8 April 2022

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

Issue 405

Of Eagle Eye Intelligence

Authors
Sebastien Bragg
Michael Doolan
Austin Perez
Dalia Haase
Tucker Jones

Source: The Guardian

8 April 2022

Issue 405

Of Eagle Eye Intelligence

In This Issue

NORTH KOREA: Key Missile Developments Likely Signal Future Nuclear Weapons Tests

Summary: Pyongyang seems likely to test nuclear weapons in the near future in conjunction with its rapidly advancing missile program. Pyongyang possesses advanced missile capabilities, now with a vital component for successfully launching an intercontinental ballistic missile most likely developed for reaching its target safely. Nuclear sites across the nation also display signs of reactivation after a long period of decommissioning and destruction of sites that produce or refine nuclear material.

Background: On 23 March, Pyongyang launched a new type of Intercontinental Ballistic Missile (ICBM), making this the 12th launch of the year. Supreme Leader Kim Jong-un said Pyongyang will prepare for "prolonged conflict" after the ICBM landed in Japan's exclusive economic zone territorial waters. Pyongyang news outlets call the new ICBM Hwasong-17 based on the currently operational Hwasong-15. However, South Korea reported that Pyongyang launched a Hwasong-15, not a Hwasong-17. On 5 January, Kim announced military development achievements and development plans in his speech at the 8th Party Congress of North Korea. Kim specifically mentioned the Hwasong class ICBM, submarine-launched ballistic missiles, and hypersonic missiles. Pyongyang has demonstrated these technologies in 2021 and 2022, with tests of SLBMs and hypersonic missiles conducted in late 2021. Kim also stressed the need to strike targets at 9,000 miles, advance nuclear technology, and develop tactical nuclear weapons.

Missile Milestones: Pyongyang most likely possesses an operational re-entry vehicle (RV) that protects a nuclear payload from re-entering the atmosphere as it strikes its target, which Pyongyang lacked previously. Pyongyang's alleged reconnaissance satellite launches carried ICBM components used for developing multiple independently targeted re-entry vehicles (MIRVs). A MIRV can contain several nuclear warheads capable of carrying decoys that can distract missile defense systems, compared to a RV's singular warhead. Hwasong-17's design indicates that the ICBM can use a MIRV system, according to experts. Pyongyang has yet to show a successful missile launch with the RV or MIRV surviving re-entering the atmosphere. Pyongyang also did not release any footage or announce the reconnaissance satellite launches. An unknown ballistic missile also exploded soon after taking flight on 16 March. Pyongyang last tested ICBM Hwasong-15 with an RV attached in 2017 that failed. Shortly after the 2017 test, Kim paused nuclear and missile tests.

Nuclear Site Reactivation: Pyongyang resuming the product nuclear materials and reactivating a nuclear test site likely indicates Pyongyang will test nuclear bombs soon. Recent satellite imagery shows new construction of buildings and the restoration of tunnels at Punggye-ri, an unserviceable nuclear testing site. Satellite imagery also shows Pyongyang's Yongbyon Nuclear Scientific Research Center capable of producing plutonium and enriched uranium used in nuclear weapons. Kim deactivated the Yongbyon center and demolished Punggye-ri with explosives in 2018, shortly after halting all nuclear and missile tests. Kangson complex, a nuclear enrichment facility, also shows signs of activity along with the Pyongsan Uranium Concentration Plant and its associated Pyongsan Mine. Pyongson mine also produces uranium ore that the plant turns into yellowcake, a uranium concentrate, a vital component of nuclear weapons production.

Outlook and Implications: Pyongyang will most likely restart nuclear tests soon with the end of its self-imposed moratorium on ICBM and nuclear testing. The recent ICBM tests most likely happened for purely technical reasons over propaganda purposes, with an important milestone reached with RVs and MIRVs. Pyongyang probably did not possess RV technology until sometime after the 2018 ban on testing. The failed launch on 16 March likely indicates that the Hwasong-17 ICBM needs more development, which Pyongyang will likely prioritize. The Hwasong-17 will most likely launch again soon as the missile contains more technically advanced, untested components such as the MIRV. Pyongyang will likely test nuclear weapons in conjunction with the latest missile advancements requiring superior warheads to complement the ICBMs.

Pyongyang will almost certainly attempt to achieve the military goals Kim outlined in his speech at the 8th congress of North Korea. Pyongyang may construct more nuclear power facilities, as Kim hinted the Yongbyon nuclear plant remains unsatisfactory for current needs. The new facilities probably will serve the crippled energy sector over the nuclear program, but nuclear material production still seems likely to increase regardless. Pyongyang may test nuclear bombs somewhere besides Punggye-ri, as the site remains far from operational. Pyongyang may test another ICBM or nuclear capability near the Day of the Sun on 15 April, former leader Kim Il-sung's birthday, with military parades occurring during the holiday.

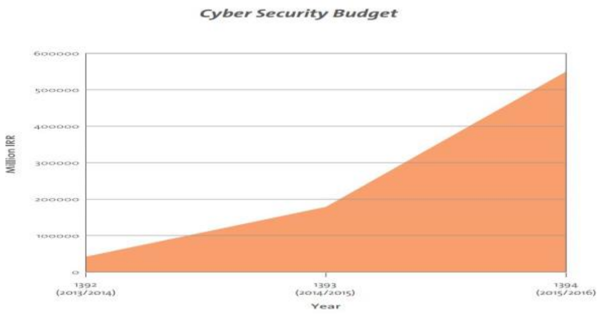
[Sebastien Bragg]

ISRAEL-IRAN: Cyber Activities Likely Indicates Growing Cyber Conflict

Summary: The activities of Jerusalem and Tehran's cyber programs likely indicate a growing cyber conflict. The secretive nature of Jerusalem's cyber program coupled with previously destructive cyber-attacks against Tehran likely indicates a robust cyber program and increased tensions with Tehran. Determined to increase its cyber capabilities to challenge Jerusalem and control a domestic dissident population, Tehran has invested heavily in its cyber program. However, this investment will still likely fail to meet the robustness of Jerusalem's cyber program.

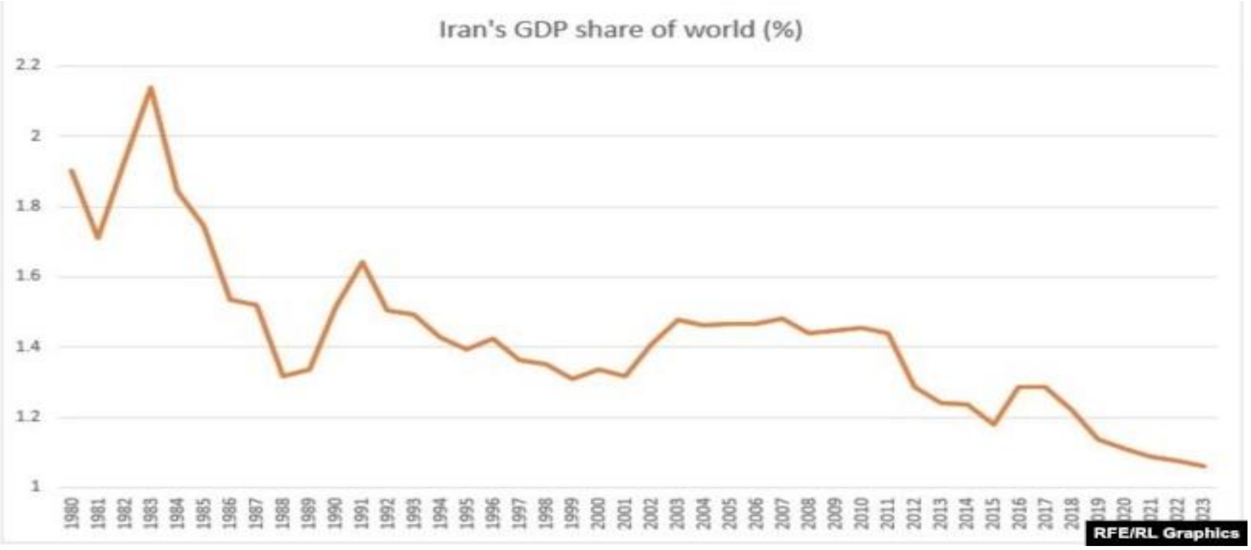
Background: Jerusalem first identified cyber as a threat to national security almost two decades ago. Rapid technological advancements reformed Jerusalem's governmental response to cyber-attacks, such as the establishment of the Israeli National Cyber Directorate, and it boasts a high defensive cyber capability. However, there remains little information about Jerusalem's offensive cyber capability due to counterintelligence efforts. To curb Tehran's nuclear program, Jerusalem allegedly created the Stuxnet worm, a powerful malicious software that disabled Iranian nuclear centrifuges, an essential component of nuclear weapons. After media outlets reported Jerusalem launched the cyber-attack, Tehran established the Supreme Council of Cyberspace. The council focuses on creating cyber strategies to target its enemies, mostly to Jerusalem, and finding ways to control its population through information restriction.

Israeli Cyber Capability: Jerusalem's cyber program, while not exactly publicly known, likely exhibits a fair degree of robustness and sophistication based on historical examples. Additionally, Jerusalem likely utilizes cyber against Tehran but refuses to publicly disclose its existence and involvement. For Jerusalem's overall cyber defense, evidence shows that Jerusalem possesses a strong cyber defense due to strong collaboration efforts between the Israeli government, academia, private sector, and key international partners. However, details relating to cyber intelligence efforts and offensive cyber capabilities remain largely unknown. Historical examples offer some insight into Jerusalem's cyber program. The Stuxnet worm, allegedly created by Unit 8200 of Israel in collaboration with the NSA, highlights Jerusalem's ability to sabotage critical infrastructure as it set Tehran's nuclear program back. In 2020, Unit 8200 launched a cyber-attack against a critical Iranian port in retaliation for a Tehran-sponsored cyber-attack against Israel's water treatment facilities. Jerusalem shifted its tactics over time, with more of an emphasis on propaganda and cognitive warfare rather than sophisticated cyber-attacks. This likely serves to influence public perception of the Iranian regime, as Tehran regularly launches disinformation campaigns to portray Israel as evil and warmongering.



Iranian Cyber Capability: Tehran's cyber program, while not exactly publicly known, likely does not meet the robustness and sophistication of Jerusalem's cyber program due to domestic problems and historical examples. Even though Tehran saw its budget for cyber increase by 1,200% from 2012 to 2016, internal issues stemming from economic sanctions, political turmoil, terrorism, and other internal deficiencies suggest that its limited resources cannot increase Tehran's cyber program quickly enough to match Jerusalem.

However, Tehran hacker proxies known as Advanced Persistent Threat groups (APTs) still attempt to hack, with moderate to low success. These APTs likely serve to shift official blame from Tehran. The technical success of most Iranian APT attacks remains low. Reports from Tehran-based cyberattacks show that Tehran regularly engages in low-impact cyber-attacks, specializing in social engineering and public defacement. Overall, Tehran-sponsored operations lack sophistication and ingenuity.



Outlook and Implications: Jerusalem and Tehran's cyber capabilities likely indicate a growing cyber conflict. Overall, a cyberwar will likely occur due to evidence of both countries ramping up their cyber program and utilizing it against each other. However, neither country will likely admit to getting hacked because of the embarrassment of having its cyber defenses penetrated. Tehran and Jerusalem will likely shift their targeting away from the more secure military organizations and shift to the less secure private sector, as recent cyber-attack trends show that targeting the private sector leads to a higher chance of successfully breaching a system. Additionally, even though Tehran likely does not possess the capability to conduct any meaningful cyber-attack against Israel, it will likely continue to try to sabotage Jerusalem.

[Michael Doolan]

AFRICA: Prolonged War in Ukraine Likely to Affect Food Supply in African Nations

Summary: Sustained conflict in Ukraine and expanded sanctions against Moscow will likely exacerbate hunger issues in African nations.

Development: On 16 March, the United Nations released a report titled *The Impact on Trade and Development of the War in Ukraine*, outlining rising issues patriating to food stability brought on by the Russia-Ukraine Conflict. The report detailed the increasing issues with wheat demand for a variety of developed and struggling African nations including Somalia, Egypt, Sudan, Congo, Madagascar, Libya, and Tunisia. The report outlined how 25 African countries import more than one-third of their wheat from either Russia or Ukraine; 15 of these nations receive over half. Furthermore, redundant suppliers lack the ability to replace imports from the Russian Federation and Ukraine through trade within Africa as wheat production appears comparatively small, and many parts of the continent lack efficient transport, infrastructure, and storage capacity. Patterns of civil unrest have coincided when food scarcity occurs in this region such as the 2007–2008 food riots and the Arab Spring of 2010.

Analysis: With the conflict continuing in Ukraine, farmers will likely face hardships in planting and harvesting seasonal crops. This will likely lead to issues with maintaining the current agriculture dependency throughout Africa. If not addressed in a rapid manner, supply and demand could lead to increased food scarcity in some of the most under-developed nations on the continent. Food scarcity will likely lead to civil unrest and possible regime changes based on similar scarcity cycles having coincided with major political events. The missing allocation of food will likely require subsidization from both government and non-government organizations to prevent unnecessary starvation and prevent civil unrest.

[Austin Perez]

RUSSIA: Hesitancy to Scale Back Despite Peace Talks Will Likely Prolong Conflict

Summary: Since the beginning of the Russian-Ukraine crisis, government officials have attempted to negotiate an end to the relentless invasion of Ukraine. Russian attacks have not significantly regressed, likely leaving Kyiv ready for further incursions.

Development: On 30 March, Ukrainian President Volodymyr Zelenskyy and Russian President Vladimir Putin began taking strides towards compromise regarding the unattainable demands Moscow placed on Kyiv. These demands originally included no association with the North Atlantic Treaty Organization (NATO), the protection of Russian language within Ukraine, recognition of Crimea as Russia, and the independence of Eastern Ukrainian regions Donetsk and Luhansk, according to VOX News. Recent events revealed negotiations between Putin and Zelenskyy, like Ukraine agreeing to remain independent of NATO and Russia conceding to the withdrawal of military presence in major Ukrainian cities. Despite minimal reduction in military activity in certain areas of Ukraine, shelling and military strikes continue near Kyiv and other large cities.

Analysis: Putin's disregard for his promise of military withdrawal likely indicates that any further negotiation for peace is futile attempt by Zelenskyy. Moscow failing to halt military operations in central Ukraine probably indicates Putin's lack of sincerity for all future negotiations, drawing the war out to what will most likely be a bloody end.

[Dalia Haase]

LEBANON: Seized Assets May Lead to Increased Stability and Bring Justice for National Bank

Summary: The European Union (EU) seized $130 million in assets that associate with corrupt bank officials in Lebanon. This will likely start a domino effect to bring justice to the members of the National Bank of Lebanon and may provide stability for the upcoming parliamentary elections.

Development: On 28 March, the EU seized $130 million in assets that belonged to members of the National Bank of Lebanon. France, Germany, and Luxembourg seized assets like bank accounts and properties within their borders from Riad Salameh, the head of the Lebanese Bank. Salameh denied all allegations of money laundering from his own country. Salameh claims his fortunes are from his previous career as a private banker. Salameh has plunged the country almost single handedly into an economic crisis while diminishing his people's savings while allowing Hezbollah to profit largely from Lebanon's currency plunge. With Hezbollah gaining more power through the country's crisis, the upcoming parliamentary elections scheduled for 15 May proves crucial for Hezbollah's future in Lebanon.

Analysis: The EU will likely bring a swift movement before the upcoming elections in mid-May. The results of the upcoming election will likely have long-lasting impacts. The Bank of Lebanon may receive justice while being overseen along with consequences dealt to violators within. This will likely bring stability to the election, which will likely remain a major goal of the EU's involvement in Beirut. The seizing of assets may impact Hezbollah's ability to act, potentially influencing its success in the May elections.

[Tucker Jones]

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.

Alli McIntyre, 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 405, 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 86301
eagleeyeintel.com