 April, reports say that the sharp decline for the past few years might bottom out, swiftly followed by reports of these low prices paving the way for other nations to get a chance for a share in the market, according to Bloomberg. Additionally, with the rise of the new foreign minister Qin Gang and the key government official overseeing the economy He Lifeng, the new officially branded slogan of "dare to struggle" (often derisively referred to externally as wolf-warrior diplomacy) exists loud and clear in the lithium gain and processing industry and in Beijing's persistence in gaining there whenever and wherever they can.

Lithium's Leverage: Lithium will likely hold power in the marketplace due to predicted increased use globally, including incentives that encourage further lithium battery usage over other means, and the fact it could draw power away from Taipei and towards the PRC. Lithium aids the making of batteries and semiconductors for various technologies but also serves a purpose when constructing electric cars or other innovations of the future. This niche will likely grow, especially in Europe's 2035 plan to move away from fossil-fuel vehicles entirely; almost certainly pushing the market towards batteries and their lithium. Beijing sees a future in lithium use, so will not want to let up after almost two decades of pressure on production and acquisition. Furthermore, Beijing incentivizes the use and innovation of lithium batteries by offsetting some of the material with sodium, yet still not fully eliminating lithium. Beijing's

access to lithium allows Beijing to make these batteries, which once again points towards a future made by lithium despite the current dip in prices and cost.

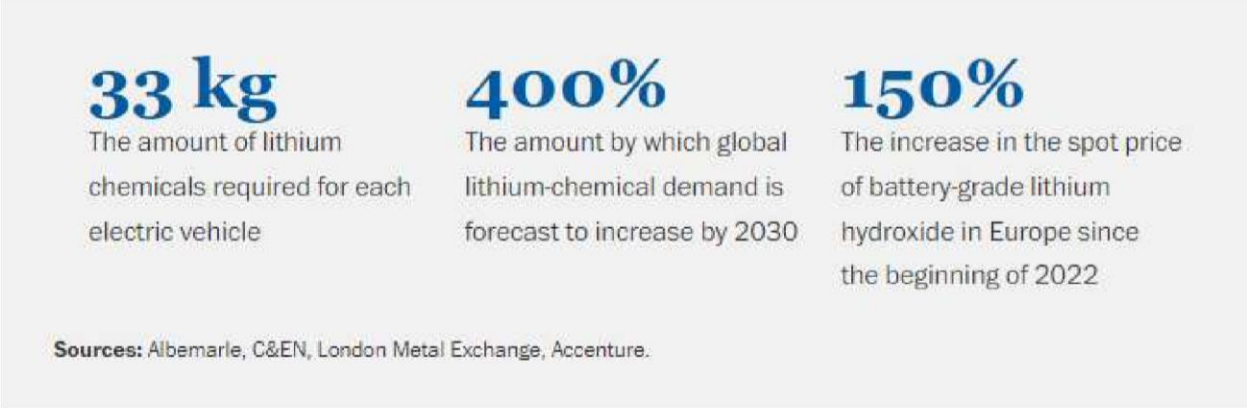


Figure One: Gives figures that explain the importance of lithium moving through 2030.

Unhealthy Competition: With the market slowing down and prices at a low, Beijing will almost certainly take advantage of the cost to try and get further ahead. While numerous sources report the market bottoming out soon, others do not assume that will stick for very long. On 16 April, a report published by Bloomberg remains skeptical of current markets but projects an increase soon. This market lapse started an influx of reports in Washington and the European Union (EU) wanting to catch up to Beijing, which holds a significant chance to further motivate Beijing to corner the market. Since late 2022, the EU started to compete with Beijing over the most environmentally friendly options while also ramping up its efforts whenever possible. While they continue to do so, Beijing's dominance keeps them from achieving any real sense of progress or support for their desire for electric vehicle batteries or other lithium products and technologies. This desire despite the intention and progress to try and crack into this niche still leaves China in a beneficial position, so Beijing does not likely want to give it up anytime soon. Some officials even debate if Beijing can keep up with both its demand and the EU's, regardless of ramping up capacity. Either way, Beijing possesses the motivation to further corner the lithium market through a sense of competition with the West.

Possible Policy Win: One of Beijing's possible main goals of cornering the lithium market as they prepare to follow through in their newest "dare to struggle" policy, and where they currently stand in this industry almost certainly makes it an easier target than ever before. This likely comes almost twofold with such an important victory attached to it. Beijing already possesses or

trades with many lithium producers and processing areas, especially with the larger ones in the industry. Further cornering the market in a near monopoly could make an easy win due to the sheer quantity of control Beijing holds and the already nearly completed job. Beijing's trade and/or Belt and Road Initiative (BRI) efforts established with all the nations within Latin America's lithium triangle, along with the countries with large reserves found in Africa keep it afloat; along with currently working on tapping into the Canberra marketplace.

Outlook and Implications: Lithium could act as a major driver of future change, and Beijing almost certainly wants to capitalize on that to prove its new policy while likely securing significant economic control and profit. The benefit of having a working trade relationship with Beijing through the BRI could mean once-difficult access to lithium turning into one more plentiful, something that Beijing might seek by going after lithium this heavily. Furthermore, a potential to urge national unity with Taipei through increased lithium trade and dependence back onto the PRC might happen. Possession of essential heavy metals along with lithium for Taipei's major chip industry requires Taipei's reliance on Beijing for materials and therefore a significant economic industry might apply just enough pressure to speed up the timeline on Beijing's reunification efforts.

[Amanda Franklin]

[RUSSIA: Potential Escalation in Cyber Attacks Could Spread the War in Ukraine]

Summary: Moscow's war in Ukraine continues to face resistance, possibly contributing to the reason why Moscow reaches beyond Ukraine for cyber-attack targets, according to Google's Threat Analysis Group. Russian-backed cyber-attacks could drag other countries into the war or spread the conflict globally.

Background: After declaring special military operations on 24 February 2022, the Russian military invaded Ukraine, and pro-Russian hacker groups focused their efforts on crippling Ukraine. While Russian ground forces struggled to secure any advances made, Kyiv constantly fought a war on two fronts focusing on both physical and virtual battlefields. In the year 2022, Ukraine received the brunt of Russian cyber-attacks. However, as the war progressed, Russian hacker groups refocused their efforts on other countries and sources of information. In the year 2022, cyber-attacks against Ukraine rose 250 percent. During the same period, cyber-attacks on North Atlantic Treaty Organization (NATO) members also rose 300 percent, according to Google's Threat Analysis Group. The target of these attacks, NATO, possesses 31 member countries around the globe.

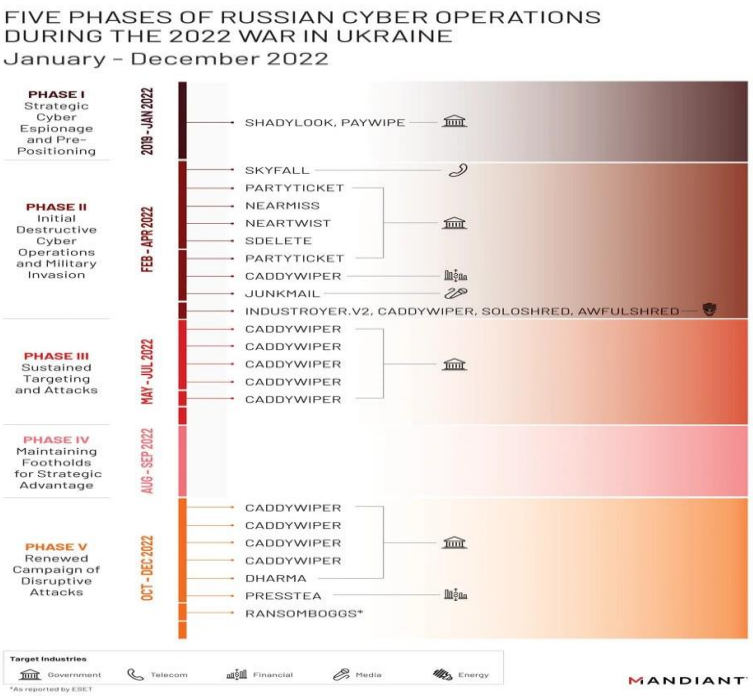


Figure 1: Google's predictions of each phase of the Russian-Ukraine war.

NATO Tensions Rise: Should these cyber-attacks continue, tensions with NATO countries around the globe may continue to rise, which could force them into the ongoing conflict between Russia and Ukraine. On 9 December, NATO Secretary-General Jens Stoltenberg conveyed that while NATO actively attempts to avoid a war with Russia, war remains a possibility. The tension between Russia and NATO members increases as Moscow repeatedly accuses NATO members of joining the armed conflict between Russia and Ukraine. These accusations exist due to NATO members extending military support to Ukraine, such as weapons, training, and critical military intelligence. With increasing tensions between NATO and Russia and the increased involvement of NATO members in Ukraine, Moscow appears to pursue cyber-attacks on other NATO members. Countries such as Montenegro, Finland, Sweden, and Estonia all received focused cyber-attacks against their respective governments, most of which conducted their own investigations. In their findings, these countries discovered Russia, or pro-Russian hacker groups responsible for the attacks. Contrarily, Russia's Federal Security Service of the Russian Federation (FSB) accused NATO of launching over five thousand cyber-attacks against key infrastructure since the start of Moscow's invasion. The FSB pinpointed the attacks as originating from Ukrainian territories, as well as introducing new methods of cyber warfare. Currently, the FSB accuses other countries of using Ukrainian infrastructure to conduct their attacks. These attacks only increase the animosity towards Russia, and should other countries choose to involve themselves in this war, it could force their allies, or all of NATO to respond and honor their treaties.

Potential Offensive: If Moscow directs its military to pursue cyber-attacks on NATO members, it could change the direction of Russia's war with Ukraine. Analysts observed a pattern in Moscow's cyber attacks, indicating Ukraine may come under threat of a large cyber-attack, according to Google's Threat Analysis Group. Pro-Russian hackers would likely back this potential offensive approach against Ukraine, and while the Ukrainians could recover, Russian hackers might continue to develop their skills and plan a new offensive strategy. Throughout this time, Russian hackers continue to probe other countries that associate themselves with NATO, which may draw other countries into this conflict and exacerbate the situation. NATO sanctions and aid created a point of contention with Russia which could pressure Moscow into acting upon an aggressive offensive attack on Ukraine.

Moscow's Potential Concerns: If Moscow continues actively attacking Ukrainian allies and NATO members, the attacks might result in NATO triggering Articles Four and Five. NATO Article Four allows parties to consult if any of the party's territory or political independence feels threatened. If Article Five became invoked, it would allow NATO allies to, "provide any form of assistance they deem necessary to respond to the situation." While not formally enacted, NATO countries continue to provide support to Ukraine, as they see fit. Article Five does not limit support to just aid, it also allows the use of armed force if the defending country deems it necessary to restore or maintain peace in the North Atlantic area. The leadership in Moscow should know of these Articles, and it may contribute to why Russian hackers target other countries. Russian President Vladimir Putin could want war with NATO members directly, instead of viewing it as a proxy war.

Outlook and Implications: Assuming Moscow continues to direct military and freelance hacker groups to attack other countries, the results may negatively impact all countries around the globe. Leaders in Moscow could directly declare war on NATO members, or other countries with allies, which would cause many signed treaties to take effect, as well as trigger NATO Articles Four and Five. The 31 NATO members could all declare the use of armed forces as a reasonable form of assistance for Ukraine, or in defense of their own country. Should Russia carry out a possible cyber-based offensive and target many allied countries, regardless of their NATO status, the majority of countries in the world might end up at war with Russia.

[Bobby Roe]

CHINA: Plan to Maintain Russian Oil Supply May Include Lithuanian Invasion

Summary: With Moscow eager to win the war against Ukraine, Beijing may invade Lithuania to not only take down a common enemy but support Moscow without alarming Western powers by participating in an invasion of Ukraine. To maintain a global image of neutrality, Beijing may quietly attack Lithuania to maintain its relationship with Moscow, especially since Russia supplies most of Beijing's energy resources.

Background: Throughout the Russo-Ukrainian War, Beijing continues to publicly support Moscow while simultaneously claiming that it maintains a neutral stance. On 21 March, Chinese President Xi Jinping said that during their decades of cooperation and trade, Beijing and Moscow consistently worked on strategic projects together, shared cultural exchanges, and bolstered each other's industrial supply chains. Xi additionally said Beijing can now "expand cooperation with Russia in trade, investment, supply chain, mega projects, energy and high-tech areas," according to Xinhuanet.

Figure 1: Chinese President Xi Jinping (left) and Russian President Vladimir Putin (right) speaking during a meeting in Moscow on 20 March.

Oil and Energy: Because of Beijing's dependence on Russia for its abundance of materials necessary to keep the country's energy grid running, Beijing will likely take strategic measures to keep Moscow in its good graces, and ergo, the imports ongoing. Since the initial Russian invasion of Ukraine, Beijing's imports from Russia rose by more than 50%, according to Bloomberg. Russian energy imports, such as crude oil, coal, and gas, inflated to 88 billion dollars, thus beating out Saudi Arabia as China's top oil supplier, according to Bloomberg. If tensions between Kyiv and Moscow continue to grow, Moscow may threaten Beijing with cutting off its supply to China if Beijing doesn't attack Kyiv alongside Moscow.

Why Lithuania: Beijing and Moscow may target Lithuania because both countries see Vilnius as a common enemy. Additionally, Vilnius may serve as a substitute to Kyiv if Moscow's possible threats come to fruition. Beijing may even excuse the diverted attack with the fact that Beijing and Moscow share Vilnius as an adversary, and that if Beijing follows through with an attack on Ukraine, that event would pit Western powers against Beijing at more drastic rates. Vilnius repeatedly stood in opposition to autocratic regimes historically, such as the ones in Belarus, Beijing, and Moscow. Over the last few years, both Beijing and Moscow had several incidents involving Vilnius:

- In May 2021, Vilnius backed out of a diplomatic event where Beijing appealed to European governments and urged other European Union members to do the same.
- In November 2021, Taipei opened an office in Vilnius. A year later in November 2022, a Lithuanian trade office opened in Taipei.
- Since 2021, Vilnius, in conjunction with the European Commission, brought together a case against Beijing to the World Trade Organization.
- On 11 March 2022, Lithuania showed support for Ukraine with a large, public demonstration. Since then, it also actively welcomed Ukrainian refugees and raised funds for Ukrainian military forces.
- During the Russo-Ukrainian War, Lithuania closed off airspace to Russian planes, closed ports to Russian ships, and stopped purchasing Russian gas.
- Beijing stopped all Lithuanian imports into China, then as a result, garnered a lot of backlash from European countries that rely on Lithuania's supply chain.

- In April 2022, Vilnius withdrew its ambassador from Moscow and exiled the domestic Russian ambassador.

Quiet Solidarity: Beijing very likely wants to keep Moscow as a close confidant and will do so by enacting plans that support Moscow without taking part in the highly publicized Russo-Ukrainian War to maintain its image of neutrality. Throughout the war, Western powers criticized Beijing's actions, such as when it sent 12 shipments of body armor, drone parts, and weapons, in 2022, according to Politico. With that material support from Beijing raising eyebrows, Beijing will most likely not advance on Kyiv but may take physical action elsewhere on the globe.

Outlook and Implications: With international attention currently on Ukraine, Beijing may take this opportunity to target Vilnius while many remain distracted by the tense situations in other parts of the world. With Moscow's sights on Kyiv and Beijing's on Taipei, international spectators would likely not expect Beijing to divert and attack an exceptionally different part of the globe. If done strategically, said attack may even go unnoticed or underreported. This surprise assault on Vilnius would give it little time to react on a scale appropriate to counter Beijing's power, and its potential surrender would act both as a motivator and excuse for Beijing and Moscow to act against other, smaller countries that larger governments want possession of. Because of Beijing's attempt to distract and cover up its other atrocities by putting on an act of neutrality, any action taken by it could ultimately function to strengthen its relationship with Moscow. With how much Beijing relies on Moscow's energy supply, Beijing will very likely do something, possibly as extreme as the invasion of another country, to show Moscow that it supports it. From this show of solidarity, Beijing would also urge Moscow to continue to prioritize Beijing for its imports.

[Julia Rieth]

JORDAN: Arrest of Parliament Member Likely to Exacerbate Tensions with Israel

Summary: Tel Aviv and Amman will likely experience increased tensions due to a Jordanian parliament member's arrest and ongoing Israeli-Palestinian violence.

Development: On 23 April, Israeli Border Guards arrested Imad al-Awan, a Jordanian Member of Parliament, between the de-facto border of Jordan and the West Bank. Israeli Border Guards received credible intelligence that al-Awan continues to smuggle weapons and other contraband into Israel. An arrest video of al-Awan showed 12 machine guns, 270 small and medium weapons, and three bags with 100 kg of gold, according to Middle East Eye. Tensions between Tel Aviv and Amman continue to grow due to the violence between the Israeli Defense Forces (IDF) and Palestinians, the Al-Aqsa Mosque, and the illegal Israeli settlements in the West Bank. The House of the Jordanian King, Abdullah the 2nd, takes care of the Al-Aqsa Mosque, a significant holy site in Islam. The IDF's increased presence at the mosque prompted criticism from the King. Israel alleges that many weapons supporting various Palestinian terror groups, most notably Hamas, come across the Jordanian border. Tehran backs Hamas through funding, training, and arming. Tel Aviv's current government enacted many reforms regarding the restriction of religious freedoms, the power of judicial courts, and the power of Israeli security forces. These reforms resulted in many large protests across Israel.

Analysis: Tel Aviv will most likely use the arrested member of parliament as a scapegoat, showing that the current heavy border security practices are crucial in protecting the Israeli people. Tel Aviv will likely utilize this to focus the public attention away from domestic politics towards the perceived constant threat against the Israeli state to unite the populace in its favor. The large Palestinian population will likely motivate King Abdullah the 2nd to fight for the release of the Jordanian parliament member.

[Mason Meinzinger]

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.

Savannah Gallop, 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 431, 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