ASSESSING IRAN'S CYBER STRATEGY
RISKS TO THE FINANCIAL SECTOR

COLUMBIA UNIVERSITY | SIPA

APRIL 2021

ASSESSING IRAN'S CYBER STRATEGY

RISKS TO THE FINANCIAL SECTOR

Capstone Advisor: Adam Segal
Capstone Team: Erika Bañuelos, Clara Brackbill, Kirill Buskirk, Haakon Husoy, Jiwon Ma, Meg Mannix, Daniel Sorek, Sam Weaver

COLUMBIA UNIVERSITY | SIPA — CAPSTONE REPORT

Published in April 2021
Capstone Report
Columbia University | School of International and Public Affairs

Cover Design by Kirill Buskirk ©
Report Design by Erika Bañuelos, Kirill Buskirk, Jiwon Ma

Following Image by STP/AFP via Getty Image
Page 12 Photo by Eric Lafforgue/Art In All Of Us/Corbis via Getty Images
Page 25 Photo by Fatemeh Bahrami/Anadolu Agency/Getty Images

ASSESSING IRAN'S CYBER STRATEGY

TABLE OF CONTENTS

ASSESSING IRAN'S CYBER STRATEGY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

COLUMBIA UNIVERSITY | SIPA CAPSTONE REPORT

On request by a global financial institution, the Columbia University School of International and Public Affairs (SIPA) capstone team assessed the likelihood that the Islamic Republic of Iran (Iran) will adopt a policy of financially motivated cyber attacks against international financial institutions within a two-year timeframe. The team concludes that it is unlikely that the Iranian government will adopt the policy for two main reasons:

- The costs of the policy would outweigh the potential benefits. Despite facing international isolation for decades, Iran continues to demonstrate an interest in reintegrating into the international system. Targeting financial institutions would likely jeopardize these efforts and damage Iran's credibility as an economic partner.
- The potential gains from a financially motivated cyber attack campaign would likely be immaterial compared to the size of Iran's ~$610 billion Gross Domestic Product (GDP)[1] and would need to be of an unprecedented scale and persistence to represent a meaningful and reliable source of income for the Iranian government. For reference, the Iranian Sam Sam ransomware campaign required almost three years to target 200 victims and generate $30 million, or less than $150,000 per victim.[2]

The capstone team used structured analytic techniques to develop an assessment and a scenario analysis framework that the client can utilize to monitor ongoing developments. The capstone team interviewed leading cyber and Iran specialists in and outside the United States (US) with experience in the White House, National Security Council, the Intelligence Community, private sector, and academia to collect original insights to answer the client's novel question. The team also analyzed strategic and cyber decisions by North Korea and Iran to develop its assessment.

ASSESSING IRAN'S CYBER STRATEGY
RISKS TO THE FINANCIAL SECTOR

1 INTRODUCTION

The Columbia University School of International and Public Affairs (SIPA) capstone team has on request by a global financial institution, the client, conducted a comprehensive analytical project to assess the likelihood that the Islamic Republic of Iran (Iran) will adopt a policy of state-sponsored, financially motivated cyber attacks against foreign financial institutions. The main objective of this project is to provide the client with an understanding of the cyber threat posed by Iran, as well as an analytical framework that will enable its cyber threat intelligence team to monitor and anticipate future developments in the cyber threat landscape.

2 BACKGROUND AND OBJECTIVE

The client has tasked the SIPA capstone team with addressing the following question:

Assuming further economic isolation resulting from sanctions and/or other similar policies, what is the likelihood that Iran will adopt a policy of state-sponsored, financially motivated cyber attacks? Specifically, is Iran likely to target financial institutions in a program of cyber theft similar to that perpetrated by North Korea?

This report is meant to supply the client's cyber threat intelligence (CTI) team with a nuanced understanding of current and emerging cyber threats as they pertain to Iranian state-backed and non-state actors. In the process of researching and interviewing subject matter experts on Iranian politics, history, and cyber capabilities, the team has developed two key deliverables. The first is an analytical framework, consisting of plausible future scenarios for Iran and a list of indicators to monitor these developing scenarios. The second is a written report, comprising an assessment of the project question and scenarios deemed most likely and most dangerous if they were to occur.

Given that Iranian cyber actors have historically focused on espionage campaigns and attacks against critical infrastructure, rather than attacks on the financial sector, the capstone team examined North Korea as a case study. The comparative analysis between these two politically and economically-isolated nations aids in understanding Tehran's decision-making process as it pertains to the use of emerging cyber capabilities for financial gain. Thus, with the constraints these two nations face, understanding the risk of Iranian state-sponsored cyber attacks motivated by financial gain is crucial in assessing the dangers these actors' motivations pose to the financial services sector.

3 METHODOLOGY

3.1 METHODOLOGY AND JUSTIFICATION

The SIPA Capstone team chose the structured analytical technique, ***scenario analysis*** (also known as ***alternative futures*** or ***scenario planning)***, to address the project question posed by the client.[3]

A scenario analysis is a framework for considering and generating a range of plausible futures. It is particularly useful when assessing complex, evolving, and uncertain situations where predicting a single outcome is both difficult for the analysts and not ideal for decision-makers, who rely on the assessment to plan for a range of possible futures. The framework also helps to hone the analysts' attention on the key underlying and driving forces that are most likely to impact how the situation develops.[4]

Scenario analysis offers several benefits that are of particular relevance to this project. First, whether a state actor adopts cyber operations for financial gains depends on a multitude of uncertain and interacting factors. Scenario analysis provides a structured framework to handle this complexity, and a means to analyze how the factors might develop, interact, and manifest as future scenarios.[5] Second, pursuing such operations would be an unprecedented course of action by Iran. Scenario analysis is an efficient tool to anticipate what would otherwise be surprising developments by challenging assumptions and forcing analysts to also consider low-risk, high-impact events.[6] Third, scenario analysis creates a living framework that can continually be adjusted and updated.

3.2 ANALYTICAL PROCESS

The capstone team initially conducted literature reviews and structured interviews[7] with a range of subject matter experts to gain a comprehensive understanding of the project question and a foundation to build the scenario analysis framework.

3.2.1 Literature Review

While the literature that specifically addressed the project question was limited, writings on current Iranian offensive cyber operations provide insights into the motivations and severity of attacks. Other works on Iran's strategic environment, policy preferences, domestic interests, and foreign policy also helped the group consider how Iranian cyber operations might shift in the future.

There is widespread agreement that past Iranian government cyber attacks on the financial sector—such as the 2011-2013 DDOS attacks on US banks—were motivated by grievance retaliation, as opposed to financial benefit, and that future attacks on the financial sector could be similarly motivated. Furthermore, most analysts have argued that the financial sector would remain a high priority target for the Iranian government and a likely candidate for future attacks.[8] These attacks are low cost and Tehran may consider them as relatively non-escalatory, compared to attacks on US government infrastructure.[9] Moreover, the financial services industry's status as a symbol of the US economy make it attractive to Iran.[10]

Even as analysts agree that the international financial sector would be a priority target, there are competing hypotheses regarding the impact of increased sanctions pressure on the future direction of cyber attacks. Following the 2012 implementation of widespread sanctions on the Iranian financial and energy sectors, as well as the 2018 US "maximum-pressure" campaign, some hypothesized that Iran would retaliate with destructive attacks on the US financial system because the sanctions had effectively cut Iran off, and so there would be limited costs.[11] Others pointed out that even when blocked from accessing the US financial system, a systemically destructive attack would be detrimental to Iran's sanctions evasions tactics that depend on illicit access to the system.[12]

None of the current studies explicitly address the report's question. Insights on possible future developments were drawn from studies of (Healey et al., 2018), (Lewis, 2019), and (Fixler, 2020), among others.

3.2.2 North Korea Case Study Justification

This report examines the domestic politics as well as the strategic goals and challenges that have motivated North Korea to implement a policy of financially motivated cyber attacks as a case study. While Iran and North Korea have different geopolitical backgrounds, the two countries threaten the international order with nuclear development and sanctions evasion in pursuit of regime stability.

While both countries maintain strict control over their borders, North Korea restricts its citizens' access to the internet and foreign materials meanwhile the Iranian government focuses on silencing dissidents and the Iranian diaspora who challenge the regime's policies. Both countries' economies continue to shrink due to various international sanctions regimes. However, North Korea experiences much deeper economic pressure and political isolation, to the point that it relies on cyber operations to generate revenue for regime stability (such as the funding for the nuclear weapons program). North Korea's Byungjin policy emphasizes simultaneous economic growth and development of nuclear weapons programs. North Korea undertakes ambitious cyber operations that target financial institutions to evade sanctions and generate revenue for the regime. For North Korea, financially motivated cyber attacks are a statecraft tool to disrupt the international financial system. One example of this is the 2016 Bangladesh Central Bank Heist that aimed to disrupt the SWIFT system.

Iran views itself as an important stakeholder in the region and strives to influence the outcomes of a variety of issues within the Persian Gulf and wider Middle East. Various actors, such as Iraq and Bahrain, have accused Iran of intervening in their domestic affairs. Iran's cyber operations focus on espionage, destructive effects, and quelling dissent directed towards the regime. Unlike North Korea, Iran maintains a wide array of diplomatic and economic links to the international system, despite rhetoric by the Supreme Leader emphasizing resistance and a political willingness to adapt policy in the face of economic pressure. Financially motivated cyber attacks have so far not been used because they may present greater potential losses than benefits. Thus, this report examines North Korea and Iran's similarities and differences to understand the necessary conditions and likelihood that Iran will attempt to use its cyber capabilities to attack the financial system.

3.2.3 *Identification and Analysis of Drivers*

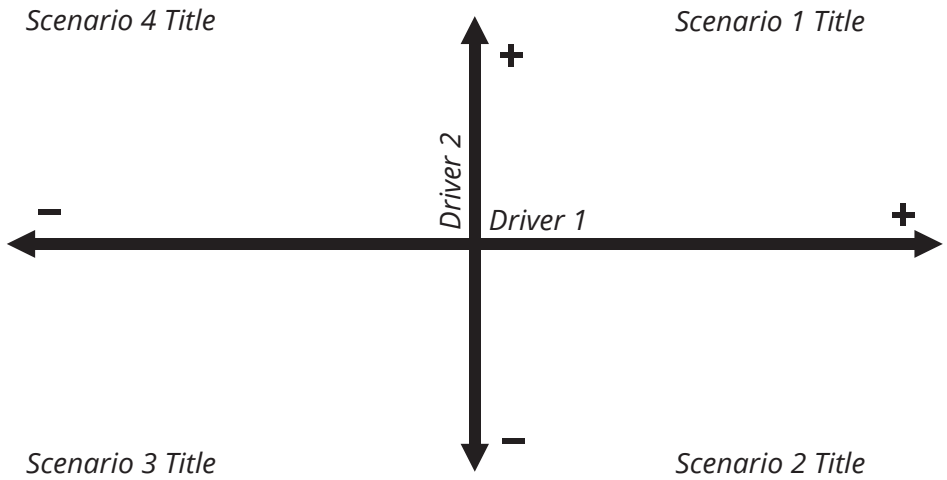
Using inputs from the literature review and interviews, the capstone team employed a structured brainstorming analytical technique to nominate a wide range of variables, hereby referred to as drivers, that could impact the focal issue.[13] The driver selection criteria were initially left flexible to encourage creativity and new ideas. A total of 20 drivers were eventually nominated and organized into categories based on the Political, Military, Economic, Social, Information, and Military (PMESII) framework.[14]

The capstone team reduced the preliminary list down to ten drivers for further analysis by removing the least practical drivers. The remaining list of drivers was analyzed using a ***paired comparison matrix***—a technique used to assign a score to rank and visualize the most important drivers relevant to each other.[15]

In order to assess the importance of the drivers, two main criteria were employed: (1) the likelihood that a driver would be subject to change within the next two years, and (2) the impact that a driver has on the focal issue. The paired comparison matrix technique ultimately helped the team determine which two key drivers were most important to the future development of the focal issue.

3.2.4 *Scenario Development*

Using the two identified key drivers, the capstone team developed a 2x2 scenario matrix with the horizontal dividing line representing the first driver's spectrum, while the vertical dividing line represented the second driver's spectrum. The two ends of each line represented the extremes of each driver's spectrum. For example, if driver one represented "Iran's GDP", the right end of the horizontal dividing line would signify a strong GDP, while the left end would signify a weak GDP (see illustration below).



A total of four scenarios were generated using a combination of the two drivers, represented by each of the four quadrants of the matrix illustrated above. The team then developed a narrative for each hypothetical scenario, which included a hypothetical chronology of key dates and events, along with the implications should the scenario arise.[16]

In addition to generating the scenarios, the capstone team also identified the scenario most dangerous (MD) to the client's business and operations, and the scenario most likely (ML) to occur. The capstone team described the justification and background for both assessments in this report.

3.2.5 Indicator Development

Upon completion of the scenario development, the capstone team developed a list of indicators for each scenario. These indicators can assist the client's CTI team in determining which of the four developed scenarios appears closest to real world events. An indicator list is a set of observable actions, conditions, facts, or events, that can be monitored to obtain strategic warning of a future development and track an emerging scenario.[17]

Indicators were nominated using a structured brainstorming[18] technique and then assessed against the following pre-defined criteria:

- **Observability**
- **Validity**
- **Reliability**
- **Stability**
- **Uniqueness**


당창건 65돐
강성대국건설사에 특기할
전변의 해로!

4 BACKGROUND

4.1 CYBER THREAT LANDSCAPE

Cyber operations of advanced persistent groups (APTs) and non-state actors are becoming more sophisticated and attacks more damaging to both financial institutions and their customers. According to Verizon's 2020 Data Breach Investigations report, 91% of cybersecurity incidents in North America are financially motivated, compared with 70% in the Europe, Middle East and Africa (EMEA) region.[19] Cyber actors attempt to steal personal and confidential information in order to infiltrate the networks and systems of financial institutions, impacting customers' trust and reliance on financial institutions across the globe. An increased reliance on mobile bank and payment services offerings, smartphones, malware disguised in the form of mobile applications and contactless point-of-sale (POS) terminals constitute additional opportunities for cyber attacks. For example, the North Korean APT group, known as the Lazarus group, executed financially motivated cyber attacks on behalf of the North Korean regime. Today, the Lazarus group and its subgroups continue to target international financial systems, leaving financial institutions and their major stakeholders vulnerable to potential cyber attacks while allowing the North Korean government to evade international sanctions. Iran faces similar economic constraints as North Korea due to international sanctions.

4.2 NORTH KOREA CASE STUDY

The Kim Family regime has governed the Democratic People's Republic of Korea (DPRK or North Korea) since 1948.[20] Almost thirty years later, under the leadership of Kim Jung Il, the authoritarian country began taking steps to develop nuclear weapons.[21] The US and its allies responded by employing financial and diplomatic sanctions in order to apply pressure on North Korea's economy and military. Negotiations between North Korea and the international community have stalled several times and while the sanctions and other tools have slowed the DPRK's development of nuclear weapons, they have not been successful in terminating the program.

4.2.1 Strategic Goals and Challenges

The main national objective of North Korea is to preserve the Kim family regime through four strategic goals: (1) reunify the Korean peninsula and remove US forces; (2) simultaneously develop its economy and nuclear weapons program (***Byungjin*** policy) (3) gain international recognition as a nuclear power; and (4) maintain restrictive control over its borders.[22]

The DPRK continues to develop irregular and asymmetric military capabilities to deter potential attacks by the US and South Korea.[23] According to current analysts, Kim Jong Un perceives nuclear weapons as not only a means to guarantee regime survival but also a deterrence against the US and its allies.[24]

The decrease in Russian and Chinese patronage has exacerbated economic pressures on the DPRK since the Cold War. The DPRK relies on cyber theft to fund nuclear programs and evade sanctions.

4.2.2 Important Cyber Organizations and Incidents

North Korea relies on offensive cyber operations as a low-cost method to carry out the regime's strategic goals in cyberspace. The DPRK's three main motivations for cyber attacks include disruption, espionage, and financial gains.[25] The DPRK's cyber attacks fall below the usual threshold for effective deterrence, ensuring little operational risk to the regime. It mainly targets the United States, South Korea, and Japan to collect intelligence and cause disruption.[26]

Two older traditions influence the DPRK's cyber strategy: (1) the disruption of opposing conventional operations through asymmetric means; and (2) the peacetime use of disruptive provocations.[27]

- The first tradition executes irregular peacetime operations to sidestep conventional deadlock on the Korean peninsula and coerce its opponents.[28] Its cyber operations against ROK targets resemble this strategy or provide a lower-cost alternative without the risk.
- The second tradition emphasizes disrupting the status quo while guaranteeing little risk of immediate retaliation. The DPRK operates below the threshold of kinetic war since it could not survive a conventional conflict.[29]

The DPRK's cyber capabilities are developed primarily under the Reconnaissance General Bureau (RGB) and the Korean People's Army (KPA)'s General Staff Department (GSD).[30] Cyber operations, such as psychological warfare and propaganda, are conducted by the RGB and GSD with other smaller agencies. The Korean Worker's Party (KWP) is also known to conduct small intelligence operations.[31]

The RGB was formed in 2009 following a government reorganization, combining the KWP and the Ministry of People's Armed Forces (MPAF).[32] It is the central hub of intelligence, commando, and sabotage operations.[33] It is suspected to be the leading organization that orchestrates the DPRK's cyber operations, including research and intelligence collection.[34]

The RGB consists of seven bureaus: 1st Bureau Operations, 2nd Bureau Reconnaissance, 3rd Bureau Foreign Intelligence, 5th Bureau Inter-Korea Dialogue, 6th Bureau Technical, 7th Bureau Rear Services, and Bureau 121.[35] Bureau 121 is the DPRK's most important cyber unit that conducts a range of cyber missions:[36]

- **Lab 110**: develops hacking techniques and malware.[37]
- **414 and 128 Liaison Offices**: support intelligence collection using cyber espionage.[38]

- **Unit 180**: leads financially motivated cyber attacks abroad.[39]
- **Unit 91**: targets isolated networks, particularly on ROK's critical national infrastructure.[40]
- **Associated state-sponsored actors include**: Lazarus, BlueNoroff, HIDDEN COBRA, Andariel, APT37, ScarCruft, Reaper, and Group123.[41]

The GSD is led directly by Kim Jong Un for operational command and planning and management of the KPA. Cyber operations involve five bureaus of the GSD:

- **Operations**: makes key decisions on cyber force planning.[42]
- **Communications**: secures KPA communications and monitors domestic and foreign telecommunications.[43]
- **Electronic Warfare (EW)**: trains all EW and electronic intelligence assets within the KPA.[44]
- **Command Automation**: conducts computer network operations, develops malware, and searches for exploits.[45]
- **Enemy Collapse Sabotage (Unit 204)**: conducts psychological and information warfare, spreading anti-ROK propaganda.[46]

Due to North Korea's separation from the Internet, North Korea is able to operate in cyberspace with little reprisal. North Koreans have limited access to the Internet, which means that any cyberspace operations targeting the DPRK have a limited impact on its economy.

- North Korean cyber actors use third-party nation Internet infrastructure, primarily through Chinese and Russian networks. Operating in third-party countries provides them access to the internet and a stable electricity supply, allowing them to overcome cyber infrastructure limitations and avoiding the use of North Korean IP addresses to conduct these cyber operations.[47] For example, New Zealand's network is the primary hub for North Korea's BitTorrent, video streaming, and gaming services activity.[48]
- North Korean traffic in Malaysia has decreased over the past several years, especially with Malaysia-North Korea relations degrading in recent years in the wake of Kim Jong Nam's assassination and other political events.[49]
- India, Nepal, Kenya, Mozambique, Indonesia, China, Thailand, and Bangladesh may wittingly or unwittingly host North Korean cyber actors within their networks.[50]

North Korean cyber operators continue to execute low-intensity disruptive cyber attacks that do not result in extensive damages but erode the confidence of critical infrastructure and commercial sectors.[51] The DPRK's operational military strategies integrate cyber operations, such as reconnaissance and espionage for mission assurance.[52] Furthermore, North Korea is increasingly relying on cybertheft to generate revenue for the regime and evade international sanctions. North Korea's increasingly sophisticated cyber capabilities pose a disruption to international financial systems and damage the integrity of the cyber infrastructure of its highly networked targets.

North Korean cyber operators use similar tactics, techniques, and procedures (TTPs) to target financial institutions. The attackers used stolen credentials to initiate fraudulent transfer requests to the SWIFT network, obfuscating the evidence of fraudulent transfers by using malware.[53] Cyber operations are persistent over a long period since the nature of cyberspace operations requires sufficient time for cyber operators to understand its target to infiltrate into their systems.[54]

- Traditionally, the DPRK's cyber operations are cost-effective, using less sophisticated attacks, making tradeoffs between the cost and effectiveness of the attacks based on timeliness and barriers to entry of targets.[55]
- The most common method of exploits is zero-day exploits based on frequently used programs of its adversaries, such as Adobe Flash and Hangul Word Processor (HWP) files.[56]

4.2.3 Economic Environment and Sanctions Implications

The DPRK economy is one of the most closed off in the world. While it does not publish economic data, widely-used Bank of Korea (BoK) data estimates the DPRK's 2019 real GDP at $32.9 trillion KRW ($28.3 billion), a 0.4% expansion from 2018.[57] This compares to respective 3.5% and 4.1% GDP declines in 2017 and 2018.[58] DPRK's 2019 exports were estimated at $280 million and its imports at $2.97 billion.[59]

UN Security Council sanctions on the DPRK have gradually increased since 2006 in response to nuclear proliferation activities, with most new sanctions levied in direct response to repeated DPRK missile tests. The strength of the sanctions increased beginning with UN Security Council Resolution (UNSCR) 2371 in 2017, which closed a UN sanctions exemption that had previously allowed DPRK to continue exporting coal to preserve "people's livelihood."[60] By the end of 2017, the DPRK's major export commodities—such as coal, minerals, textiles, marine products, and electrical equipment—had been banned along with imports of luxury goods, machinery, and metals. Also, Iran was once again disconnected from SWIFT. Narrow limits on petroleum imports and overseas labor authorizations were also enacted.

US unilateral sanctions have expanded UN sanctions and maintained secondary sanctions provisions that block individuals or entities that facilitate unsanctioned North Korean trade or offer correspondent banking services from the US financial system. They have been primarily focused on impeding the DPRK's missile and nuclear technology programs but have also been enacted in response to several DPRK-attributed cyber attacks.[61] These include the 2014 breach of Sony's computer systems, in retaliation for the release of the film, "The Dictator", and the 2017 WannaCry ransomware attack.

The DPRK has also been fully cut-off from the SWIFT interbank messaging system for cross-border transactions since 2017. SWIFT is the primary method by which financial institutions communicate cross-border payment instructions with each other, and is overseen by the G-10 central banks. According to the UNSC, prior to being cut off, North Korea had been utilizing its access to the network in order to flout international sanctions.[62]

The sanctions' impact has been debated by North Korean experts. Since the imposition of the enhanced sanctions in 2017, exports have decreased by 90.1% and imports have decreased by 20%.[63] In line with the UN sanctions, Chinese customs data has not reported any textile or coal imports from the DPRK, and most other countries have entirely ceased official trade.[64]

Despite these major contractions, estimates of basic food, commodity, and petroleum prices, along with the USD-KPW market exchange rate within the DPRK have all remained relatively stable since the imposition of enhanced sanctions. This price stability points to the DPRK's ability to maintain a basic level of economic durability despite severe sanctions restrictions.[65] Stable internal petroleum prices also indicate that overall petroleum supply is stable as well, despite UNSC Resolution 2397 that mandated an import cap of 500,000 barrels per year.[66]

Sanctions Evasion

The DPRK is extremely adept and prolific in its sanctions evasion actions. It utilizes a range of clandestine techniques, including increasingly through cyber means, in order to conduct sanctioned trade and access illicit funds. The UNSC estimates that the DPRK has obtained a total of $2 billion from cyber methods alone.[67]

Offensive Cyber Methods:

- **Financial Institutions**: The DPRK has successfully penetrated the internal networks of banks located in

Vietnam, Bangladesh, Taiwan, Mexico, Malta, and Africa, stealing more than $1.2 billion between 2015 and 2019.

- **Virtual Currencies**: Since 2017, Lazarus Group has targeted over 100 cryptocurrency exchanges in efforts to gain cryptocurrency for direct financial gain as well as for use in laundering schemes. In a single hack of the major cryptocurrency exchange, Kucoin, Lazarus successfully stole $275 million, representing more than half of total stolen crypto assets in 2020.[68] It is estimated that Lazarus has stolen $1.75 billion in crypto assets since formation. DPRK agents also sold Initial Coin Offering (ICO) Marine Chain tokens that falsely offered investors shares in Singapore maritime ventures.[69] It is unclear how much money was raised from these sales. DPRK has also engaged in bitcoin and monero mining in order to generate funds and launder profits.[70]
- **Ransomware**: The DPRK has successfully employed malware to extort funds from businesses around the world, and have been recently increasing their capability.
- **ATM Cash-outs**: Following the installation of malware on a financial institution's network, DPRK hackers intercept ATM transaction data and cause fraudulent ATM withdrawal requests to be approved. Networks of mules would attempt to withdraw ill-gotten funds at the same time to achieve as much cash as possible prior to the operation being shut down. These mules would sometimes be DPRK agents, and sometimes third-party networks operating in coordination with the DPRK.

Other primary sanctions evasion methods:

- **Illicit Transshipments**: According to the UN Security Council Sanctions Committee on North Korea, there were a total of 221 illegal transshipments of petroleum products into North Korea in 2019.[71] Depending on the capacity of the identified transshipments, North Korea illicitly imported between 1.73 and 4.67 million barrels in addition to the 500,000 that were officially allowed under the sanctions provisions.[72] If these transshipments were filled to 90% capacity or higher as reasonably expected, the DPRK has seen almost no change to its petroleum supply despite international sanctions. The UNSC Committee also reported that the DPRK was able to export 4.1 million tons of illicit coal to China between January and August 2020 despite an import ban pursuant to UNSCR 2371.[73]
- **Obfuscation Techniques**: The DPRK uses a range of basic to more advanced obfuscation techniques such as flag and name changes, night transfers, ship identity theft, and false Automatic Identification System (AIS) transmissions make these illicit transshipments viable and sustainable. They are also abetted by shipbrokers and trading companies that maintain lax due diligence and compliance practices due to either negligence or an interest in securing considerable arbitrage profits that purchase and resale of below-market price North Korean exports can elicit.
- **Bulk Cash and Gold Smuggling**: The DPRK's agents physically carry cash and gold obtained abroad in exchange for exports into North Korea. According to the UNSC Committee, representatives of two DPRK arms firms were monitored flying between Tehran and Dubai more than 262 times between 2014 and 2016, suspected of carrying cash as a part of a money laundering scheme.[74] The DPRK has successfully sold arms to the Houthis in Yemen as well as militant groups in Uganda and Sudan, by way of a Syrian arms trafficker.[75]
- **Shell and Front Company Networks**: The DPRK has successfully used these networks to obfuscate beneficial ownership information and form joint ventures with unsuspecting foreign companies who do have access to the US financial system. The DPRK's agents have also opened bank accounts held in the name of front companies at Chinese banks that have correspondent banking relationships with the US. A recent DOJ indictment uncovered a web of more than 250 shell companies that successfully laundered over $2.5 billion in assets through the international banking system to the DPRK's Foreign Trade Bank.[76]
- **North Korean Overseas Laborers**: DPRK nationals continue to work overseas and generate income for the DPRK through remittances despite a UNSC resolution 2397 mandate that all DPRK overseas

laborers return to their home country as of December 22, 2019. Prior to the deadline, the US State Department estimated that there were about 100,000 DPRK workers abroad generating between $200 and $500 million in revenue per year.[77]

- **Information Technology Services**: Clandestine DPRK IT companies have inserted themselves into global corporate supply chains where they are able to sell IT-services products without their customers realizing their identity.

4.3 IRAN BACKGROUND

4.3.1 Domestic Politics and Government Structure

Historical Perspective of Isolation

Iranian perceptions of the international order and the outside world are heavily informed by the country's historical relationship with the US. The US saw Iran as a steady source of oil and as a regional counterweight to the Soviet Union.[78] In 1953, the Central Intelligence Agency (CIA) carried out a coup against Iran's elected Prime Minister, Mohammad Mossadegh, a beloved Iranian political figure who had nationalized the Iranian oil industry, which resulted in huge losses for the United Kingdom.[79] In response, the United Kingdom (UK) turned to the CIA for help, which led to the overthrow of Mossadegh and restoration of full power to Mohammed Reza Pahlavi.[80] This intervention soured Iranian public consensus on Washington's influence in the region.

Amidst growing dissatisfaction with the regime's governing style, opulence, and perception of a corrupt relationship with the West, the 1979 popular uprising against Reza Shah resulted in the installation of Ayatollah Ruholla Khomeini as the Supreme Leader. The US has worked to isolate Iran since its inception as retaliation for holding US Embassy employees hostage.[81] Since then, Iran's sense of isolation has been reinforced by the international community's failure to restrain Iraq during the 8-year war and more recently, the 2001 invasion of Afghanistan and 2003 invasion of Iraq.

Iranian Shi'ism further isolates the country from the region. While Shi'ism existed in Iran long before the Ayatollah, the integration of religion and politics solidified regional fears of exportation of the Shi'a revolution, further entrenching Iranian isolation. Among Iranian citizens themselves, most are religiously moderate and see the strict rules placed on daily life as tyrannical.[82, 83] Shi'ism is certainly utilized by those in power to maintain firm control over the public—following Green Movement protests, the regime used cyber capabilities to suppress dissent. The religiosity of the state, however, does not accurately represent that of the population. In fact, there is a popular desire among Iranians to be seen by the world as they are: young, highly educated, and modern. The dissonance between international perception and domestic reality leads to domestic challenges for Iranian leaders.

The Supreme Leader

Iran is governed by the Supreme Leader, Ayatollah Khamene'i, who oversees the executive, parliamentary and judicial branches of government. The supreme leader is selected by an Assembly of Experts based on candidates' piety, expertise in Islamic law, and political acumen. There are no term limits on the supreme leader, and so Iran has only seen two leaders since the revolution: Ayatollah Khomeni from 1979 to 1989, and Ayatollah Khamene'i from 1989 to the present.[84]

The Ayatollah sets overall policy direction, paying special attention to regional and national security issues. Both Ayatollah Khomeni and Ayatollah Khamene'i have expressed extreme hatred of the US and Israel during their respective tenures, and thus pursued an aggressive forward defense strategy to buttress Iranian interests abroad. Ayatollah Khamene'i often blames the West for Iran's internal dilemmas and calls for a self-sufficient Iran.

The President

From a western perspective, it is important to note that while the Iranian president is elected by a citizen electorate and is responsible for the day-to-day administration of government and implementations of laws, the presidential candidates must be approved by the Ayatollah, effectively limiting the possible candidates to a very small pool of conservative Shia islamists.[85]

Nonetheless, Iranian experts note that since the 1979 revolution, each president has tested the office's boundaries and authorities.[86] Current President Rouhani, formerly the chief nuclear negotiator, was elected in 2013 and seen as a moderate. He initially walked a fine line between calling for freedom of expression and criticizing the clergy, political establishment, and Islamic Revolutionary Guard Corps (IRGC) and ultimately calling for unity.[87] While President Rouhani has resisted intervening in the Ayatollah's direction of foreign policy, he did initially stress the importance of maintaining relations with the US, for which he received criticism from hardliners.

The Islamic Revolutionary Guard Corps

The IRGC is a military and internal security force primarily responsible for pursuing Iran's regional and foreign policies through its Quds Force.[88] The US Department of State formally designated the IRGC as a foreign terrorist organization in 2019.[89] Following the Iraq-Iran war, the IRGC was in charge of rebuilding Iran's infrastructure. This allowed them to take on an expanded role in society and the economy.[90] Following the 2009 Iranian Green Movement and American sanctions imposed in 2010, the IRGC's role once again expanded. It started to establish dozens of companies to act as fronts to circumvent US-imposed sanctions through large-scale smuggling operations.[91] The IRGC has invested in all sectors of Iran's economy and current estimates suggest that the IRGC retains control over approximately 20% of the national economy.[92]

4.3.2 Strategic Goals and Challenges

The Iranian state exists to safeguard its national sovereignty, security, and revolutionary ideals by diffusing and defeating both internal and external threats and enhancing their role and influence as a genuine regional and global power.[93, 94] To do so, Iran attempts to achieve comprehensive and sustainable long-term development culturally, politically, economically, and militarily through its support to allied groups, use of terrorism, military action, and other soft power tactics.[95]

On a more granular level, Iran's pursues its strategic goals by limiting economic contraction and domestic strife by skirting sanctions; competing with regional actors including Saudi Arabia and Israel; continuing to fund regional proxies in Iraq, Yemen, and Syria; and disrupting domestic terrorist threats, particularly by radical Sunni groups, such as ISIS and Al Qaeda, ethno-separatist groups, and the Mojahedin-e Khalq (MeK) opposition group.[96, 97]

4.3.3 Important Cyber Organizations and Incidents

Iran's historical activity in cyberspace

Cyber is an important tool for the Iranian military and intelligence communities in their asymmetric offensive and defensive operations.

Iran has been considered a lower-tier cyber adversary given its preference for less sophisticated tactics, techniques, and procedures (TTP). These TTPs include social engineering, spear-phishing, password spraying, and DDoS attacks, the last of which are now generally considered less novel and destructive in their effects. However, Iran has improved its cyber capabilities. Various Iranian-attributed cyber operations–such as the 2012 Shamoon Malware attack on Saudi Aramco, the 2020 alleged attempt to tamper Israel's National Water System, and even the 2020 use of influence operations against the US presidential elections–collectively demonstrate (1) Iran's acquisition and/or development of sophisticated, destructive tools and (2) its improved

targeting capabilities. Appendix C contains select Iranian-attributed cyber operations that illustrate various targets, capabilities, and intentions. Below are several noteworthy observations, particularly as they relate to the question posed by the client.

- Historically, Iranian government cyber entities have not directly pursued financially motivated cyber attacks. Iranian government-linked operations have targeted the financial sector primarily to achieve destructive, punitive, or deterrent effects rather than the financially motivated goals displayed by North Korean cyber operations.
- Recently, Iranian actors have successfully pursued financially motivated cyber attacks. The connection between these operations and the Iranian government is debated and remains unclear. It is not possible to conclude that these recent operations suggest a material change in Iranian cyber policy towards financial gain. However, this observation does not entirely eliminate the possibility that seemingly independent, criminal Iranian actors pursuing financially motivated cyber operations are connected to the government.[98] A FireEye analyst has shared her high confidence assessment that the actors responsible for the financially motivated attacks against Israeli targets, in August to September 2020 and December 2020, have previously executed operations with other intentions on behalf of the Iranian government using the same tools. While the analyst is unable to determine whether the Iranian government is directing these groups to pursue financially motivated attacks, she believes with high confidence that the Iranian government is aware of the decisions made by these contractors. It is also important to consider the broader intentions of certain cyber attacks that may be obfuscated as financially motivated.[99]
- The Iranian government's reluctance to pursue financially motivated attacks may stem from a variety of reasons. The risks may outweigh the rewards. The risks associated with such a strategy may include detection, blowback in the form of further isolation from the international financial system, and perhaps unintended encouragement of domestic financially motivated hacking. Instead, Iran's focus has been to direct its cyber capabilities towards graver and more immediate national security concerns relating to regime preservation and establishing deterrence against domestic and external actors. While Iran has perhaps demonstrated a lack of will, subject matter experts have assessed with high confidence that it could choose to develop the requisite capabilities for significant financially motivated cyber attacks overnight either through organic means or renting tools from third parties.[100]
- Iranian actors have demonstrated the ability to persistently and effectively conduct financially motivated attacks, though primarily through ransomware or ATM cash-outs. Analysts assess with high confidence that Iran lacks a SWIFT hacking capability similar to the one developed by North Korea. Given the organizational coordination and investments required to successfully execute SWIFT attacks, the time to achieve this capability may extend beyond two years with the potential to be shortened if acquired inorganically.[101]
- Iran's cyber capabilities have grown with respect to: the sophistication of tools employed; the diversity of well-defended targets spanning individuals, corporations, governments, and countries; and the increasing degree of damage, financial and other, that these operations display in their outcomes or potential.

Iran's development of this capability is recent relative to the world's leading cyber actors. Many analysts believe that Iran's decision to ramp up its capabilities was made in response to the reported damage caused by the Stuxnet malware virus, a joint operation attributed to the US and Israel that targeted the industrial control systems of Iran's suspected nuclear weapons programs. The extent of Stuxnet's surprise and damage, to what many consider one of Iran's primary national security goals, likely catalyzed the perceived need for cyber capabilities to pursue varying goals including:

- **Prevent future cyber operations or limit their effects**. Understanding how and why both successful and unsuccessful cyber operations occurred allows the Iranian government to continuously improve its understanding of the broader domain.
- **Punishment and destruction**. This is primarily achieved by targeting various critical infrastructure sectors as seen in the 2011-2013 DDoS attacks against the US financial sector and the 2012 Shamoon

Malware attack against Saudi Arabia's petroleum and gas companies. Iran has attacked US critical infrastructure with limited success. However, ongoing reconnaissance may allow it to hold vulnerable US assets at risk in a future conflict.[102] Iran typically avoids targeting government assets.[103]

- **Surveillance**. Iran typically targets the aerospace, defense, natural resources, and telecommunication sectors.[104] Furthermore, Iranian actors have targeted vulnerabilities within company supply-chain systems.[105]
- **Retaliation while avoiding escalation**. Iranian leaders generally prefer kinetic means for retaliatory effects, particularly in response to destructive covert actions such as assassinations of Iranian personnel or other sabotage operations. Nevertheless, several examples exist of Iran's use of cyber capabilities to retaliate in a low-cost manner[106] and demonstrate brinkmanship without crossing the threshold of war. These include: the 2014 $40 million destruction of Las Vegas Sands Corporation computer equipment[107] in response to the CEO Sheldon Adelson's public call for military action against Iran; a year-over-year doubling in overall cyber attacks against the US in the first half of 2019 after the imposition of additional sanctions;[108] and the 2020 defacement of US government websites, in conjunction with ballistic missile attacks against the US' Al Asad airbase outside Baghdad, in response to the assassination of Qassem Soleimani.[109]
- **Domestic surveillance and silencing regime threats**. These include (1) regime critics located in and outside of the country's borders and (2) ethnic minorities–such as Iranian-Arab, -Baluch, and -Azeri citizens–who intentionally or unwittingly raise concerns over increased autonomy or self-determination that challenge the current regime's legitimacy. The Iranian government's strategy in cyberspace includes protecting the regime's stability and spreading its values, making its cyber capabilities both a source of national pride but also a tool for suppressing resistance movements.[110] The Iranian government often receives support from independent "Patriotic Hackers" to pursue this goal.

Given the noted improvements in Iran's cyber capabilities, some analysts now regard it as almost on par with China and other leading cyber adversaries.[111] Nevertheless, Iran faces organizational challenges across its various cyber agencies, which are discussed in greater detail below.[112]

Iranian cyber agencies

Iran's offensive cyber activities are primarily overseen by the Ministry of Intelligence and Security (MOIS) and the IRGC. The former is similar to the US National Security Agency (NSA) and conducts Signals intelligence (SIGINT). The latter is a branch separate from the Armed Forces that reports directly to the Supreme Leader and is dually tasked with preserving the 1979 Islamic Revolution and executing foreign special operations. The IRGC directly oversees both the Electronic Warfare and Cyber Defense Organization and the Basij Cyber Council, an elite force falling under the Basij volunteer, paramilitary organization.[113] Targets of the IRGC and the MOIS have included Iranian government critics, private corporations, and nation states such as Israel, Saudi Arabia, and the US.

While the Iranian government maintains its own cyber capabilities and personnel, analysts note that Iran lacks an established, mature, top-down cybersecurity ecosystem.[114] Indeed, they point to the contracting model that officers and operators in these government agencies pursue with various underground Iranian criminal groups.[115,116] In this manner, "an ideologically and politically trusted group of [government] middle managers translate intelligence priorities into segmented cyber tasks which are then bid out to multiple contractors… [leading to] a quasi-capitalistic system that pits contractors against each other for influence with the Iranian government."[117] Indeed, the Iranian government relies on approximately 50 organizations that compete for government contracts to create products or services and on local universities to recruit new talent. As a result, the number of Iranian, non-state threat actor groups are wide-ranging, with varying capabilities and motivations. Noteworthy Iranian APT groups include the following:

- **APT 33** is a suspected threat group that has carried out operations since 2013 against organizations across multiple industries in the US Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.
- **APT 34** is a suspected threat actor that has targeted organizations in the financial, energy, government, chemical, and telecommunications sectors worldwide for the purpose of espionage.
- **APT 35**, also known as Phosphorus, has been active since 2014 and conducts long-term operations to collect intelligence from the US and Middle Eastern defense, diplomatic, and government personnel, as well as private companies.
- **APT 39** is a cyber espionage group that has been active since 2014 and has targeted telecommunications and travel companies to collect personally identifiable information (PII).

While the number of Iranian malicious cyber actors is numerous, and their capabilities continue to grow, Iran must nevertheless overcome the varying organizational and institutional hurdles within government agencies and contractors. To add, Iran must contend with the long-standing and crippling economic sanctions that directly reduce the Iranian government's resources and indirectly contribute to Iranian society's long-standing scientific brain drain estimated at 150,000 immigrants per year.[118, 119] Understanding Iran's responses to these sanctions may be critical for assessing its potential adoption of financially motivated cyber attacks.

4.3.4 Economic Environment and Sanctions Implications

The Iranian economy has contracted due to both the extensive sanctions regime targeting almost every export sector and the COVID-19 pandemic. The International Monetary Fund (IMF) estimates that Iran's 2020 GDP was $610 billion, a drop of 4.99% from the previous year.[120] Iran has been reducing its dependence on oil and gas revenues since 2011 to the point that in 2019 to 2020, 92.6% of GDP originated in non-oil sectors.[121] Iran's other primary revenue streams are from the industrial, manufacturing, and services sectors, at 25%, 16.1%, and 57.1% respectively. Iran's unemployment rate is 9.5%.[122]

China is Iran's primary trading partner, with a total bilateral trade of $14.9 billion according to Chinese customs data, as of February 2021.[123] Recently in March 2021, Iran and China concluded a 25-year, $400 billion security and investment agreement, despite US sanctions.

US unilateral sanctions on Iran have existed since the US-Iran hostage crisis in 1979 and were initially intended to end both Iranian sponsorship of terrorism and limit Iranian strategic power in the MENA region. These were expanded during the Bush administration and ramped up further under the Obama administration in response to increasing concerns over nuclear proliferation. Beginning in 2012, oil exports were significantly curtailed and widespread financial sanctions were implemented. These sanctions froze all US-held Iranian government assets and blocked any financial entity that facilitated sanctioned Iranian trade from the US financial system. In 2013, sanctions were further expanded to include Iran's automotive sector, as well as any transactions in Iranian Rial.

Under the 2015 Joint Comprehensive Plan of Action (JCPOA) between Iran and the UNSC's 5 permanent members plus Germany (P5+1), most US secondary sanctions were waived or terminated in exchange for significant and verifiable reductions in Iran's proliferation activities. The removal of these secondary sanctions allowed third parties to restart trade with Iran without being blocked from accessing the US market or financial system. Primary sanctions banning direct US-Iran trade and investment remained in place, as did trade relating to the military, terrorism, proliferation, human rights, or the IRGC. Finally, Iran, which was first cut-off from the SWIFT interbank messaging system for cross-border transactions in 2012, was reauthorized access through the agreement. UN Security Council sanctions on Iran were initiated in 2006 following the election of Mahmoud Ahmadinejad and the restart of nuclear activities in Iran. They gradually expanded through 2010, implementing an arms embargo and focusing on limiting Iranian ability

to expand its WMD infrastructure. Following the JCPOA agreement, UNSC Resolution 2231 lifted all UN sanctions in 2016, but maintained a heavy arms embargo until October 2020.[124]

In May 2018, the Trump administration formally announced the US withdrawal from the agreement, which was followed by the Iranian government's January 2020 announcement marking the end of its own commitments. After its withdrawal, the US attempted to trigger a snapback provision that would restore all UNSC sanctions on Iran but was rejected by UNSC members on the grounds that the US was no longer a participant of JCPOA.[125] In March 2021, Iran announced its openness to resuming negotiations to rejoin the JCPOA if the Biden administration lifted the US sanctions triggered by the 2018 withdrawal within a year.[126]

Recent sanctions

When the US unilateral exited the JCPOA, the Trump administration's 'maximum pressure' campaign reimplemented all of the sanctions that were waived or eased under the JCPOA and expanded the measures to cover Iran's mining, construction, manufacturing, textile, and metals sectors.[127] Significant Reduction Exemption (SRE) waivers that had allowed minimal levels of Iranian oil exports were left to expire in May 2019, effectively subjecting all Iranian oil exports after this date to US secondary sanctions.[128,129] Most recently, the US has specifically enforced sanctions provisions on a handful of shipping and petrochemical companies based primarily in China, Hong Kong, and the UAE that were found to be facilitating illicit Iranian trade.

The sanctions have had a clear economic impact on Iran. As sanctions were ramped up in 2012, Iran experienced respective declines in GDP and crude oil exports of 7.7% and 50%, meanwhile, the government was blocked from accessing a large portion of its foreign reserves, and its currency depreciated considerably.[130] It is widely accepted that the sanctions regime is a major factor that led to the initial signing of the JCPOA agreement. In 2016, following significant sanctions reduction under the JCPOA, Iran saw a 13.3% increase in GDP and an increase in crude oil exports back to pre-sanctions levels.[131]

These sanctions have also in part caused an increased diversification in Iran's economy as seen by considerable growth in non-oil exports and geographic complexity. Under sanctions, Iran dramatically decreased trade with highly sensitive trade partners such as the EU, Japan, South Korea, and Switzerland, but increased trade with a range of other countries that were less sensitive to sanctions such as China, India, Malaysia, Russia, the UAE, Turkey, and others.[132] Iran also saw marked increases in a range of export-sectors that were largely undeveloped under sanctions, such as Iron ore, chemical fertilizers, ethylene, and others.[133] In their 2020/2021 budget, Iran only accounted for $10 billion in oil revenues.[134]

Sanctions Evasion

Like the DPRK, Iran has also engaged in a variety of covert sanctions evasion mechanisms in order to conduct trade and gain access to illicit funds. Unlike the DPRK, Iran has not utilized offensive cyber actions in order to do so.

Primary sanctions evasion methods:

- **Illicit Transshipments**. Estimates of the exact amount of illegal transshipments of petroleum exports from Iran have varied. Estimates from independent oil tracking services, which observe tanker movement via satellite, place January 2021 exports between 800,000 and over 1 million barrels per day, the highest level since SRE waivers expired in April 2019. The most recent Central Bank of Iran (CBI) report shows a 5.1% quarterly increase in the Iranian oil sector between June and September 2020.[135]
- **Obfuscation Techniques**. Iran engages in a variety of deceptive shipping practices similar to that of the DPRK, but on a much larger scale. Obfuscation techniques such as flag and name

changes, night transfers, ship identity theft, and false AIS transmissions are all utilized. Large-scale ship-to-ship transfers and customs data misrepresentation are also employed. In one prominent example, China, which had purchased Iranian oil, has consistently reported monthly petroleum imports from Malaysia of $500 million more than the total value of Malaysia's oil production.[136] Since the SRE expiration, China has been the primary importer of Iranian oil, but Syria and Venezuela have recently begun minor imports as well. Turkey has ceased purchases of Iranian oil since the SRE expiration, in compliance with US sanctions.

- **Bulk Cash and Gold Smuggling**. Networks of couriers carry gold and other physical currency into Iran in exchange for exports. A report by the Organized Crime and Corruption Reporting Project (OCCRP), details a "gas for gold" scheme whereby a 22-member team transported more than 200 tons of gold in suitcases between Turkey, Dubai, and Iran as a part of a global money laundering operation.[137]
- **Shell and Front Company Networks.** Rather than directly paying the CBI for its exports, companies divide their payments into smaller outflows utilizing complex layering schemes that rely on different front companies for brokering, settling, and laundering. Often, transactions are recorded as non-sanctioned goods such as food and humanitarian items. They may also utilize potentially complicit or unwitting international banks. The US has sanctioned entities that were central to these arrangements, such as Hong Kong-based Triliance Petrochemical Ltd., yet payments have continued with slight reconfigurations of the networks. In March 2021, the Biden administration reportedly warned China that it will enforce sanctions on such shipments.[138]
- **Complicit Financial Institutions**. Bank of Kunlun, a regional Chinese financial entity, is estimated to have accounted for 80% of Iran-China oil transfers up until SRE expiration. It was able to operate despite direct sanctions in 2012 because it primarily dealt with large State-Owned Enterprises (SOEs) and did not transact in US dollars.[139] Turkey's Halkbank faces penalties of up to $20 billion and removal from the SWIFT interbank network in a New York trial scheduled for May 2021 for illicitly maintaining accounts on behalf of Iran and facilitating the "cash-for-gold" scheme mentioned above. In 2014, BNP Paribas was fined a then record $8.9 billion for deliberately obfuscating SWIFT codes to illicitly provide dollar clearing services on behalf of Sudan, Iran, and Cuba.
- **INSTEX Special Purpose Vehicle**. The EU created the INSTEX SPV in order to facilitate European-Iranian trade without sanctioned cross-border transfers by enabling European exporters to be paid for exports to Iran by European importers who are importing goods from Iran. As of March 2021, there has only been one successful transaction, as European companies still fear US sanctions that target any business with Iran, regardless of transaction type.
- **Virtual Currencies.** While Iranians are currently blocked from most international cryptocurrency exchanges, several local exchanges nevertheless facilitate cryptocurrency transactions in the face of US sanctions. These exchanges were utilized to launder the proceeds of the SamSam Ransomware attacks between 2015 and 2017. The Iranian government has taken action to block private use of cryptocurrency, while at the same time authorizing cryptocurrency mining as long as it is sold directly to the central bank. The CBI has also announced that it is studying the development of a rial-backed central bank digital currency.

5 IRAN STRUCTURED ANALYTIC FRAMEWORK

COLUMBIA UNIVERSITY | SIPA CAPSTONE REPORT

The DPRK is the only nation in the world known to have adopted a policy of state-sponsored, financially motivated cyber attacks. While currently the sole example of these types of operations, North Korea is a useful case study for assessing the conditions that could drive Iran to adopt a similar policy of financially motivated attacks.

5.1 IDENTIFICATION AND ANALYSIS OF DRIVERS

To determine the DPRK's motivations for implementing this policy, the capstone team utilized a PMESII framework for assessing what may have led DPRK to conduct financially motivated cyber attacks, such as the Bangladesh Central Bank attack in February 2016 and the WannaCry 2.0 attack in May 2017. The assessment identified 11 drivers which may have some impact on the DPRK's decision to perpetrate these cyber operations:

1. **Perception of Isolation**: The DPRK is almost completely cut off from the global economy, reliant on China and Russia for connection to the international environment, though the countries vary in their degree of patronage. Decisions in Moscow and Beijing to support or distance themselves have a large impact on whether DPRK must rely on illegal measures.
2. **International Resolve to Enforce Sanctions**: The degree to which the international community effectively enforces sanctions directly impacts the country's revenue.
3. **Status of Negotiations**: The international community has made multiple attempts to reverse or slow the DPRK's nuclear development program through negotiations, often holding out the promise of sanctions relief in return for a change in Pyongyang's behavior. While diplomatic efforts have had little impact in achieving their primary goal, the status of negotiations has in some cases resulted in short-term changes to North Korea's aggressive behavior. For example, in 2018 when negotiations between the US, ROK, and the DPRK were set to begin, the DPRK announced that it had temporarily halted missile and nuclear tests.[140]
4. **Domestic Regime Stability:** Regime survival is the DPRK's primary goal. The regime uses sanctions evasion to buy the support of the military, elites, and other key groups.
5. **Relationship with ROK**: The level of tensions with the South is often a good indicator of how aggressive North Korea is in pursuing foreign policy goals, including its cyber operations.[141]
6. **Key Leadership Composition**: Kim Jong Un has made developing cyber capabilities a national priority. While it is likely that any successor would maintain those capabilities, new leadership could bring a radically different military and foreign policy.
7. **Grievance Retaliation**: The DPRK has in a number of cases used cyber operations to directly retaliate or address perceived grievances, such as with the 2014 Sony Pictures hack, in part a response to the movie ***The Interview***, a comedy about a plot to assassinate Kim Jong Un.[142]
8. **Prioritization of Military Capabilities**: The DPRK has used cyber operations and sanctions evasion to develop its nuclear, conventional, and unconventional weapons programs. A change in military strategy and force structure could impact the scope and pace both in the development and deployment of cyberweapons.
9. **Economic Welfare**: Financially motivated cyber attacks are by definition a method of obtaining money. Therefore, the DPRK's economic welfare plays a central role in determining how and when these cyber attacks are conducted as well as the overall prioritization of other methods of illicit financing that can materially boost North Korean GDP growth.
10. **Cyber Capabilities**: The sophistication of its cyber capabilities likely plays a role in if and how the DPRK decides to pursue financially motivated cyber attacks, as financial exchanges and banks have typically invested more than other sectors in software, hiring personnel, and training programs that reduce the success probability of both less sophisticated credential or email compromise attacks or more sophisticated espionage and destructive attacks.
11. **Nuclear Development**: The continued development of a nuclear arsenal plays a role in determining the sense of security of the regime and international isolation as well as if the regime needs to pursue cyber operations to fund its development.

5.1.1 Assessing Differences Between DPRK and Iran

Though the DPRK and Iran share a number of drivers that could explain Iran adopting a policy of financially motivated cyber attacks in the future, there are important differences between the two countries. In multiple respects, Iran is in a similar, but less extreme, geopolitical position than the DPRK. The key differences between the two countries, with regard to motivations and driving forces, are as follows:

- **Economic Position**: While both countries are heavily targeted by international sanctions that have had serious and crippling effects on their economies, the GDP of each country differs vastly. In 2019, the DPRK's real GDP was estimated to be $28.3 billion;[143] Iran's was estimated to be more than 20 times larger, at $610 billion.[144] This difference in size is in large part due to Iran's vast oil reserves,[145] with no comparable commodity available to the DPRK.[146] Overall, North Korea's economic situation is currently far direr than that of Iran.
- **Degree of Isolation**: The number and depth of diplomatic and economic linkages significantly differ. Both countries are largely perceived as pariahs by the West, but Iran maintains a far larger number of diplomatic missions and economic trade relations with countries around the world than the DPRK.[147, 148] Additionally, Iran has for years made use of regional proxies, such as Hezbollah and the Houthi rebels in Yemen, while the DPRK has no comparable extension of its power.[149]
- **Foreign Patronage**: While the DPRK faces a much more challenging economic environment and level of isolation, it also benefits from more direct patronage from China and to some degree Russia.[150] Iran has increased its cooperation with these two countries, but it does not maintain the same level of dependence on Russia or China as the DPRK.[151] A disruption in ties may isolate Iran and embolden it to pursue financial cyber operations.
- **Leadership Structure**: Though both Iran and the DPRK are considered dictatorships, they have vastly different government structures. The DPRK is operated entirely by the Kim regime in a clear linear hierarchy,[152] whereas Iranian policymaking is a function of various actors, primarily including the Supreme Leader, the President, and the head of the Islamic Revolutionary Guard Corps.[153] While there is predictability in Iran's presidential elections, changes of administration allow for new and distinct policies that could reorient how the country manages its cyber operations.[154]
- **Negotiations**: There have been appeals to both the DPRK and Iran through diplomatic negotiations. However, negotiations with the DPRK have been far more ineffective than those with Iran.[155] Despite the US abandoning the Joint Comprehensive Plan of Action (JCPOA) during the Trump administration,[156] it still appears that there is a path forward with Iran.[157] As a result, it is possible that the status of negotiations will have a more significant impact on both Iran's economic welfare and decision-making, particularly with regard to aggressive behavior, than the status of any negotiations with the DPRK, if they were to take place.
- **Cyber Capabilities:** The DPRK has showcased high-level cyber capabilities in its financially motivated cyber attacks, particularly the Bangladesh Bank heist. Iran has similar capabilities to those of the DPRK and could quickly acquire what it needs to replicate such an operation, though Iran would initially face a learning curve attempting to target hardened targets like large financial institutions.[158]

5.1.2 Determining Iran Drivers

The DPRK drivers provide some indication of how Iran might adopt financial cyber operations similar to those already undertaken by North Korea. The capstone team distilled a similar set of drivers for Iran. A shift in one or more drivers could impact whether Iran adopts a policy of state-sponsored financially motivated cyber attacks in the future.

1. **Key Leadership Composition**: Key leadership composition includes the supreme leader, the president, and other high-level officials, such as the chief commander of the Iranian Revolutionary Guard Corps. While there is not as clear a link between individual leaders and the decision to adopt financially motivated attacks in Iran as in the DPRK, substantial changes in the key leadership would play a role in determining the nation's goals, allocation of resources, foreign policy decisions, and most importantly, it approves any high-level cyber investments and operations.[159]
2. **Perception of Isolation**: The capstone team believes that Iran's perception of isolation will influence its usage, targeting, likelihood, and the overall cost-benefit analysis of various cyber operations. Increases in perceived isolation, through trade disputes, decreased foreign assistance, or alienating foreign policy decisions, will likely create conditions more supportive of financial cyber operations.
3. **Grievance Retaliation**: Iran has retaliated in limited circumstances using cyber attacks largely for disruptive or destructive purposes.[160] The degree to which Iran embraces a policy in which its retaliatory behavior is financially focused could influence the country's overall cyber policy and potentially motivate the country to more broadly utilize cyber attacks as a tool for revenue generation.
4. **Domestic Regime Stability**: Iran's domestic stability has always been a primary concern of the regime. The nation's government expends considerable resources, including cyber capabilities, to suppress dissent and surveil dissidents.[161] While domestic politics are in many ways distinct from policy decisions that involve utilizing cyberweapons abroad, domestic stability and internal protests likely play a role in determining how Iran prioritizes its cyber resources and targets.
5. **JCPOA Negotiations**: The course of negotiations surrounding Iran's nuclear program and the state of sanctions heavily influence how Iran perceives its place in the international order and its future economic outlook, and as a result, may change its existing cyber strategy.
6. **Risk Appetite**: As with any change in the status quo involving the adoption of a more aggressive course of action, risks are involved. Iran's risk appetite, indicated by its non-cyber pursuits, likely plays a role in motivating whether the country would continue its existing cyber strategy or shift to perpetrating financially focused cyber attacks that could potentially undermine its efforts to reintegrate with the global economy.
7. **Economic Welfare**: Iran's economic welfare is directly related to how much revenue the government can generate, both from traditional financial means and through more illicit channels. Severe declines in the country's welfare may make it more willing to adopt aggressive cyber policies that generate revenue.[162]
8. **Cyber Capabilities**: The acquisition and development of specific types of exploits or TTPs may be a sign of Iranian priorities.
9. **Nuclear Development**: Iran's nuclear development has been key to establishing itself as a serious regional and global force, potentially allowing it to embrace more aggressive policies, such as financially motivated cyber attacks, with greater impunity. Additionally, as the program develops, Iran may need to grow its illicit revenue streams, increasing the likelihood that it could do so through cyber means. However, the program's development has recently faced several obstacles and setbacks, and it is unclear whether substantial progress or implementation could be made in the next two years.[163,164]

5.1.3 Methodology Recap — Impact and Probability

During the analysis stage, the capstone team ranked the nine drivers based on each driver's impact and probability using *a pair comparison matrix*. The matrix compared (1) the likelihood that each driver would be subject to change within the next two years, and (2) the impact that each driver has on the question of whether or not Iran will pursue financially motivated cyber attacks.

5.1.4 Ranking of Drivers

Assuming further economic isolation resulting from sanctions and/or other similar policies, the project question examined the likelihood that Iran will adopt a policy of state-sponsored, financially motivated cyber attacks. Specifically, and based on the findings in the report's case study, is Iran likely to target financial institutions in a program of cyber theft similar to that perpetrated by North Korea?

Below is the capstone team's ranking of drivers by impact and probability:

1. **Driver 1**: Key Leadership Composition (score: 14.5)
2. **Driver 2:** Perception of Isolation (score: 12.5)
3. **Driver 7:** Iran's Economic Welfare (score: 12)
4. **Driver 5:** JCPOA Negotiations (score: 10)
5. **Driver 6:** Iran Risk Appetite (score: 9)
6. **Driver 3:** Grievance Retaliation (score: 8)
7. **Driver 4:** Domestic Regime Popularity (score: 3)
8. **Driver 8:** General Cyber Capability (score: 2)
9. **Driver 9:** Nuclear Development (score: 0)

These top three drivers scored medium on impact but high in probability:

1. **Driver 1:** Key Leadership Composition (score: 14.5)
2. **Driver 2:** Perception of Isolation (score: 12.5)
3. **Driver 7:** Iran's Economic Welfare (score: 12)

The following three drivers are still highly relevant. However, these drivers ranked below the top three, either because they were probable but not impactful, impactful but not probable, or only moderately impactful and probable. For example, the capstone team ranked *JCPOA Negotiations* as the second most probable driver after *Key Leadership Composition* but found it less impactful than many other drivers. Conversely, *Grievance Retaliation* scored relatively high on impact but low on probability.

4. **Driver 5:** JCPOA Negotiations (score: 10)
5. **Driver 6:** Iran Risk Appetite (score: 9)
6. **Driver 3:** Grievance Retaliation (score: 8)

These final three drivers were deemed to be both without impact and improbable.

7. **Driver 4:** Domestic Regime Popularity (score: 3)
8. **Driver 8:** General Cyber Capability (score: 2)
9. **Driver 9:** Nuclear Development (score: 0)

5.1.5 Top Two Drivers

Following the discussion weighing the impact and probability of each driver, the capstone team ranked *Key Leadership Composition* and *Perception of Isolation* as the top two drivers, with Iran's *Economic Welfare* a close third. While *Key Leadership Composition* scored as the highest driver, the capstone team chose not to nominate it as a driver to create the scenario analysis for several reasons. First, the *Key Leadership Composition* driver is relatively opaque and difficult to quantify. It would be difficult for the client to measure, quantitatively or qualitatively, change in policy, posture, or personnel along an axis such as 'Hawkish' versus 'Dovish.' Second, the driver's impact on the decision to adopt a policy of financially motivated cyber attacks would be sufficiently captured in the development of scenarios by the other drivers. For example, in the interview with Kenneth Pollack, he noted that both the probability of changes and the impact of *Key Leadership Composition* remains high, likely impacting the other drivers.

5.2 MATRIX OVERVIEW — SCENARIO DEVELOPMENT

5.2.1 Reintroduction of Scenario Analysis

Using the two identified key drivers, *Economic Welfare* and *Perception of Isolation*, the capstone team developed a 2x2 scenario matrix with the horizontal dividing line representing the first driver's spectrum, while the vertical dividing line represented the second driver's spectrum. The two ends of each line represented the extremes of each driver's spectrum.

A total of four scenarios were generated using a combination of the two drivers, represented by each of the four quadrants of the matrix illustrated above. The team then developed a narrative for each hypothetical scenario, which included a hypothetical chronology of key dates and events, along with the implications should the scenario arise.[165]

Below are summary tables and descriptions of the four scenarios using the two nominated drivers. Table 1 illustrates how changes in the value of the drivers can lead to the occurrence of a given scenario. Table 2 provides hypothetical events that illustrate how a scenario could materialize.

Table 1 - Illustrative Scenario Analysis

Scenario 4: Persian Perestroika

Policy of financially motivated cyber attacks is unlikely

Economic Welfare	Perception of Isolation
• Contracting GDP • Increased sanctions • Fewer trade partners • Oil revenues decline due to decrease in price and demand • Reduced foreign direct investment • Increased inflation • Increased unemployment	• Increased and deepened bilateral and multilateral relations • Increased trade agreements • Increased technology sharing • Increased inclusion in international organizations

Scenario 1: A New Iran

Policy of financially motivated cyber attacks is unlikely

Economic Welfare	Perception of Isolation
• Growing GDP • Oil revenues increase due to price expansion and sanctions evasion • Increased economic diversification • Reduced sanctions pressure • Reduced brain drain • Increased foreign direct investment • Lower inflation • Lower unemployment	• Increased and deepened bilateral and multilateral relations • Increased trade agreements • Increased technology sharing • Increased inclusion in international organizations

Perception of Isolation (+ / -)

Economic Welfare (- / +)

Scenario 3: Nothing Left to Lose

Policy of financially motivated cyber attacks is likely

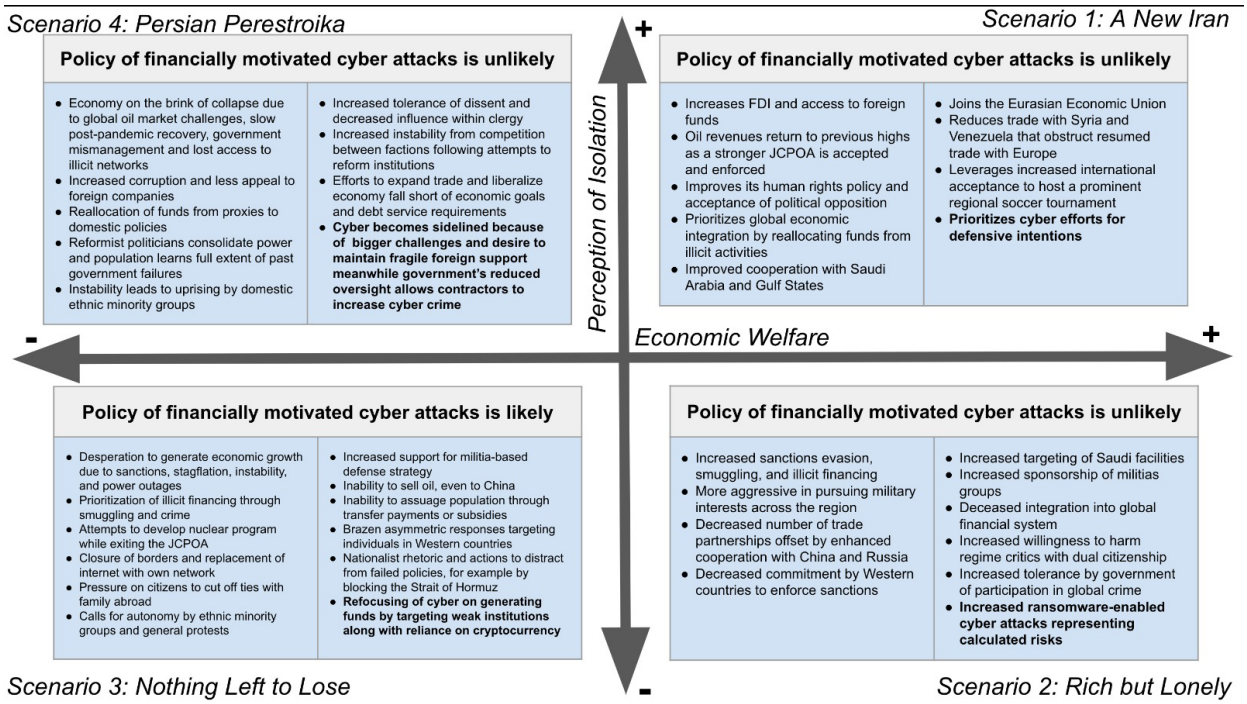
Economic Welfare	Perception of Isolation
• Contracting GDP • Increased sanctions • Fewer trade partners • Oil revenues decline to price compression & demand destruction • Reduced foreign direct investment • Increased inflation • Increased unemployment	• Breakdown of relations with partners • Declining stature in the region • No path toward global integration

Scenario 2: Rich but Lonely

Policy of financially motivated cyber attacks is unlikely

Economic Welfare	Perception of Isolation
• Growing GDP • Oil revenues increase due to price expansion and sanctions evasion • Increased economic diversification • Reduced sanctions pressure • Reduced brain drain • Increased foreign direct investment • Lower inflation • Lower unemployment	• Strained of relations with partners • Declining stature in the region • Limited paths to global integration

Table 2 - Illustrative Scenario Analysis with Hypothetical Events Indicators



5.2.2 Scenario 1: A New Iran

In this scenario, it is unlikely[166] that Iran will pursue a policy of financially motivated cyber attacks against financial institutions. Financially motivated cyber operations would be expected to be of limited benefits relative to Iran's improved economic situation and the high potential damage to the country's international standing.

In this hypothetical, set in March 2023, the drivers ***Economic Welfare*** and ***Perception of Isolation*** have extreme positive values. Iran enjoys high economic welfare and high integration into the international system. Its path to this point can be envisioned as follows:

> *The Supreme Leader is succeeded by an unprecedentedly moderate cleric, who prioritizes reconciliation with the West and domestic reform to reintegrate Iran into the international system. Consequently, the regime's domestic support increases as it broadens its leadership by cooperating with non-clerical political factions. While Iran is not aligned with Western countries, it is more cautious of Russia and China, downplays its relations with states such as Venezuela, and more mindful of maintaining stability with the US and its allies. Iran has reduced support for regional militias, and as a result its neighbors and others support the easing of sanctions, as well as increased trade and foreign direct investment. Easing of tensions with the West is accompanied by expanded grassroots ties with international civil society organizations, improving Tehran's ability to project soft power. Iran maintains a robust cyber capability but limits its use towards only the most concerning national security priorities.*

5.2.3 Scenario 2: Rich but Lonely

In this scenario, it is unlikely that Iran will pursue a policy of financially motivated cyber attacks on financial institutions. Financially motivated cyber operations would be expected to be of limited potential benefits relative to its improved economic situation. Iran would like to deepen its integration into the international system but not at the expense of abandoning priorities that contradict Western interests.

In this scenario, set in March 2023, ***Economic Welfare*** is valued on the positive extreme and ***Perception of Isolation*** is valued on the negative extreme. Iran enjoys high economic welfare but low integration into the international system. Its path to this point can be envisioned as follows:

> *The Supreme Leader remains in control of the Iranian regime and committed to the same ideals and policies that he previously outlined. Consequently, Iran continues to operate under the pressure of Western sanctions. Nevertheless, Iran has withstood isolation and improved its economic standing due to a global recovery in energy markets and an improved ability to evade sanctions. It pursues an assertive foreign policy across the Middle East by increasing its support of proxies and takes escalatory actions towards regional adversaries. It has deepened economic and political ties to US adversaries such as China and Russia. Despite harsh international condemnation, the Iranian regime remains repressive, severely punishing dissent and cracking down on civil society.*
>
> *Despite its increased assertiveness, Iran pursues calculated risks. Consequently, the gains from financially motivated cyber attacks are judged too limited compared to the costs of potential diplomatic, economic, and cyber retaliation if operations are attributed to Iran.*

5.2.4 Scenario 3: Nothing Left to Lose

In this scenario, it is likely that Iran will pursue a policy of financially motivated cyber attacks on financial institutions. The benefits of these operations are high, due to Iran's contracting economic base and deteriorating international standing, both of which are unlikely to improve.

In March 2023, ***Economic Welfare*** and ***Perception of Isolation*** have extreme negative values. Iran faces unprecedentedly low levels of economic welfare and integration into the international system. Its path to this point can be envisioned as follows:

> *The Supreme Leader has passed away and his successor pursues the same ideals and objectives but with greater zeal, ambition, and resources. In the past two years, Iran has pursued an increasingly aggressive foreign policy targeted at regional adversaries and the US presence in the Gulf. The level of domestic repression and control over the population has risen to unprecedented levels. Sanctions have been reimposed and the economy has contracted. Tehran has resorted to asymmetric capabilities, such as cyber operations, to project power. Its determination to achieve its foreign policy goals and reduced financial resources have led Iran to direct government entities and contractors to target Western financial institutions with cyber tools to generate revenue. Western governments increasingly observe parallels between Iranian and North Korean operations.*

5.2.5 *Scenario 4: Persian Perestroika*

In this scenario, it is unlikely that Iran will pursue a policy of financially motivated cyber attacks. The Iranian government intends to maintain its improved standing in the international system. However, domestic and economic instability incentivize actors linked to the Iranian government to independently pursue financially motivated cyber attacks unbeknownst to regime leaders.

In March 2023, ***Economic Welfare*** is valued on the negative extreme, but ***Perception of Isolation*** is valued on the positive extreme. Iran experiences a low level of economic welfare but increased integration into the international system. Its path to this point can be envisioned as follows:

> *The Supreme Leader has been succeeded by a cleric committed to a starkly different trajectory. His vision is supported by a reform-minded President, who has outlined a plan to turn Iran's future around by reconciling with the West after years of efforts to withstand economic and political isolation. The dialogue regarding Iran's nuclear program has progressed and the regime has begun to reallocate resources away from foreign adventures towards repairing domestic fractures. While the Iranian government's desire for reform is sincere, its efforts may be too little too late especially since global oil prices are depressed and political infighting intense. Reports have emerged of IRGC officials and other regime insiders abusing their positions to enrich themselves with apparent impunity, leading the population to lose faith in key institutions. Occasionally, these abuses appear to fuel competition that some predict will escalate into factional violence.*
>
> *The Iranian government sees limited benefit in financially motivated cyber attacks that could critically impair costly efforts to integrate into the international system. Nevertheless, the state's increased disarray and reduced government oversight have provided rogue officials and underground cyber actors with opportunities to target financial institutions in the region and abroad. Iran has taken steps to clamp down on these activities but its success has been limited.*

5.3 INDICATOR DEVELOPMENT

To complement the scenario framework, the capstone team developed a set of indicators that they used to evaluate how certain events impact Iran's position in the 2x2 scenario matrix. The indicators are as follows:

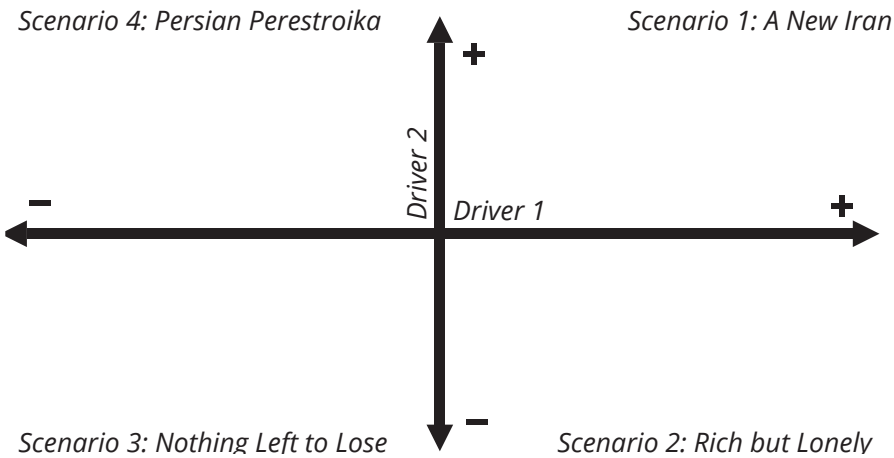
- **A change in key leadership to a more conservative or liberal approach**: for example, if a hardline president is elected or the Supreme Leader dies and is succeeded by a more extreme figure.
- **A change in the status of negotiations between the US and Iran**: whether they fail, return to the previous JCPOA agreement, or go beyond the former agreement and bring increased prosperity to Iran as well as significant inclusion in the international community.
- **A change in the status of sanctions imposed on Iran**: whether they are increased, partially lifted, or are significantly rolled back. Specifically, increased sanctions would include increased enforcement as well as the targeting of intermediary entities that enable Iran to evade sanctions. Partially lifted sanctions would look similar to the sanctions under the previous JCPOA agreement, while a larger repeal of sanctions would also lift human rights sanctions that have been in place for decades.

- **Increased or decreased pressure on Iranian opposition either domestically or abroad**, such as the execution of a journalist or the release of prominent opposition leaders from prison, respectively, which leads to either serious international condemnation and loss of certain multinational agreements or international praise and an opportunity for increased involvement in the international community.
- **Increased or decreased engagement with authoritarian countries**, through unprecedented official visits, bilateral trade deals, international forums, cultural exchanges, or other high-level interactions. For example, increased engagement could take the form of Iranian Foreign Minister Zarif visiting Caracas to discuss collaboration between Iran and Venezuela, and decreased engagement could take the form of Qatari politicians severely criticizing Iranian actions in the region.
- **The culpability of a serious international event**: for example, if Iran is found to have deliberately shot down Ukraine International Airlines flight 752 in January 2020,[167] placed bounties on US soldiers in Afghanistan that resulted directly in US casualties,[168] or attempted an assassination in the US that resulted in casualties.
- **Increased or decreased kinetic conflict involving Iran**. Increased conflict could either be outside of Iran through Iranian-backed groups and Western-backed powers or through missile strikes against US bases in the Middle East, resulting in the death of US soldiers. Decreased conflict would be illustrated if Iran terminated funding to its proxies in places like Yemen and Lebanon.
- **The discovery that Iranian nuclear facilities are far more developed than previously believed**.
- **Substantial improvements or declines in Iran's economy**, separate from sanctions. Improvements could take the form of increased foreign investment, reductions in unemployment, and new trade deals with neighboring states. Economic declines would be evident by rolling power outages, border closures, hyperinflation, serious decreases in currency stability, increased tanker seizures, and potentially the complete blockage of the Strait of Hormuz.

The capstone team separated each of these indicators into separate events, where applicable. For example, the sanctions indicator was broken down into three events: increased sanctions, partially lifted sanctions, and completely lifted sanctions; similarly, the status of negotiations indicator is also represented by three stages. In total, the indicators account for 18 distinct events.

5.3.1 Analysis of Competing Hypothesis Framework In Practice

These 18 distinct events have been placed into an analysis of competing hypothesis framework, which enables the ability to track Iran's position within the following 2x2 scenario matrix:



Each event provides an opportunity to falsify a scenario (or scenarios) and move Iran within the matrix. The use of a falsification approach rather than a confirmation approach reduces the potential bias of the indicator creation and still presents a clear sign of the direction Iran is moving. Confirmation of a scenario by an event is therefore rated as equivalent to neutral and given a score of 0, whereas refutation of a scenario is given a score of -1. However, in certain instances, the capstone team determined that extreme confirmation would also warrant an event receiving a score of 1.

In practice, here are three example events to illustrate how this framework functions:

- In the next few months, Iran significantly increases its pressure on domestic opposition groups by shutting off the internet and arresting human rights advocates, which enrages the international community. This event would falsify Scenario 1 and Scenario 4, as it isolates Iran while confirming Scenario 2 and Scenario 3. As a result, Scenario 1 receives a score of -1, as does Scenario 4; the other scenarios maintain scores of 0.
- A month after Iran increased its pressure on domestic opposition groups, a leaked internal report uncovers that it deliberately destroyed Ukraine International Airlines flight 752. This event also goes against Scenario 1 and Scenario 4, while confirming Scenario 2. However, because this is such an egregious international violation that resulted in the deaths of hundreds of civilians, it particularly isolates Iran and results in some financial repercussions, extremely confirming Scenario 3 and giving it a score of 1. Following this event, Scenario 1 has a cumulative score of -2, as does Scenario 4, while Scenario 2 maintains a score of 0, and Scenario 3 now has a score of 1.
- Finally, six months after it was revealed that Iran was responsible for the downing of the passenger jet, an annual assessment of the country's economy is published that indicates it is facing serious food and electricity shortages, which are predicted to negatively impact its GDP. This event falsifies Scenario 1 and Scenario 2, while confirming Scenario 3 and Scenario 4, giving a cumulative score of -3 to Scenario 1, 0 to Scenario 2, 1 to Scenario 3, and -3 to Scenario 4.

In this example, these three events happening in succession would indicate that Iran has moved very much away from both Scenario 1 and Scenario 4 and moved definitively toward Scenario 3, the "Nothing Left to Lose" scenario, and as a result, is likely to implement a policy of financially motivated cyber operations.

6 CONCLUSION

6.1 KEY ASSESSMENT

The following conclusion outlines the capstone team's key assessment, highlighting the most likely scenario, the most dangerous scenario, factors that could change the key assessment, as well as future and alternative considerations for the client.

The capstone team assesses that Iran is unlikely to adopt a policy of financially motivated cyber attacks within the next two years.

First, the costs of this policy would likely outweigh the potential benefits.[169] Although Iran has in recent years experienced increasing isolation and subsequently retaliated through a more assertive foreign policy, the Iranian government continues to demonstrate its goal of reintegrating into the international system. Evidence of efforts to reintegrate include: negotiations with the European JCPOA participant states to establish the INSTEX trading mechanism;[170] Iranian leadership statements on a desire to return alongside the US to the JCPOA;[171, 172, 173] and efforts to circumvent economic and political isolation through deepened diplomacy and trade, particularly with China[174] and Russia.[175] A state-sanctioned policy of financially motivated cyber attacks against international financial institutions would jeopardize these interests, especially Iran's efforts to return to the Joint Comprehensive Plan of Action (JCPOA). Furthermore, Iran may view retaliation through both destructive and financially motivated cyber attacks against the financial system as economic retaliation that is proportionate to sanctions regimes.[176]

Second, the potential gains from financially motivated cyber attacks are immaterial compared to the size of Iran's ~$610 billion GDP,[177] which is forecasted to resume growth in 2021,[178, 179] or its ~$44 billion of 2019 government revenues.[180] Iran's GDP is estimated to be 20 times larger than that of North Korea, where cyber attacks represent a significant source of revenue for government priorities.[181]

For reference, the Iranian Sam Sam ransomware campaign required almost three years to target 200 victims and generate $30 million, or less than $150,000 per victim.[182] Even an attack equal to the $100 million 2016 Bangladesh Bank heist, would be small relative to Iranian economic figures. In addition, the $4 billion[183] 2017

WannaCry campaign equates to only $20,000 per incident after attacking approximately 200,000 victims across 150 countries.[184] Therefore, an Iranian financially motivated cyber attack campaign would need to be of an unprecedented scale and persistence to represent a valuable source of income for the Iranian government.

Iran does not lack the necessary cyber capabilities, but rather the motivations for adopting a policy of financially motivated cyber attacks within the selected two-year time frame.[185] Structured interviews assess that Iran has ransomware and ATM cash-out capabilities to execute a financially motivated cyber attack policy but will require more than two years to organically develop SWIFT hacking tools.[186]

6.1.1 Most Likely Scenario

The scenario assessed as the most likely to materialize within two years is a variant of the "Rich but Lonely" scenario, in which the ***Economic Welfare*** and ***Perception of Isolation*** drivers are respectively positive and negative. In this scenario, it is unlikely that Iran will adopt a policy of financially motivated cyber attacks. The capstone team assesses that the scenario's likelihood is supported by the current JCPOA negotiations, which recent history demonstrates would (1) improve economic welfare by lifting most sanctions enacted during the Trump administration[187] and (2) reduce political isolation by improving trade and investment between Iran and the West. However, the capstone team assesses that the prospects for continued integration into the international system are limited even if the JCPOA makes progress on Iran's nuclear program. A deep divergence would remain between Iran and the West on various issues, such as Iran's history of hostage-taking, sponsorship of terrorism, and threats to the US and its partners' interests. Breakthroughs in these domains, which are unlikely within the project's timeframe, may lead to a "New Iran" scenario if improvements in economic welfare are sustained.

6.1.2 Most Dangerous Scenario

The scenario assessed as the most dangerous scenario if it were to materialize is the "Nothing Left to Lose'' scenario, in which the Economic Welfare and Perception of Isolation drivers are both negative in the extreme. The capstone team assesses that it has the highest probability of Iran adopting a policy of financially motivated cyber attacks. In this scenario, Iran's leadership composition and policies lead to further isolation and sanctions efforts led by the US. Iran nevertheless remains determined to achieve its foreign policy goals despite reduced financial resources. Iran is cut off from the international community to the point where the government feels it has no reasons or options to cooperate with the West. The Iranian leadership consequently directs both government entities and contractors to target financial institutions with cyber tools to generate revenue.

6.1.3 Factors That May Change the Key Assessment

The capstone team assesses that the below list contains the most apparent factors that may significantly increase the probability or incentives for adopting a financially motivated cyber attack policy. These factors differ from indicators that specifically reflect the development of one of the four scenarios previously described. However, it is not necessarily exhaustive.

- Recent financially motivated cyber attacks by Iranian non-state groups that may have appeared discrete continue and cyber artifacts clearly indicate explicit government instruction, rather than tolerance of independent hacker activity. It does not appear that the Iranian government ordered

recent financially motivated cyber attacks but rather circumstantial evidence suggests government awareness of them.[188]

- The current COVID-19 pandemic may significantly impede Iran's economic recovery or contribute to continued economic contraction.
- A continued drop in Iran's foreign exchange reserves. As of 2020, the IMF estimates Iran's reserves at $4 billion compared with a 2018 high of $120 billion.[189] While Iran's reserves are forecasted to rebound to $12.2 billion and $21 billion in 2021 and 2022, economic shocks may impede this growth and provide an increased incentive to pursue financially motivated attacks.
- Major cyber or kinetic actions executed by or against Iran could lead to a sustained escalation that in turn reduces expected costs relative to the benefits of a financially motivated cyber attack policy. The probability of this development may increase as some of Iran's regional adversaries, such as Saudi Arabia and the United Arab Emirates, augment their offensive and defensive cyber capabilities.
- Reduced US involvement or presence in the Persian Gulf and broader Middle East that significantly reduce a financially motivated cyber attack policy's expected costs relative to benefits.

6.2 CONSIDERING NON-FINANCIALLY MOTIVATED CYBER ATTACKS

While the capstone team concluded that it is unlikely the Iranian government will adopt a policy of financially motivated cyber attacks against international financial institutions within a two-year time frame, the report's assessment did not cover non-financially motivated cyber attacks. As discussed in Appendix C, the capstone team identified five separate non-financially motivated cyber attacks perpetrated by Iran, targeting international financial institutions.[190] Had non-financially motivated cyber attacks been considered as well, it is likely that the assessment and primary drivers would have changed. First, a state-sanctioned policy of cyber attacks based on grievance retaliation, as opposed to financial gain, would be easier to justify, and would be less likely to jeopardize reintegration efforts. Second, while attacks on financial institutions are unlikely to make a substantial impact on Iran's overall economic position, they do hold strategic value in messaging aimed at Iranian adversaries.

Despite not being specifically aimed at generating revenue, non-financially motivated attacks have the potential to inflict considerable costs on their victims. The 2011-2013 DDoS attacks perpetrated by Iran on the US financial sector, known as Operation Ababil, incurred tens of millions of dollars in disruption costs.[191] More recently, the 2013-2017 Mabna spear-phishing campaign totaled more than $3 billion.[192] While only a small percentage of cyber attacks against international financial institutions have been attributed to the Iranian government, it is important to remain abreast of the associated risks, especially in the face of ongoing antagonism between the West and Iran.

Because these attacks primarily occur as a result of grievance retaliation, they are much harder to predict. Whereas financially motivated cyber attacks might be developed over a long period of time, these are more likely to be developed quickly, making them generally both harder to prepare for but also less effective. Because Iran engages in these attacks to prove a strategic political point, the method that is employed varies based on the specific goals. DDoS attacks are a common disruptive attack that is used in these cases, but other types of attacks are utilized as well. Ransomware attacks are generally not associated with this type of attack, and would be a strong indicator of the attack being financially motivated.

6.3 FUTURE CONSIDERATIONS

In the course of analysis, as well as in discussion with experts, the capstone team encountered a number of factors that do not currently impact the team's assessment on the likelihood of financially motivated cyber attacks but are growing in importance in the medium-term. They are cryptocurrency mining, central bank digital currencies, and Iran's development of a national, "halal" internet. The first two affect the capstone's scenario conditions based on the ***Economic Welfare*** and ***Perception of Isolation*** indicators. The third affects the scenario conditions based on the ***Domestic Regime Popularity*** and ***Perception of Isolation*** indicators.

Cryptocurrency Mining and Money-Laundering

In March 2021, the Iranian Presidential Center for Strategic Studies, a think tank affiliated with President Rohani's office, stressed the need for a "cryptocurrency extraction" policy that could generate $2 million per day, or $700 million per year, in revenue from mining as well as an additional $22 million in transaction fees.[193] This comes after a year in which the Iranian government has taken substantial steps to take control over the country's cryptocurrency industry. While personal cryptocurrency trading is still banned, the government distributed licenses for legal crypto mining for companies and individuals with connections to the IRGC or the government, as well as some foreign firms based in China and Turkey.[194] The government also shut down over 1,620 illegal unregistered mining farms, seized 45,000 cryptocurrency mining machines, and mandated that all newly mined cryptocurrency be sold directly to the CBI.[195] Most recently, in April 2021, the CBI announced that it will soon issue permits for banks and licensed currency exchange offices to use domestically mined cryptocurrency to pay for imports.[196]

These policy actions pave the way for future large-scale use of cryptocurrency mining for government revenue and sanctions evasion. According to the Cambridge Centre for Alternative Finance, Iran's share of global bitcoin mining has been growing and currently represents the sixth largest mining share globally.[197] Beyond gaining revenue through taxes on domestic crypto miners, the Iranian government could conceivably mine cryptocurrency directly by utilizing domestic energy capacity that is not exported due to sanctions. With essentially free electricity, the government would only be limited by the amount of mining machines it owns, which could continue to be seized from the domestic population or smuggled in from abroad. While mining profitability varies wildly based on hashing difficulty and currency prices, at the current bitcoin price ($55,000), a standard crypto mining machine could generate about $850 per month.[198] Just by using the 45,000 recently seized machines, the government could generate approximately $460 million annually.

If the Iranian government can increase government revenues through direct crypto mining and taxes, it could partially free itself from the severe economic constraints brought by sanctions, and gain leverage in negotiations around its nuclear program and sanctions apparatus. It would substantially affect the capstone team's scenario considerations based on the ***Perception of Isolation*** and ***Economic Welfare*** indicators. Furthermore, because the cryptocurrency would be domestically mined, the government could more easily use the currency to evade sanctions. While US law enforcement has been relatively successful at tracking cryptocurrency flows and working with exchanges to report and block illicit activities, newly mined coins can be very difficult to track because they do not necessarily need to go through any regulated exchanges in order to be utilized, i.e. they do not have any transaction history to be traced. If the CBI wanted to change its cryptocurrency into Iranian Rials, it would be able to easily utilize a domestically controlled exchange that would not be subject to any sanctions restrictions. Cryptocurrency is also critical to facilitating ransomware attacks. Iran's increased activity in this domain may increase its likelihood of conducting financially motivated cyber attacks. If the government develops a policy for incorporating cryptocurrency profits from cryptocurrency mining, it will be easier for it to develop a policy for incorporating cryptocurrency profits from ransomware attacks. Obviously, ease of use is not the only factor influencing whether they engage in ransomware attacks, but it increases likelihood.

Indigenous Central Bank Digital Currency (CBDC)

The Iranian government's goal is to help facilitate international trade outside of the conventional banking system.[199]While this is possible through cryptocurrency, as explained above, relying on wildly volatile mining profits in a currency it has no direct control over for consistent trade is not ideal. Further, US and international cryptocurrency regulations are only going to strengthen as the nascent industry becomes more established. A domestically-issued, CBI-controlled, and Rial-backed currency that Iran could use to trade bilaterally with other national central bank digital currencies would be preferable. The currency would be distributed at the sole discretion of the CBI, and could not be mined. Multiple national central bank digital currencies utilizing the same distributed ledger platform, such as in the m-CBDC Bridge project currently jointly underway between the central banks of China, Hong Kong, Thailand, and UAE, can be traded instantaneously and directly with each other.[200] All transaction clearing and messaging is done within the network, without having to utilize third party currencies such as the US Dollar, international clearing networks, or global messaging networks such as SWIFT, all of which Iran is blocked from using.

In 2018, the CBI announced it was developing a CBDC on an Iranian national blockchain platform that would initially focus on domestic use.[201] Later that year, deputy head of the management development department of the vice presidency for science and technology, Alireza Daliri, suggested that the government should consider partnering with friendly nations to develop cross-border distributed ledger solutions.[202] The central bank is partnering with multiple different private, domestic companies to test different pilots for the eventual implementation of the CBDC.[203] If Iran is able to join up with pivotal trade partners such as China or Venezuela, it will make trade easier, increase government revenues, and increase leverage in international negotiations. This would decrease the likelihood of financially motivated cyber attacks, because Iran would gain more income through sanctions evasion.

National Internet

Finally, the Iranian government has been developing a national, "halal" internet complete with a search engine, messenger, social media platforms, and user registration information since 2013. Known as the National Information Network (NIN), and developed partially in response to the 2010 Stuxnet attack, it has greatly increased the censorship capabilities of the Iranian government.[204] The government has demonstrated that it can maintain the NIN while simultaneously shutting down connections to the open net in order to inhibit coordination during domestic protests.[205] In 2019, President Rouhani announced that Ayatollah Khamenei had ordered the further development of the NIN to reduce dependence on foreign networks.[206]

As the Iranian government continues to expand the use of the NIN, it will become increasingly difficult for domestic opposition to enact significant political change. Even if the regime is very unpopular, the opposition will most likely have a minimal impact on the Iranian government policy. This is in line with the analysis of ***Domestic Regime Popularity*** as one of the least influential indicators for scenario development. Expansion of the NIN or complete blockage of the open net would also likely decrease integration into the international system. For example, in 2019, the US sanctioned Iranian Minister of Information and Communications Technology, Azari Jahromi, over his role in shutting down the open net during the November 2019 protests.[207] Increased censorship, therefore, would likely bring more international criticism.[208] This would increase the likelihood of financially motivated cyber attacks because of the increase in ***Perception of Isolation***.

7 APPENDICES

7.A STRUCTURED INTERVIEWS

Interview Methodology

Interviews with the listed subject matter experts (SME) were structured around 15 questions, with follow-up questions further extending the discussion. Over the course of the project, the team conducted fourteen structured interviews with the following SMEs:

1. **J. Michael Daniel**, President of the Cyber Threat Alliance and the former Special Assistant to President Obama and Cybersecurity Coordinator on the National Security Council (NSC) – March 17, 2021.
2. **Richard Nephew**, Senior Research Scholar at SIPA's Center on Global Energy Policy and the former Principal Deputy Coordinator for Sanctions Policy at the Department of State and Director for Iran on the NSC[209] – February 5, 2021.
3. **Kenneth M. Pollack**, Resident Scholar at the American Enterprise Institute and former director for Near East and South Asian affairs director for Persian Gulf affairs at the NSC and Central Intelligence Agency (CIA) Analyst – March 30, 2021.
4. **Sanaz Yashar**, Principal Analyst at FireEye, Inc. – April 6, 2021.
5. **Luke McNamara**, Principal Analyst at FireEye, Inc. – March 16, 2021.
6. **JD Work**, Research Scholar at Columbia University's Saltzman Institute of War and Peace Studies – March 24, 2021.
7. **Annie Fixler**, Deputy Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies (FDD) – March 25, 2021.
8. **Matt Ha**, Research Analyst at the Center on Military and Political Power at FDD – March 25, 2021.
9. **Colonel (res.) Gabi Siboni**, head of the Military and Strategic Affairs Program and Cyber Security Program at the Institute for National Security Studies – March 16, 2021.
10. **A former senior White House official** (White House Official) – April 9, 2021.
11. **A former senior US intelligence community official** (Intelligence Community Official) – March 23, 2021.
12. **A former senior US federal law enforcement official** (Law Enforcement Official) – March 30, 2021.
13. **A private sector cybersecurity researcher** (Private Sector Researcher #1) – March 19, 2021.
14. **A second private sector cybersecurity researcher** (Private Sector Researcher #2) – March 19, 2021.

The insights shared by the SMEs informed the capstone team's analysis and presented alternative conclusions. Some of these comments have been used to highlight potential blind-spots and qualify the report's assessments when necessary.

7.B INTERVIEW TAKEAWAYS

Select Questions	Notes and Selected Responses
What is the likelihood that Iran will adopt a policy of financially motivated cyber attacks?	• **Almost all subject matter experts assessed that Iran was unlikely to adopt a policy of financially motivated cyber attacks within a two-year time but stressed that Iran could do so if it believed it were in its interest.** • **One FireEye analyst assessed that 2020 financially motivated cyber attacks against Israeli targets were executed by actors who have worked extensively for the government.** • "Iranian actors already attack financial institutions...we are not sure if they are directed by the government but they have executed other operations and we believe that the government is aware of their actions because they use the same tools. We are certain that the actor behind the Pay2Key ransomware used in 2020 against Israeli targets has performed other operations on behalf of the Iranian government." – Sanaz Yashar • "Barring major changes, this seems very unlikely. Pay2Key appears more disruption oriented and less financially motivated. I do not believe that it and the Shirbit hack were directed by the government." – Private Sector Researcher #1 • "Things need to get a lot worse. Stealing funds admits that the regime isn't functioning." – J. Michael Daniel • "Iran wants adversaries to reduce sanctions. Financially motivated attacks undermine this effort." – JD Work • "Financially motivated attacks are just a part, not the focus, of a revenue generating portfolio of capabilities." – Gabi Siboni
What are the necessary conditions for Iran to adopt this policy?	• **Almost all experts believe that further economic contraction and international isolation must occur for Iran to adopt a financially motivated cyber attack policy.** • "Highly effective maximum economic pressure campaign." – JD Work • "The more isolated they feel with less to lose, the more likely they are to move in this direction, particularly if their potential allies will not help them." – J. Michael Daniel • "A loss of all remaining connections to the international economy." – Private Sector Researcher #1 • "Desperation or running out of money. Iran has in the past lacked foreign exchange reserves or government revenue. If Iran had a more confrontational president, it might prefer non-diplomatic avenues to acquire cash." – Annie Fixler • "If financial or petroleum sanctions were reimposed after recent instances of removal, that may indicate to the Iranian leadership that their previous judgement is incorrect. Therefore, the likelihood of financially motivated cyber attacks would rise. A financial crisis could have the same effect." – White House Official
What TTPs would you be most concerned with if Iran adopted this policy?	• **All experts believed that Iran will require more time to develop a SWIFT capability. Almost all experts believe that Iran could pursue ransomware immediately. Some raised Iran's ATM cash-out capability.** • "Reversible attacks like DDOS that avoid permanent damage and are less escalatory." – J. Michael Daniel • "Actors can attack institutions and obfuscate it as theft." – Sanaz Yashar • "Ransomware that permits deniability and spear phishing." – Luke McNamara • "The deployment of trojans." – JD Work

Select Questions	Notes and Selected Responses
What would be the most likely targets?	• **All experts focused on less defended targets. Some experts highlighted crypto exchanges given the role of crypto currencies in facilitating ransomware.** • "Vulnerable regional banks." – Intelligence Community Official • "Firms that have name recognition but are not the largest and most protected. Western financial institutions and those of regional adversaries, such as Saudi Arabia and Israel. Local banks do not provide the desired attention." – J. Michael Daniel • "Insurance companies because they are weaker but have more personal identifying information." – Sanaz Yashar • "Crypto currency holdings because of the ad-hoc nature of these operations and the technology's novelty. I would look at where an institution has joint ventures, special purpose vehicles, areas with an overlapping Iranian footprint that are of interest to Iran. Together, these might create vulnerabilities." – JD Work
Which events would you monitor for warning purposes?	• "Changes in Iranian government messaging; Disappearance of known actors from message boards because of pre-operational planning; reconnaissance; the purchase of tools on the dark web." – J. Michael Daniel • "Increasing economic isolation and breakdown in the JCPOA negotiations."– Private Sector Researcher #1 • "I do not think the Iranians would ever provide signals." – Kenneth Pollack • "Increased attacks against crypto currency targets." – JD Work • "Their cash position and challenges to meet debt obligations or previously acceptable trade agreement terms. Insight in these areas is available. Erratic behavior to retrieve foreign funds, such as tanker seizures." – White House Official
Is Iran deepening cooperation / control over non-state cyber groups for financially motivated attacks? Why is this possible or not?	• "They are not deepening. The government looks for new tools wherever available." – Intelligence Community Official • "They have always had a good relationship. Many companies are fronts for the IRGC." – J. Michael Daniel • "It is happening but Sam Sam ransomware operators were not necessarily connected to the government." – Private Sector Researcher #2 • "Yes but with caveats. This is how Iran already pursues foreign policies, i.e. with proxy groups or other contractors. Part of this makes them more risk-tolerant however they have been disappointed by unexpected proxy behavior. Proxies do not provide perfect plausible deniability." – Kenneth Pollack • "I see improvements in coherent, structural control. As cyber operations become increasingly iterated and we see more experienced cyber operators rising in the military or intelligence ranks, we may see improvements in capabilities and their increased integration. These could lead to reduced reliance on contractors." – JD Work
What are the upsides and downsides of this policy?	• **Almost all subject matter experts believed that financially motivated cyber attacks could do more harm, primarily through increased isolation, than good to Iranian interests.** • "There are no downsides since the US has failed to deter Iran after their repeated cyber attacks. The upside is that they can demonstrate their equal footing with the US." – Intelligence Community Official • "Almost no upside. Generating enough to run a country from cyber operations is incredibly difficult. The negatives outweigh the positives." – Private Sector Researcher #1 & #2 • "Some IRGC officials could potentially generate large personal profits. To the extent that the Banyad system becomes unstable, they might prioritize personal interests over those of the state." – JD Work • "The downside is Iran becomes viewed outside the international community." – White House Official

Select Questions	Notes and Selected Responses
How does the process for decision-making over cyber in Iran occur?	• **Most experts believe that the US lacks insight into this process.** • "They are gray zone tools to counter sanctions and reach sophisticated adversaries. They prefer the gray zone because of how the US treated Saddam Hussein at the end of the Iran-Iraq war. A limited attack can be done by a mid-level intelligence official." – Intelligence Community Official • "It is unclear. Iran is much more bottom-up and the government attempts osmosis. It is hard for analysts to see everything that is occurring there." – Sanaz Yashar • "I do not think that we know because the US lacks access and because the Iranians themselves do not know. I suspect they will continue their various efforts if they are not punished by the US." – Kenneth Pollack
If Iran's sanctions evasion capability eroded, what would be the most likely or effective compensation method?	• "The concept of a sanctions evasion capability is unclear. The JCPOA protects oil export, revenue repatriation, and financial system access." – Intelligence Community Official • "Increased oil smuggling." – Kenneth Pollack • "Seizure of vessels." – JD Work • "Overcoming damage from unilateral sanctions requires enormous effort." – White House Official
What are the biggest similarities and differences between Iran and North Korea?	• **All experts highlighted North Korea's much deeper international isolation.** • "Both are disruptors and are happy to challenge the international system. The main difference is the regime structure. Iran uses cyber more for proportionate response while the DPRK steal to prop up the regime." – J. Michael Daniel • "Iranian and DPRK cyber capacities developed differently. Iran is more grassroots." – Private Sector Researcher #1 • "Principalists (hard-liners) have talked about autarky through the resistance economy though they have expressed desires to rejoin the global economy." – Kenneth Pollack • "Criminal activity has been part of the DPRK modus operandi since the 1970s because it is central to regime survival. This is not the case for Iran." – Matt Ha
In what ways do the DPRK and Iran collaborate over cyber or other areas?	• **Most experts were unaware of meaningful cooperation between both states.** • "Iran does not need them and their cooperation is exaggerated by the media." – Intelligence Community Official • "Iranians generally think about their own interests, which is a problem in that even if they think long-term they can be short-sighted and transactional when it comes to allies. They will not necessarily do things to support allies and garner future goodwill. Their attitude is usually 'We will not do something that does not benefit us. If this benefits you more than us, then we will not assist.'" – Kenneth Pollack
What cyber or national security lessons has Iran learned from North Korea?	• "Iran has learned lessons on gray zone operations from the DPRK, China, and Russia." – Intelligence Community Official • "The US lacks this information. I cannot point to an example when Iran copied North Korean action." – Kenneth Pollack • "The Bank of Bangladesh heist has illustrated that they can get away with financially motivated attacks." – Annie Fixler • "Iran could eventually appreciate the value of cryptocurrency in facilitating these attacks." – Matt Ha

Select Questions	Notes and Selected Responses
Other Notes	• **All subject matter experts believed that financially motivated cyber attacks were insufficient forms of retaliation.** • "Iran strives for publicity and wants the US to know they can reach us." – Intelligence Community Official • "They're being attacked through the financial system so it's proportional to respond in kind with cyber but not for financial gain... they are top tier in cyber but struggle with organizational challenges... Ababil was not sophisticated and occasionally targeted small banks. We figured they were working off an unsophisticated targeting list." – J. Michael Daniel • "Russia helps their capacity building but we always believed they would get an older tool." – J. Michael Daniel • "ATM cash-out attacks could occur anywhere with a Hezbollah or Iranian proxy footprint. Iran would conduct these attacks where they gain the least attention." – Private Sector Researcher #2 • "Khamenei's successor will not necessarily be like him. It took Khamanei years to consolidate his position and feel at ease in his role or giving unpopular orders. He's rather indecisive and has allowed moderates to pursue their agenda. He could be replaced by a committee of hardliners... I actually do think that the Iranian president does matter and almost as much as the Supreme Leader." – Kenneth Pollack

7.C SELECT CYBER OPERATIONS ATTRIBUTED TO IRAN, 2011-2020

Cyber Operations Against Financial Sector Targets	
Operation Description	**Intentions and Additional Commentary**
2011-2013 DDoS attacks against the US Financial Sector. The operation cost 46 victims "tens of millions of dollars" in remediation expenses, and were perpetrated by seven individuals linked to the IRGC. One member of the group gained access to the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam in Rye, New York.[210]	**Non-Financial Motivation, Retaliation, Punishment, Destruction**. One member of the group was linked to a separate organization that had previously hacked servers belonging to NASA.[211] Some analysts view the operation as a response to the alleged Stuxnet attack by the US and Israel.[212]
2013-2017 Mabna Spearphishing Campaign directed primarily at educational institutions and US financial institutions.[213]	**Espionage, Motivation, Knowledge Acquisition.** Iranian actors targeted hundreds of universities around the world between 2013 and 2017, stealing over $3 billion of intellectual property and selling stolen data to Iranian institutions. The "hackers-for-hire" of the Mabna Institute, an Iran-based company dedicated to stealing foreign scientific resources, launched the spearphishing campaign to gain access to about 8,000 academics' email accounts.[214]
2015-2018 SamSam Ransomware Campaign. Attacked numerous corporations, hospitals, universities, and government agencies in several countries and held over 200 known victims' data at risk for financial gain.[215, 216]	**Financial Motivation**. Government nexus was not demonstrated. The attack prompted the US Department of Treasury, for the first time, to identify associated digital currency addresses to "pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards."[217]

2020 Ransomware Operation against Israeli insurance company, Chirbit.[218]	**Financial Motivation**. Both intentions and government nexus remain disputed by analysts.[219]
2020 Pay2Key Ransomware attacks targeting Israeli companies.[220, 221]	**Financial Motivation and / or Disruption**. Both intentions and state nexus remain disputed by analysts.[222]

Cyber Operations Against Other Targets

Operation Description	Intentions and Additional Commentary
2009 Iranian Cyber Army exploitation of Twitter DNS records to temporarily reroute all traffic to a site with a defacement message.[223]	**Domestic Surveillance**. The group, which is unofficially linked to the Iranian government and largely composed of individuals classified as "patriotic hackers" attacked other pro-demonstration sites following the Green Movement protests disputing election outcomes.
2011 Iranian government attack against DigiNotar, a Dutch security firm to collect information on Iranian citizens. The Iranian government used false security certificates to access all domestic Gmail accounts in a man-in-the-middle attack.[224]	**Domestic Surveillance**. The attack allowed the Iranian government to intercept the private communications of citizens.[225] This ranks as one of history's largest security breaches.
2012 Shamoon data-wiping malware attacks against Saudi Aramco, temporarily halting operations. The operation occurred in the wake of tensions with the US and Saudi Arabia and in response to malware attacks on Iranian oil facilities.[226]	**Destruction, Retaliation**. A group known as Cutting Swords of Justice took responsibility for the attack, though a government nexus is assessed with high confidence. Shamoon was designed to erase hard drive data by relying on a logic bomb to trigger this action at a specific local time during Ramadan.[227]
2017 IRGC-linked attack on the UK Parliament to exfiltrate personal information.[228]	**Espionage, Information Exfiltration**. More than 9,000 email accounts were compromised, including that of then Prime Minister Theresa May.[229]
2018 Shamoon malware attacks against Saudi Arabian and other Middle East targets along with increased attacks against the US post JCPOA withdrawal.[230]	**Destruction, Retaliation, Supporting Wider Political Objectives**. Analysts debate the extent to which Iran has used cyber and other means to coerce adversaries, primarily the US, to adopt policies, particularly over the JCPOA, benefiting its strategic positions.
April 2020 Government-backed Iranian cyber actors launch phishing campaign against WHO staffers in the midst of the COVID-19 pandemic.[231]	**Espionage, Sabotage, Information Exfiltration**. The hackers attempted to access employee credentials using phishing techniques.
May 2020 Iranian cyber group, Greenbug, compromised three telecommunication companies in Pakistan.[232]	**Espionage, Information Exfiltration**. While the attacker was noted for using off-the-shelf tools, it displayed commitment maintaining a low profile on the victims' network for an extended period.[233] In addition to backdoors and webshells, the attacker employed tools such as Mimikatz, Cobalt Strike, and Metasploit.[234]

April and July 2020 attempted breach of the Israeli national water system.	**Espionage, Destruction, Retaliation**. The April operation was reported as unsuccessful yet may have invoked in May an Israeli attributed cyber disruption of Iran's largest port in the Strait of Hormuz.[235] Israel's Water Authority immediately requested facilities to change the passwords of their Industrial Control Systems (ICS) The July operation targeted two water pumping and filtration sites[236] and may have occurred in retaliation to numerous fires, attributed as covert destructive actions, at Iranian nuclear facilities.[237]
2019-2020 Phosphorus (an Iranian cyber threat group) attacks various US targets, including credential compromise attempts against ~3,000 journalists, US government officials, politicians, and electrical grid elements.[238]	**Espionage, Sabotage, Societal Interference**. While the various credential compromise attacks utilized relatively unsophisticated means, they displayed high ingenuity in exploiting personal identifying information.[239] Phosphorus relied on open source intelligence (OSINT) and account recovery features to attempt account takeovers.[240]
2020 influence operations against the US presidential elections.[241] The operation was probably directly ordered by Ayatollah Khamene'i and supported by several thousand inauthentic social media accounts dating back to 2012.[242]	**Societal Interference, Concept Testing**. The operations impersonating The Proud Boys displayed understanding of US society but were quickly attributed due to poor operational security and tradecraft. In addition, the FBI announced that Iranian cyber actors targeted election websites to download voter registration information.[243]
February 2021 Iranian cyber actors targeted UAE and Kuwaiti government agencies as part of cyber espionage campaign.[244]	**Espionage Supporting Political Objectives**. These operations follow the UAE and Israel governments beginning the process of normalizing relations in 2020.

7.D SELECT CYBER OPERATIONS ATTRIBUTED TO NORTH KOREA, 2011-2020

Cyber Operations Against Financial Sector Targets	
Operation Description	**Intentions and Additional Commentary**
2011 Ten Days of Rain targeted South Korean media, financial, and government institutions by injecting malware into two peer-to-peer file-sharing websites.[245]	**Disruption**. The attackers infected up to 40 websites and 11,000 personal computers. The attack destroyed 273 of NongHyup Bank's 587 servers by infiltrating the bank's computers for over seven months.[246]
2013 Dubbed as Operation DarkSeoul, North Korean hackers targeted ROK public broadcasters, financial institutions, and the government's Domain Name System.[247]	**Retaliation, Disruption**. The attacks followed 13 days after the UNSC Resolution 2094 imposed new sanctions on DPRK for conducting its third nuclear test. Targets experienced network shutdowns, and only 10% of the websites were working within two days, with 48,000 machines infected.[248]
2016 The Lazarus group executed a fraudulent transfer of $81 million in a Bangladesh Central Bank Attack by using stolen SWIFT credentials.[249].	**Financial Motivation**. The hackers used the same code used in the 2014 operations against Sony Pictures Entertainment.[250]

2017 The Lazarus group created a WannaCry 2.0 ransomware cryptoworm from a leaked NSA exploit known as Eternal Blue.[251]	**Financial Motivation and Disruption**. The ransomware infected thousands of computers globally, asking users to pay a $300 ransom in bitcoin.[252] The ransomware was especially dangerous since it can spread across an infected network by exploiting Windows computers' critical vulnerabilities.[253]
2016-2020 North Korean actor, HIDDEN COBRA, has targeted banks in Africa and Asia in operations known as the FASTCash Campaign.[254]	**Financial Motivation**. Hackers compromise payment switch application servers within banks to facilitate fraudulent transfers through FASTCash schemes. Hackers enable cash to be withdrawn from ATMs in 23 different countries.[255]
2017 The BlueNoroff hackers, a subgroup of Lazarus, targeted South Korea's cryptocurrency exchange, YouBit in a series of attacks.[256]	**Financial Motivation**. The hackers first stole $5 million in April and stole $15.6 million in December 2017.[257] After the two attacks, Youbit lost 17% of its assets, forcing it to declare bankruptcy.[258]
2018 South Korea's cryptocurrency exchanges, Coinrail and Bithumb were targeted by North Korean hackers.[259] 2020 cryptocurrency exchange based in Hong Kong, KuCoin was targeted by the Lazarus group.[260]	**Financial Motivation**. The two exchanges lost $37 million and $40 million, respectively.[261] Bitcoin suffered a 5% devaluation following the Coinrail attack.[262] The Lazarus Group stole $275 million in cryptocurrency from KuCoin, which is the largest cryptocurrency theft of the year.[263]

Cyber Operations Against Other Targets	
Operation Description	**Intentions and Additional Commentary**
2013 North Korean hackers targeted South Korean think tanks and the Ministry of Reunification in an operation known as Campaign Kimsuky.[264]	**Disruption, Information Exfiltration, Espionage**. The attacker distributed malware through spear-phishing emails, which triggered the download and execution of remote control access to access data related to nuclear deterrence and economic sanctions.[265]
2014 Operation Korean Hydro and Nuclear Power, North Korean hackers targeted Korea Hydro and Nuclear Power (KHNP), South Korea's nuclear power plant operator.[266]	**Disruption, Espionage**. Over 5,000 phishing emails infected with malware. The attackers stole reactor designs and 10,0000 files on personnel.[267]
2014 A group of hackers known as "the Guardians of Peace" attacked Sony Pictures Entertainment in retaliation against the Kim regime's comedic portrayal in the film, "The Interview."[268]	**Destruction, Retaliation, Information Exfiltration**. The hackers stole confidential information, erased data, and published stolen files on the Internet using file-sharing hubs.[269] One of the identified attackers was a member of the RGB's Lab 110.[270] It is the first-ever attribution to a nation-state made by the US president and the first time an act of coercion through cyberspace had compelled a major organization to revise its business operation plans.[271]

7.E JUDGMENTS OF LIKELIHOOD

The capstone team used the following chart from the US Intelligence Community's guidance and framework on Estimative Language[272] to convey judgments of likelihood contained in sections 7.2 Scenario Development and 7.3 Key Assessment. The chart summarizes how judgments of likelihood correlate with certain percentage outcomes.

Very Unlikely	Unlikely	Roughly Even Odds	Likely	Very Likely
0% to 20%	20% to 40%	~50%	60% to 80%	80% to 100%

7.F CAPSTONE TEAM'S KEY DISCUSSIONS ON THE DRIVER'S IMPACT

The following section details the five key internal discussions among the capstone team members that took place while weighing the impact of each driver.

Key Leadership Composition v. Iran's Risk Appetite | Vote: 0-8

The first discussion was on whether Iran's *Key Leadership Composition* is more impactful than *Iran's Risk Appetite.* Those who advocated for *Iran's Risk Appetite* expressed the following:

- Iran would have limited advantages for adopting an escalatory posture.
- Experiencing a significant increase in economic pressures from international sanctions could press Iran to be more risk-accepting and willing to address the consequences of adopting a more aggressive posture.

Those who advocated for *Key Leadership Composition* expressed the following:

- Iranian leadership dictates all of the key policy decisions and thus, has the highest impact.
- The opacity and the unpredictability of the Iranian's key leadership composition mean that changes in Key Leadership Composition could result in major policy changes.
- Iran would not be taking significant risks by attacking financial institutions. For example, Iran did not face a proportional retaliation following the Las Vegas Sands casino cyber attack.[273]

Key Leadership Composition v. Perception of Isolation | Vote: 8-0

The second discussion was on whether *Key Leadership Composition* is more impactful than *Perception of Isolation*. The capstone team agreed that both drivers are impactful but parsed out the arguments for and against *Key Leadership Composition* in this discussion.

In addition to the arguments previously mentioned for *Key Leadership Composition*, those who advocated for this driver expressed the following:

- Changes in leadership composition are the only way there will be structural changes to the Iranian posture.
- While the Supreme Leader and the President are not necessarily involved in the decision-making process surrounding FM cyber attacks, they have senior officials who represent their viewpoints and anticipate what actions are necessary to pursue to accomplish the regime's foreign policy objectives.
- The promotion of cyber operators within Iran's military, especially within the IRGC, underscores the importance of decision-making at the top leadership level.

Those who argued against *Key Leadership Composition* expressed the following:

- MOIS and the IRGC are still learning how to better coordinate their cyber operations at the operational and tactical levels. Therefore, their operations are not related to the structure of the top leadership of the Iranian government.
- Perception of Isolation drives the key leadership's decisions.

Key Leadership Composition v. Grievance Retaliation | Vote: 2-6

The third discussion was on whether *Key Leadership Composition* was more impactful than *Grievance Retaliation*. The key argument against Grievance Retaliation was that it would be an unprecedented event for Iran to pursue this policy. Thus, it is important to consider how Iran would respond to increased international sanctions in the future.

Grievance Retaliation v. Economic Welfare | Vote: 5-3

The fourth discussion was on whether ***Grievance Retaliation*** is more impactful than Iran's ***Economic Welfare***. External events have a greater impact on Iran's foreign policy than its domestic economic situation. For Iran to adopt this policy, the capstone team considered the proportionality of attacks in response as a Grievance Retaliation. For example, if Iran feels increased economic pressures, it would be logical for Iran to respond with cyber attacks against financial institutions.

Iran's Risk Appetite v. Economic Welfare | Vote: 7-1

The fifth discussion was on whether ***Iran's Risk Appetite*** is more impactful than Iran's ***Economic Welfare.*** While other factors could influence Iran's risk appetite, such as military activities in the region, the currently shrinking economy has not led the regime to adopt such a policy. Those who advocated for Iran's ***Economic Welfare*** asserted that economic pressures felt by Iran determine the country's risk acceptance. However, if the Iranian economy continued to contract, Iran would need to have a higher risk tolerance to adopt a financially motivated cyber attacks policy.

7.G CAPSTONE TEAM'S KEY DISCUSSIONS ON THE DRIVER'S PROBABILITY

The following section details the five key discussions among the capstone team that took place while weighing the probability of each driver.

JCPOA Negotiations v. Perception of Isolation | Vote: 6-2

The first discussion was on whether ***JCPOA Negotiations*** are more likely to change than Iran's ***Perception of Isolation***. It is more probable for ***JCPOA Negotiations*** to change due to the current and ongoing efforts to re-engage in discussions. Simultaneously, external factors, such as increased hostile activities towards Iran, affect the probability of Iran's ***Perception of Isolation*** changing.

Grievance Retaliation v. Key Leadership Composition | Vote: 2-6

The second discussion was on whether ***Grievance Retaliation*** is more likely to change than ***Key Leadership Composition***. ***Grievance Retaliation*** is considered to be an action taken by Iran in response to sanctions, which could be highly probable if further enacted. However, several immediate changes in ***Key Leadership Composition*** are more likely to occur that the team considered. For example, the Supreme Leader's death and the upcoming Iranian presidential election, replacing President Rouhani with a hardline candidate.

JCPOA Negotiations v. Key Leadership Composition | Vote: 2-6

The third discussion was on whether ***JCPOA Negotiations*** are more likely to change than ***Key Leadership Composition***. The capstone team believed that these two drivers were connected. Some capstone team members considered that the outcome of Iran's presidential election would not change Iran's policies on financially motivated cyber attacks but affect the outcome of JCPOA negotiations.

Iran's Risk Appetite v. Domestic Regime Popularity | Vote: 5-3

The fourth discussion was on whether ***Iran's Risk Appetite*** was more likely to change than ***Domestic Regime Popularity***. Some members of the capstone team argued that upcoming events, such as the Iranian presidential election and the potential JCPOA negotiations, are more likely to change the ***Domestic Regime Popularity*** than ***Iran's Risk Appetite***, and that ***Iran's Risk Appetite*** will remain steady and unlikely to change significantly, while domestic stability could impact other drivers. However, these domestic events could change ***Iran's Risk Appetite***, even if it meant that these were incremental changes.

General Cyber Capabilities v. Domestic Regime Popularity | Vote: 2-6

The last discussion was on whether ***General Cyber Capabilities*** are more likely to change than the ***Domestic Regime Population*** of Iran. Some members of the capstone believe Iran's ***General Cyber Capabilities*** could change incrementally sooner than its ***Domestic Regime Popularity***. However, the capstone team believed that there is a general disapproval of the Iranian government, which will remain steadily high or incrementally increase over time. For example, regardless of a new presidential candidate, dissatisfaction with the regime will continue to increase.

7.H IRAN DRIVER COMPARISON TABLE – IMPACT AND PROBABILITY

During the analysis stage, the capstone team ranked the nine drivers based on each driver's impact and probability using a pair comparison matrix. The matrix compared (1) the likelihood that each driver would be subject to change within the next two years, and (2) the impact that each driver has on the question of whether or not Iran will pursue financially motivated cyber attacks

Axis: X = Impact Y = Probability	1 Key Leadership Composition	2 Perception of Isolation	3 Grievance Retaliation	4 Domestic Regime Stability	5 JCPOA Negotiations	6 Iran Risk Appetite	7 Iran's Economic Welfare	8 General Cyber Capability	9 Nuclear Development
1 Key Leadership Composition		2 (Vote 3-5)	1 (Vote 6-2)	1 (Vote 8-0)	1 (Vote 5-3)	1 (Vote 5-3)	1 (Vote 6-2)	1 (Vote 7-1)	1 (Vote 8-0)
2 Perception of Isolation	1 (Vote 2-6)		2 (Vote 5-3)	2 (Vote 8-0)	2 (Vote 6-2)	2 (Vote 5-3)	2 (Vote 5-3)	2 (Vote 7-1)	2 (Vote 8-0)
3 Grievance Retaliation	1 (Vote 2-6)	2 (Vote 3-5)		3 (Vote 7-1)	3 (Vote 5-3)	3 (Vote 6-2)	7 (Vote 2-6)	3 (Vote 6-2)	3 (Vote 8-0)
4 Domestic Regime Stability	1 (Vote 0-8)	2 (Vote 2-6)	3 (Vote 0-8)		5 (Vote 0-8)	6 (Vote 1-7)	7 (Vote 0-8)	8 (Vote 2-6)	4 (Vote 7-1)
5 JCPOA Negotiations	1 (Vote 2-6)	5 (Vote 6-2)	5 (Vote 5-3)	5 (Vote 7-1)		6 (Vote 2-6)	7 (Vote 3-5)	5 (Vote 7-1)	5 (Vote 8-0)
6 Iran Risk Appetite	1 (Vote 1-7)	6 (Vote 5-3)	6 (Vote 5-3)	6 (Vote 5-3)	5 (Vote 2-6)		7 (Vote 2-6)	6 (Vote 6-2)	6 (Vote 8-0)
7 Iran's Economic Welfare	1 (Vote 2-6)	7 (Vote 7-1)	7 (Vote 6-2)	7 (Vote 8-0)	5 (Vote 1-7)	7 (Vote 6-2)		7 (Vote 7-1)	7 (Vote 8-0)
8 General Cyber Capability	1 (Vote 0-8)	2 (Vote 3-5)	3 (Vote 3-5)	4 (Vote 2-6)	5 (Vote 1-7)	6 (Vote 3-5)	7 (Vote 1-7)		8 (Vote 8-0)
9 Nuclear Development	1 (Vote 1-7)	2 (Vote 1-7)	3 (Vote 0-8)	4 (Vote 0-8)	5 (Vote 0-8)	6 (Vote 0-8)	7 (Vote 0-8)	8 (Vote 0-8)	

8 SOURCES

1 "Islamic Republic of Iran," ***The World Bank***, https://www.worldbank.org/en/country/iran/overview#:~:text=Gross%20Domestic%20Product%20(GDP)%20has,population%20of%20about%2084%20million.
2 "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," ***US Department of Justice***, November 28, 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.
3 "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," ***American Psychological Association***, 2009, 34, https://doi.org/10.1037/e587102011-001.
4 Richards J. Heuer and Randolph H. Pherson, ***Structured Analytic Techniques for Intelligence Analysis*** (Washington, DC: CQ Press, 2011), 99–102.
5 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 99–103.
6 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 99–103.
7 See appendix for details.
8 Jason Healey et al, "The Future of Financial Stability and Cyber Risk," ***Brookings***, 10 Oct. 2018, https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/.
9 James Lewis, "Iran and Cyber Power," ***Center for Strategic and International Studies***, 25 Jun. 2019, https://www.csis.org/analysis/iran-and-cyber-power/.
10 Annie Fixler, "The Cyber Threat from Iran after the Death of Soleimani," ***Combatting Terrorism Center at West Point***, February 2020, 25, https://ctc.usma.edu/wp-content/uploads/2020/02/CTC-SENTINEL-022020.pdf.
11 "The Battlefield of Today and Tomorrow: Cyber-Enabled Economic Warfare," ***FDD***, November 13, 2018, https://www.fdd.org/events/2018/11/13/the-battlefield-of-today-and-tomorrow-cyber-enabled-economic-warfare/#downloads.
12 Ilan Berman, "Iranian Cyber Threat to the U.S. Homeland," ***U.S. Government Publishing Office***, April 26 2012, 112–86, https://www.govinfo.gov/content/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm.
13 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis,*** 80–81.
14 John D. Lowrance and Janet L. Murdock, "Political, Military, Economic, Social, Infrastructure, Information (PMESII) Effects Forecasting for Course of Action (COA) Evaluation," ***Air Force Research Laboratory***, 2009, 1.
15 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 58–59.
16 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 100–104.
17 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 100–110.
18 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 80-84.
19 Gabriel Basset et. al., "Verizon Data Breach Investigations Report," ***Verizon***, 2020, https://enterprise.verizon.com/resources/reports/dbir/2020/data-breaches-by-region/.
20 Woo-ik Yu, Bae-ho Hahn, Young Ick Young Ick Lew, Chan Lee, and Jung Ha Lee, "North Korea". ***Encyclopedia Britannica***, January 11, 2021, https://www.britannica.com/place/North-Korea.
21 Kathleen J. McInnis, et. al., ***The North Korean Nuclear Challenge: Military Options and Issues for Congress*** (Washington, DC: CRS, 2017), 6, https://fas.org/sgp/crs/nuke/R44994.pdf,

22 "Military and Security Developments Involving the Democratic People's Republic of Korea," ***U.S. Department of Defense***, (Washington, DC: US Government Printing Office, 2017), 5. https://fas.org/irp/world/dprk/dod-2017.pdf.
23 "Military and Security Developments Involving the Democratic People's Republic of Korea," ***U.S. Department of Defense***, 2012, https://archive.defense.gov/pubs/report_to_congress_on_military_and_security_developments_involving_the_dprk.pdf.
24 McInnis, et. al., "The North Korean Nuclear Challenge: Military Options and Issues for Congress."
25 "Annual Threat Assessment of the US Intelligence Community," ***Office of the Director of National Intelligence***, April 9, 2021, pp. 15-16, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
26 "Military and Security Developments Involving the Democratic People's Republic of Korea," ***U.S. Department of Defense***, 2012, 13.
27 Jenny Jun, Scott LaFoy, and Ethan Sohn, directed by Victor Cha and James Lewis, "North Korea's Cyber Operations: Strategy and Responses," ***Center for Strategic and International Studies***, October 2015, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.
28 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 27.
29 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 5.
30 Jun, LaFoy, and Sohn, "North Korea's Cyber Operations," 38.
31 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 38.
32 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 35.
33 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 36.
34 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 36.
35 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 37.
36 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 41.
37 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 42.
38 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 43.
39 Ji Young Kong and Kyoung Gon Kim,, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," ***International Conference on Cyber Conflict***, 2018, 6, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.
40 Kim and Kong, "The All-Purpose Sword," 6.
41 Kim and Kong, "The All-Purpose Sword," 7.
42 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 46.
43 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 49.
44 Jun et al., "North Korea's Cyber Operations: Strategy and Responses, 49.
45 Jun et al., "North Korea's Cyber Operations: Strategy and Responses, 47.
46 Jun et al., "North Korea's Cyber Operations: Strategy and Responses, 47-8.
47 Kong and Kim, "The All-Purpose Sword," 14.
48 Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," ***Recorded Future***, April 25, 2018, 10, https://go.recordedfuture.com/hubfs/reports/cta-2018-0425.pdf.
49 Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," 11.
50 Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," 11.
51 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 6.
52 Jun et al., "North Korea's Cyber Operations: Strategy and Responses," 44.
53 Kong and Kim, "The All-Purpose Sword," 11.
54 Kong and Kim, "The All-Purpose Sword," 13.
55 Kong and Kim, "The All-Purpose Sword," 13.
56 "APT 37 (Reaper): The Overlooked North Korean Actor," ***FireEye***, February 20, 2018, https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html.
57 Bosung Kim, "Gross Domestic Product Estimates for North Korea in 2019," Bank of Korea, July 31, 2020, 1, https://www.bok.or.kr/viewer/skin/doc.html?fn=202007300329527700.doc&rs=/webview/result/E0000634/202007.
58 Bosung, "Gross Domestic Product Estimates," 1.
59 Bosung, "Gross Domestic Product Estimates," 4.
60 Resolution 2371, ***United Nations Security Council***, August 5, 2017, https://www.undocs.org/S/RES/2371%20(2017).
61 Eleanor Albert, "What to Know About Sanctions on North Korea," ***Council on Foreign Relations***, July 16, 2018, https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea.
62 "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," S/2017/150, ***United Nations Security Council***, February 27, 2017.
63 Chang Ku Kang, "Gross Domestic Product Estimates for North Korea in 2017," ***Bank of Korea***, 2017, 4, https://www.bok.or.kr/eng/bbs/E0001959/view.do?nttId=230095&menuNo=400071&pageIndex=7.
64 "China Product Imports from Korea," World Integrated Trade Solution, 2018, https://wits.worldbank.org/CountryProfile/en/Country/CHN/Year/2018/TradeFlow/Import/Partner/PRK/Product/all-groups.
65 KKim Kyoochul, "Finding Loopholes in Sanctions: Effects of Sanctions on North Korea's Refined Oil Prices," ***KDI Journal of Economic Policy***, Vol. 42, Korean Development Institute, November 2020, 1-25, 30, http://kdijep.org/v.42/4/1/Finding+Loopholes+in+Sanctions+Effects+of+Sanctions+on+North+Korea%E2%80%99s+Refined+Oil+Prices%E2%80%A0.
66 "Resolution 2397," ***United Nations Security Council***, December 23, 2017, 2, https://www.undocs.org/S/RES/2397%20(2017).
67 "Panel of Experts Midterm Report," ***United Nations Security Council***, August 30, 2019, 691, https://www.securitycouncilreport.org/atf/cf/%7B65BF-

CF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.
68 "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options," Chainalysis Team, ***Insights***, February 21, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack.
69 "Panel of Experts Midterm Report," ***United Nations Security Council,*** August 30, 2019, 691, https://www.securitycouncilreport.org/atf/cf/%7B65BF-CF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.
70 "Panel of Experts Midterm Report," ***United Nations Security Council,*** 691.
71 "Panel of Experts Final Report," ***United Nations Security Council***, March 4, 2021, 14, https://undocs.org/S/2021/211.
72 "Panel of Experts Final Report," ***United Nations Security Council***, 15.
73 "Panel of Experts Final Report," ***United Nations Security Council***, 20.
74 "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," S/2017/150, ***United Nations Security Council***, February 27, 2017, 280.
75 "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," 43.
76 "Case 1:20-Cr-00032-RC," U.S. District Court for the District of Columbia, February 5, 2020, https://int.nyt.com/data/documenthelper/6971-north-korea-indictment/422a99ddac0c39459226/optimized/full.pdf#page=1.
77 "UN Deadline to Send North Korean Workers Home Likely Unmet," ***AP NEWS***, December 20, 2019, https://apnews.com/article/60c9e836a2ef5f61ace074338736e82b.
78 Ali M. Ansari, ed. ***Modern Iran since 1797: Reform and Revolution***, 3rd ed. (London: Routledge, 2019).
79 Ervand Abrahamian, "The 1953 Coup in Iran," ***Science & Society***, vol. 65 no. 2 (Summer 2001): 182-215.
80 Ansari, ***Modern Iran since 1797***.
81 Ansari, ***Modern Iran since 1797***.
82 Ansari, ***Modern Iran since 1797***.
83 Vali Nasr, "Iran Among the Ruins: Tehran's Advantage in a Turbulent Middle East," ***Foreign Affairs***, vol. 97 no. 2 (March/April 2018): 108-18, https://www.fpi.sais-jhu.edu/single-post/2018/04/10/iran-among-the-ruins-tehran-s-advantage-in-a-turbulent-middle-east.
84 "The Islamic Republic's Power Centers," ***Council on Foreign Relations***. February 25, 2020, https://www.cfr.org/article/islamic-republics-power-centers.
85 Wilfried Buchta, "Who Rules Iran? The Structure of Power in the Islamic Republic," ***The Washington Institute for Near East Policy***, January 1, 2000, https://www.washingtoninstitute.org/policy-analysis/who-rules-iran-structure-power-islamic-republic.
86 "The Islamic Republic's Power Centers," ***Council on Foreign Relations***.
87 Nasr, "Iran Among the Ruins."
88 "Iran's Revolutionary Guards," ***Council on Foreign Relations***, May 6, 2019, https://www.cfr.org/backgrounder/irans-revolutionary-guards.
89 "Foreign Terrorist Organizations," ***United States Department of State Bureau of Counterterrorism***, https://www.state.gov/foreign-terrorist-organizations/.
90 Ray Takeyh, "The Iran-Iraq War: A Reassessment," ***Middle East Journal***, 64 no. 3 (Summer 2010), pp. 365-83.
91 "Iran's Revolutionary Guards," ***Council on Foreign Relations***.
92 "Iran's Revolutionary Guards," ***Council on Foreign Relations***.
93 Mohammad Javad Zarif, "Mohammad Javad Zarif: Europe Must Work with Iran," ***The New York Times,*** December 10, 2017, https://www.nytimes.com/2017/12/10/opinion/mohammad-javad-zarif-europe-iran.html.
94 Wendy R. Sherman, "How We Got the Iran Deal And Why We'll Miss It," ***Foreign Affairs***, September/October 2018, 186-97, https://www.foreignaffairs.com/articles/2018-08-13/how-we-got-iran-deal.
95 Kenneth Katzman, "Iran: Internal Politics and U.S. Policy and Options," ***Congressional Research Service Report***, December 19, 2018, https://crsreports.congress.gov.
96 Farnaz Fassihi, "With Brutal Crackdown, Iran is Convulsed by Worst Unrest in Forty Years," ***New York Times***, December 1, 2019, https://www.nytimes.com/2019/12/01/world/middleeast/iran-protests-deaths.html.
97 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," Carnegie Endowment for International Peace, January 4, 2018, 39, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.
98 Supported by the interview with Private Sector Researcher #1 Interview.
99 Supported by the interview with Sanaz Yashar on April 6, 2021.
100 Supported by interviews with Private Sector Researcher #1; Private Sector Researcher #2; Intelligence Community Official; Michael Daniel; and JD Work.
101 Supported by interviews with Sanaz Yashar; Michael Daniel; Private Sector Researcher #1; and Private Sector Researcher #2.
102 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," ***Carnegie Endowment for International Peace***, January 4, 2018, 39, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.
103 Fixler, "The Cyber Threat from Iran after the Death of Soleimani," 21–22.
104 Anderson and Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," 37–38.
105 Adam Meyers, "Who is Clever Kitten," Crowdstrike, April 4, 2013, https://www.crowdstrike.com/blog/whois-clever-kitten/.
106 Fixler, "The Cyber Threat from Iran after the Death of Soleimani," 21.
107 Russell Brandom, "Iran Hacked the Sands Hotel Earlier This Year, Causing over $40 Million in Damage," The Verge, December 11, 2014, https://www.theverge.com/2014/12/11/7376249/iran-hacked-sands-hotel-in-february-cyberwar-adelson-israel.
108 Fixler, "The Cyber Threat from Iran after the Death of Soleimani," 24.
109 Marie Fazio, "Two Men Are Accused of Hacking U.S. Websites with Pro-Iran Messages," ***The New York Times*** September 15, 2020, https://www.nytimes.com/2020/09/15/us/government-websites-hacked-suleimani.html#:~:text=the%20main%20story-,Two%20Are%20Accused%20of%20Hacking%20U.S.%20Websites%20With%20Pro%2DIran,a%20federal%20indictment%20unsealed%20Tuesday.

110 Gabi Siboni, Léa Abramski, and Gal Sapir, "Iran's Activity in Cyberspace:
Identifying Patterns and Understanding the Strategy," Institute for National Security Studies, Cyber, Intelligence,and Security 4, no. 1 (March 2020), https://www.inss.org.il/wp-content/uploads/2020/03/Cyber4.1ENG_e-23-42.pdf.
111 Kevin Mandia and David Petraeus, "2021 Cybersecurity Summit Day 1," interview by Suzanne Kelley, ***The Cipher Brief***, March 23, 2021, https://www.youtube.com/watch?v=fdofqh4z-TM.
112 Supported by interviews with Michael Daniel; Private Sector Researcher 1; and Private Sector Researcher 2.
113 Catherine A. Theohary, "Iranian Offensive Cyber Attack Capabilities," ***Congressional Research Service***, January 13, 2020), https://fas.org/sgp/crs/mideast/IF11406.pdf.
114 Supported by interviews with Private Sector Researcher 1; Private Sector Researcher 2; and JD Work.
115 Supported by interviews with Private Sector Researcher 1; Private Sector Researcher 2; and JD Work.
116 Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," ***Recorded Future***, May 9, 2018, https://www.recordedfuture.com/iran-hacker-hierarchy/.
117 Gundert, Chohan, and Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations."
118 Pooya Azadi, Matin Mirramezani, and Mohsen B. Mesgaran, "Migration and Brain Drain from Iran," Stanford Iran 2040 Project, April 2020, https://iranian-studies.stanford.edu/iran-2040-project/publications/migration_and_brain_drain_from_Iran.
119 Anderson and Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," 52.
120 "World Economic Outlook Update," International Monetary Fund, January 2021, https://www.imf.org/en/Publications/WEO/weo-database/2020/October/weo-report?c=429,&s=NGDP_R,NGDP_RPCH,NGDPD,&sy=2018&ey=2020&ssm=0&scsm=1&scc=0&ssd=1&ssc=0&sic=0&sort=country&ds=.&br=1.
121 "Economic Trends No. 99 Fourth Quarter 1398," ***Central Bank of Iran***, August 2020, https://www.cbi.ir/page/20473.aspx.
122 "Economic Trends No. 101 Second Quarter 1399," ***Central Bank of Iran,*** March 2021, https://www.cbi.ir/simplelist/21402.aspx.
123 "Economic Trends No. 101 Second Quarter 1399," ***Central Bank of Iran.***
124 "Imports and Exports by Country(Region) of Origin/Destination, 2.2021," ***General Administration of Customs People's Republic of China***, March 18, 2021, http://english.customs.gov.cn/Statics/1356599a-4f92-4688-970a-fea711c22f96.html.
125 "Resolution 2231. S/RES/2231," ***United Nations Security Council,*** April 3, 2021, https://undocs.org/S/RES/2231(2015).
126 "United States Fails to Secure Multilateral Snapback Sanctions Against Iran." ***American Journal of International Law,*** vol. 115, no. 1 (2021): 140–46. doi:10.1017/ajil.2020.101.
127 Najmeh Bozorgmehr, "Iran Ready to Resume Nuclear Talks If US Lifts Sanctions Within a Year," ***Financial Times***, March 5, 2021, https://www.ft.com/content/cf9e58da-9225-422b-9f97-0b8d4bf1c9b1.
128 Kenneth Katzman, "Iran Sanctions," ***Congressional Research Service,*** November 18, 2020, 41–42, https://fas.org/sgp/crs/mideast/RS20871.pdf.
129 Kenneth Katzman, "Iran Sanctions," 19.
130 "Islamic Republic of Iran and the IMF." ***nternational Monetary Fund***, https://www.imf.org/en/Countries/IRN.
131 "Islamic Republic of Iran and the IMF." ***nternational Monetary Fund***.
132 Esfandyar Batmanghelidj, "Resistance Is Simple, Resilience Is Complex: Sanctions and the Composition of Iranian Trade," ***The SAIS Initiative for Research on Contemporary Iran,*** December 7, 2020, https://static1.squarespace.com/static/5f0f5b1018e89f351b8b3ef8/t/5fd0e4a906d21916ed79ba75/1607525546925/IranUnderSanctions_Batmanghelidj.pdf.
133 Batmanghelidj, "Resistance Is Simple, Resilience Is Complex: Sanctions and the Composition of Iranian Trade," 33.
134 "Budget Bill for 1399 Approved," ***Iran News Daily***, December 17, 2019, https://irannewsdaily.com/2019/12/budget-bill-for-1399-approved/.
135 "Economic Trends No. 101 Second Quarter 1399." ***Central Bank of Iran***.
136 Brendon Hong, "China Is Still Brimming with Iranian Oil," ***Atlantic Counci***l, 10 February 10, 2021, https://www.atlanticcouncil.org/blogs/iransource/china-is-still-brimming-with-iranian-oil/.
137 TTom Stocks, Daniela Castro, and Kelly Bloss (OCCRP) and Adam Klasfeld (Courthouse News), "'The Government Is In on It': An Insider's Account of the Reza Zarrab Conspiracy," ***Organized Crime and Corruption Reporting Project,*** September 20, 2020, https://www.occrp.org/en/the-fincen-files/the-government-is-in-on-it-an-insiders-account-of-the-reza-zarrab-conspiracy.
138 Katrina Manson, "US Warns China It Will Enforce Sanctions on Iran Oil Shipments," ***Financial Times***, March 17, 2021, https://www.ft.com/content/21eb2d88-3bae-4db3-944c-ba92f3924300.
139 Maziar Motamedi, "Policy Change at China's Bank of Kunlun Cuts Iran Sanctions Lifeline," ***Bourse & Bazaar***, January 2, 2019, https://www.bourse-andbazaar.com/articles/2019/1/2/policy-change-at-chinas-bank-of-kunlun-cuts-sanctions-lifeline-for-iranian-industry.
140 "North Korea 'halts missile and nuclear tests', says Kim Jong-un," ***BBC***, April 21, 2018, https://www.bbc.com/news/world-asia-43846488.
141 Robert Kelly, "Have the Winter Olympics repaired North-South Korea relations?" ***BBC***, February 20, 2018, https://www.bbc.com/news/world-asia-43063399.
142 "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," ***US Department of Justice,*** September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
143 Bosung Kim, "Gross Domestic Product Estimates for North Korea in 2019," ***Bank of Korea,*** July 31, 2020, 1, https://www.bok.or.kr/viewer/skin/doc.html?fn=202007300329527700.doc&rs=/webview/result/E0000634/202007.
144 "World Economic Outlook Update," ***International Monetary Fund***.
145 "OPEC Annual Statistical Bulletin 2020," Organization of the Petroleum Exporting Countries, July 13, 2020, 22, https://asb.opec.org/ASB_PDFDownload.php.
146 "North Korea," ***US Energy Information Administration,*** June 2018, https://www.eia.gov/international/analysis/country/PRK.
147 "Iran Embassies & Consulates" ***EmbassyPages***, March 21, 2021, https://www.embassypages.com/iran.

148 "Democratic People's Republic of Korea Embassies & Consulates," Embassy Pages. March 21, 2021, https://www.embassypages.com/koreademocratic.
149 Ashley Lane, "Iran's Islamist Proxies in the Middle East," ***Wilson Center***, December 17, 2020, https://www.wilsoncenter.org/article/irans-islamist-proxies.
150 Eleanor Albert, "The China-North Korea Relationship." ***Council on Foreign Relation***s, June 25, 2019, https://www.cfr.org/backgrounder/china-north-korea-relationship.
151 Ariel Cohen, "China-Iran $400 Billion Accord: A Power Shift Threatens Western Energy," ***Forbes***, April 5, 2021, https://www.forbes.com/sites/arielcohen/2021/04/05/china-iran-400-billion-accord-a-power-shift-threatens-western-energy/?sh=a79fdb49e00d.
152 Albert, "North Korea's Power Structure," ***Council on Foreign Relation***s.
153 "The Islamic Republic's Power Centers," ***Council on Foreign Relations***, February 25, 2020, https://www.cfr.org/article/islamic-republics-power-centers.
154 Karim Sadjadpour, "Maximum Drama, Minimum Change: Iran's Presidential Elections," ***The Atlantic***, May 18, 2017, https://www.theatlantic.com/international/archive/2017/05/iran-presidential-elections-rouhani/527283/.
155 "North Korean Nuclear Negotiations 1985-2019." ***Council on Foreign Relations***, 2019, https://www.cfr.org/timeline/north-korean-nuclear-negotiations.
156 Mark Landler, "Trump Abandons Iran Nuclear Deal He Long Scored," ***The New York Times***, May 8, 2018, https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html.
157 "Iran Nuclear Talks Make Some Progress in Vienna," ***Radio Free Europe Radio Liberty***, April 9, 2020, https://www.rferl.org/a/iran-nuclear-talks-vienna/31195277.html.
158 Expert interviews indicated that Iran's cyber capabilities are highly sophisticated.
159 Expert interviews indicated that any high-level policy changes regarding any major aspect of Iran's foreign policy, such as significant cyber attacks, is most likely decided by the country's key leadership.
160 Alyza Sebenius. "Iran's Cyber Attack on Billionaire Adelson Provides Lesson on Strategy," Bloomberg, January 5, 2020, https://www.bloomberg.com/news/articles/2020-01-05/iranian-attack-on-adelson-provides-lesson-on-cyber-strategy.
161 Amy Slipowitz, "The True Depth of Iran's Online Repression," Freedom House, December 2, 2019, https://freedomhouse.org/article/true-depth-irans-online-repression.
162 An expert interview indicated that the more pressed financially Iran feels, the more likely it is to look for additional or alternative means for financial gain.
163 David, Sanger, "How Israel, in the Dark of Night, Torched Its Way to Iran's Nuclear Secrets," T***he New York Time***, July 15, 2018, https://www.nytimes.com/2018/07/15/us/politics/iran-israel-mossad-nuclear.html; Mohsen Fakhrizadeh, "Iran scientist 'killed by remote-controlled weapon," ***BBC***, November 30, 2020, https://www.bbc.com/news/world-middle-east-55128970;
164 Stephen Farrell, " Iranian nuclear scientist killed by one-ton automated gun in Israeli hit; Jewish Chronicle," ***Reuters***, February 10, 2021,https://www.reuters.com/article/us-iran-nuclear-scientist/iranian-nuclear-scientist-killed-by-one-ton-automated-gun-in-israeli-hit-jewish-chronicle-idUSKBN2AA2RC.
165 Heuer and Pherson, ***Structured Analytic Techniques for Intelligence Analysis***, 100-104.
166 "Unlikely", and other likelihood assessments in this section refer to "Judgements of Likelihood", that are also commonly referred to as "Words of Estimative Probability." Further descriptions and implied percentage probabilities are described in Appendix E: Judgements of Likelihood.
167 "In secret recording, Iran's FM says downing of Ukraine flight could have been intentional," ***Arab News***, February 10, 2021, https://www.arabnews.com/node/1806881/middle-east.
168 Zachary, Cohen, "US intelligence indicates Iran paid bounties to Taliban for targeting American troops in Afghanistan," ***CNN***, August 17, 2020, https://www.cnn.com/2020/08/17/politics/iran-taliban-bounties-us-intelligence/index.htm.
169 Supported by interviews with Michael Daniel; Sanaz Yashar, JD Work; Luke McNamara; Gabi Siboni; Annie Fixler; Kenneth Pollack; Intelligence Community Official; Private Sector Researcher #1; and Private Sector Researcher #2.
170 James Kilick, et al, "European countries enable Iran trade through first INSTEX transaction and Swiss payment mechanism," ***White & Case***, April 3, 2020, https://www.whitecase.com/publications/alert/european-countries-enable-iran-trade-through-first-instex-transaction-and-swiss.
171 Patrick Wintour, "Iran says it would rejoin nuclear deal within an hour of US doing so," ***The Guardian***, December 14, 2020, https://www.theguardian.com/world/2020/dec/14/iran-says-rejoin-nuclear-deal-within-hour-us.
172 Parisa Hafezi, "Iran's Rouhani says "ball in U.S. court" over nuclear dispute," ***Reuters***, January 20, 2021, https://www.reuters.com/article/us-iran-nuclear-usa-idUSKBN29P0NK.
173 "Iran's Rohani gets green light to engage with Biden," ***Argus***, December 16, 2020, https://www.argusmedia.com/en/news/2169574-irans-rohani-gets-green-light-to-engage-with-biden.
174 Reuters Staff, "Iran and China sign 25-year cooperation agreement," ***Reuters***, March 27, 2021, https://www.reuters.com/article/us-iran-china/iran-and-china-sign-25-year-cooperation-agreement-idUSKBN2BJ0AD.
175 John Hardie and Annie Fixler, "Russia-Iran cooperation poses challenges for US cyber strategy, global norms," ***C4ISRNET***, February 8, 2021, https://www.c4isrnet.com/thought-leadership/2021/02/08/russia-iran-cooperation-poses-challenges-for-us-cyber-strategy-global-norms/.
176 Supported by the interview with Michael Daniel on March 17, 2021.
177 "Islamic Republic of Iran," ***The World Ban***k, https://www.worldbank.org/en/country/iran/overview#:~:text=Gross%20Domestic%20Product%20(GDP)%20has,population%20of%20about%2084%20million.
178 Maryam Sinaiee, "International Monetary Fund Projects 2.5% Iranian Growth In 2021," ***Iran International,*** April 7, 2021, https://iranintl.com/en/iran/international-monetary-fund-projects-25-iranian-growth-2021#:~:text=In%20its%20latest%20World%20Economic,2.5%20percent%20growth%20in%202021.
179 "Real GDP Growth," ***International Monetary Fund***, https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD.
180 Assumes a ~42,000 IRR: 1 USD exchange rate applied to a IRR 1,838,360 billion 2019 government revenue figure via https://tradingeconomics.

com/iran/government-revenues.
181 "Annual Threat Assessment of the US Intelligence Community," 15-16.
182 "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," ***US Department of Justice***.
183 "What is WannaCry ransomware?" ***Kaspersky***, https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.
184 Reuters Staff, "Cyber attack hits 200,000 in at least 150 countries: Europol," Reuters, May 17, 2007, https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX.
185 Supported by interviews with Michael Daniel; Sanaz Yashar; JD Work; Intelligence Community Official; Private Sector Researcher #1; and Private Sector Researcher #2.
186 Supported by interviews with Sanaz Yashar; Luke McNamara; Private Sector Researcher #1; and Private Sector Researcher #2.
187 "US is prepared to lift sanctions inconsistent with Iran nuclear deal: State Dep," ***Alarabiya News***, April 7, 2021 https://english.alarabiya.net/News/world/2021/04/08/US-is-prepared-to-lift-sanctions-on-Iran-State-Department.
188 Supported by the interview with Sanaz Yashar on April 6, 2021.
189 Stats Appendix File, Page 22, Table 21, "Regional Economic Outlook: Arising from the Pandemic: Building Forward Better," ***Middle East and Central Asia, International Monetary Fund,*** April 2021, https://www.imf.org/en/Publications/REO/MECA/Issues/2021/04/11/regional-economic-outlook-middle-east-central-asia.
190 See Appendix C for more information.
191 "Iranians Charged with Hacking U.S. Financial Sector," Federal Bureau of Investigation, March 24, 2016, https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.
192 See Appendix C for more detailed information regarding the Mabna spear-fishing campaign.
193 Tanzeel Akhtar, "Iran Should Mine Crypto to Skirt Sanctions, Says President-Linked Think Tank," ***CoinDesk***, March 3, 2021, https://www.coindesk.com/iran-should-mine-crypto-to-skirt-sanctions-says-president-linked-think-tank.
194 Alijani Ershad, "In Iran, Power Outages Reveal the Secret Business of Chinese Bitcoin Farms," The Observers, ***France 24***, February 1, 2021, https://observers.france24.com/en/middle-east/20210203-in-iran-power-outages-reveal-the-secret-business-of-chinese-bitcoin-farms.
195 Kevin Helms, "Iran's New Crypto Law Requires Miners to Sell Bitcoin Directly to Central Bank to Fund Imports – Regulation Bitcoin News," ***Bitcoin News***, October 29, 2020, https://news.bitcoin.com/iran-crypto-law-miners-bitcoin-central-bank/.
196 Haniyeh Sadat Jafariyeh, "Iran to Join National Crypto Owners Soon." ***Mehr News Agency***, April 10, 2021, https://en.mehrnews.com/news/171812/Iran-to-join-national-crypto-owners-soon.
197 "Bitcoin Mining Map," Cambridge Bitcoin Electricity Consumption Index (CBECI), University of Cambridge, April 2020, https://cbeci.org/mining_map.
198 "Mining Calculator Bitcoin, Ethereum, Litecoin, Dash and Monero." CryptoCompare, 2020, https://www.cryptocompare.com/mining/calculator/btc?HashingPower=95&HashingUnit=TH%2Fs&PowerConsumption=1500&CostPerkWh=0&MiningPoolFee=0.
199 Yaya Fanusie and Trevor Logan, "Crypto Rogues U.S. State Adversaries Seeking Blockchain Sanctions Resistance," Foundation for Defense of Democracies, July 2019, https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf.
200 "Multiple CBDC (MCBDC) Bridge," Bank for International Settlements, April 8, 2021, https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.
201 "Iranian Cryptocurrency's Features Revealed," IBENA News Agency, August 27, 2018, http://en.ibena.ir/news/90482/Iranian-Cryptocurrency-s-Features-Revealed.
202 Osato Avan-Nomayo, "Iran Developing National Blockchain Platform on Hyperledger Fabric," Cointelegraph, May 28, 2019, https://cointelegraph.com/news/iran-developing-national-blockchain-platform-on-ibm-hyperledger-fabric.
203 "The Minister of Information and Communications Technology said that so far, four to five Cryptocurrency test models have been implemented and decision making in this area for their activities with the central bank," 8th Annual Conference on Electronic Banking and & Payment Systems: Blockchain Revolution, January 29-30, 2019, http://conf.mbri.ac.ir/ebps8/Mobile/News_en/294135.
204 Ryan Grace, "Shatter the Web: Internet Fragmentation in Iran," Middle East Institute, December 14, 2020, https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran.
205 "Iran: Tightening the Net 2020," Article 19, September 19, 2020, 23, https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf.
206 Maziar Motamedi, "Iranians Fear a Permanent Internet Blackout Is in the Making," The Atlantic Council, December 12, 2019, https://www.atlanticcouncil.org/blogs/iransource/iranians-fear-a-permanent-internet-blackout-is-in-the-making/.
207 "Treasury Designates Iran's Minister of Information and Communications Technology in View of the Regime's Repressive Internet Censorship," US Department of the Treasury, November 22, 2019, https://home.treasury.gov/news/press-releases/sm836.
208 "Treasury Designates Iran's Minister of Information and Communications Technology in View of the Regime's Repressive Internet Censorship,"
209 Richard Nephew has since become the Deputy US Special Envoy for Iran in the Department of State but was not interviewed in this capacity.
210 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," ***US Department of Justice***, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.
211 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," ***US Department of Justice***.
212 Dustin Volz and Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," ***Reuters***, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.
213 "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," ***US Department of Justice***, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

214 "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," ***US Department of Justice.***
215 "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," ***US Department of Treasury***, November 28, 2018, https://home.treasury.gov/news/press-releases/sm556.
216 "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," ***US Department of Justice***.
217 "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," ***US Department of Treasury***.
218 Irit Avissar and Naomi Zoreff, "Shirbit hack serves as a wakeup call to every financial company," ***CTECH***, December 6, 2020, https://www.calcalistech.com/ctech/articles/0,7340,L-3879492,00.html.
219 Supported by interviews with JD Work; and Private Sector Researcher 1.
220 Ionut Arghire, "Iranian Hackers Target Israeli Companies With Pay2Key Ransomware," ***SecurityWeek***, December 20, 2020, https://www.securityweek.com/iranian-hackers-target-israeli-companies-pay2key-ransomware.
221 "Ransomware Alert: Pay2Key," ***Check Point Research***, November 6, 2020, https://research.checkpoint.com/2020/ransomware-alert-pay2key/.
222 Supported by interviews with JD Work; and Private Sector Researcher 1.
223 Charles Arthur, "Twitter Hack by 'Iranian Cyber Army' Is Really Just Misdirection," ***The Guardian***, December 18, 2009, https://www.theguardian.com/technology/blog/2009/dec/18/twitter-hack-iranian-cyber-army-dns-mowjcamp.
224 Anderson and Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," 52.
225 Gregg Keizer, "Hackers spied on 300,000 Iranians using fake Google certificate," ***Computerworld***, September 6, 2011, https://www.computerworld.com/article/2510951/hackers-spied-on-300-000-iranians-using-fake-google-certificate.html.
226 "Compromise of Saudi Aramco and RasGas," ***Council on Foreign Relations***, August 2012, https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas.
227John Worrall, "Shamoon Attack Reinforces Risks of Privileged Credential Compromise," ***CyberArk***, December 6, 2016, https://www.cyberark.com/resources/blog/shamoon-attack-reinforces-risks-of-privileged-credential-compromise.
228 "Iran blamed for Parliament cyber-attack," ***BBC***, October 14, 2017, https://www.bbc.com/news/uk-41622903.
229 Francis Elliot, "Iran attacks 9,000 email accounts in parliament," ***The Times***, October 14, 2017, https://www.thetimes.co.uk/article/iran-attacks-9-000-email-accounts-in-parliament-w5mr836cg?region=global&--xx-meta=denied_for_visit%3D0%26visit_number%3D0%26visit_remaining%3D0%26visit_used%3D0&--xx-mvt-opted-out=false&--xx-uuid=8659d09fdad8030eaedb968ab5efc1a0&ni-statuscode=acsaz-307.
230 Stephen Jewkes and Kim Finkle, "Shamoon computer virus variant is lead suspect in hack on oil firm Saipem," ***Reuters***, December 12, 2018, https://www.reuters.com/article/cyber-shamoon/shamoon-computer-virus-variant-is-lead-suspect-in-hack-on-oil-firm-saipem-idINL1N1YH0QC.
231Joseph Menn, Christopher Bing, Raphael Satter, and Jack Stubbs, "Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources," ***Reuters***, April 2, 2021, https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target- who-staff-emails-during-c oronavirus-sources-idUSKBN21K1RC.
232 Sean Lyngaas, "'Greenbug' hacking group hits three telecom firms in Pakistan," ***CyberScoop***, May 19, 2020, https://www.cyberscoop.com/greenbug-symantec-iran-hacking-pakistan/.
233 Threat Hunter Team, "Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia," ***Symantec***, May 19, 2020, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia.
234 Threat Hunter Team, "Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia," ***Symantec***.
235 Ronen Bergman and David M. Halbfinger, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks," ***The New York Times***, May 19, 2020, https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyber attacks.html.
236 Catalin Cimpanu, "Two more cyber-attacks hit Israel's water system," ***ZDNet***, July 20, 2020, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/..
237 Farnaz Fassihi, "Burning Ships in Iran Add to String of Dozens of Explosions and Fires," ***The New York Times***, July 15, 2020, https://www.nytimes.com/2020/07/15/world/middleeast/iran-ships-fire-explosions.html.
238 Tom Burt, "Recent cyber attacks Require Us All to Be Vigilant," ***Microsoft***, October 4, 2019, https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyber attacks-require-us-all-to-be-vigilant/.
239 Burt, "Recent cyber attacks Require Us All to Be Vigilant," ***Microsoft***.
240 Burt, "Recent cyber attacks Require Us All to Be Vigilant," ***Microsoft***.
241 "Foreign Threats to the 2020 US Federal Elections," ***National Intelligence Council***, March 16, 2021, 6, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
242"Foreign Threats to the 2020 US Federal Elections," ***National Intelligence Council***, 6.
243 "Joint CISA-FBI Statement: Iranian APT Actors Obtained Voter Registration Data," ***Federal Bureau of Investigation***, October 21, 2020, https://www.fbi.gov/news/pressrel/press-releases/joint-cisa-fbi-statement-iranian-apt-actors-obtained-voter-registration-data-.
244 Gage Mele, Winston Marydasan, and Yury Polozov, "Probable Iranian Cyber Actors, Static Kitten, Conducting Cyberespionage Campaign Targeting UAE and Kuwait Government Agencies," ***Anomali***, February 10, 2021, https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign -targeting-uae-and-kuw ait-government-agencies.
245 Chang Woo Kim and Carolina Polita, "The Evolution of North Korean Cyber Threats," ***Asan Institute for Policy Studies***, February 20, 2019, pp. 2, http://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/.
246 Kim and Polita, "The Evolution of North Korean Cyber Threats," 2-3.
247 Kim and Polita, "The Evolution of North Korean Cyber Threats," 3.

248 Kim and Polita, "The Evolution of North Korean Cyber Threats," 3.
249 Ben Buchanan, "How North Korean Hackers Rob Banks Around the World," ***WIRED***, February 28, 2020, https://www.wired.com/story/how-north-korea-robs-banks-around-world/.
250 Ben Buchanan, "How North Korean Hackers Rob Banks Around the World," ***WIRED***.
251 "Guidance on the North Korean Cyber Threat," ***Cybersecurity and Infrastructure Security Agency***, April 15, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-106a.
252 Symantec Security Response Team, "What You Need to Know about the WannaCry Ransomware," ***Broadcom***, October 23, 2017, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack.
253 Symantec Security Response Team, "What You Need to Know about the WannaCry Ransomware," ***Broadcom***.
254 "Guidance on the North Korean Cyber Threat," ***Cybersecurity and Infrastructure Security Agency***.
255 "Guidance on the North Korean Cyber Threat," ***Cybersecurity and Infrastructure Security Agency***.
256 Amy Castor, "After Second Hack This Year, South Korean Exchange YouBit Closes Down," ***Bitcoin Magazine***, December 19, 2017, https://bitcoinmagazine.com/culture/after-second-hack-year-south-korean-exchange-youbit-closes-down.
257 Kim and Polita, "The Evolution of North Korean Cyber Threats," 5.
258 Kim and Polita, "The Evolution of North Korean Cyber Threats," 5.
259 Kim and Polita, "The Evolution of North Korean Cyber Threats," 5.
260 "The 2021 Crypto Crime Report," ***Chainalysis***, February 16, 2021, 82, https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.
261 Kim and Polita, "The Evolution of North Korean Cyber Threats," 5.
262 "The 2021 Crypto Crime Report," ***Chainalysis***, 5.
263 "The 2021 Crypto Crime Report," ***Chainalysis***, 82.
264 "The 2021 Crypto Crime Report," ***Chainalysis***, 4.
265 "The 2021 Crypto Crime Report," ***Chainalysis***, 4.
266 "The 2021 Crypto Crime Report," ***Chainalysis***, 4.
267 "The 2021 Crypto Crime Report," Chainalysis, 4.
268 Stephan Haggard and Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace," ***East-West Center***, no. 117, May 2015, 2, https://www.eastwestcenter.org/system/tdf/private/api117.pdf?file=1&type=node&id=35164.
269 Haggard and Lindsay, "North Korea and the Sony Hack," 2.
270 Kim and Polita, "The Evolution of North Korean Cyber Threats," 8.
271 Haggard and Lindsay, "North Korea and the Sony Hack," 2.
272 "Foreign Threats to the 2020 US Federal Elections," ***National Intelligence Council***, 6.
273 Alyza Sebenius, Kartikay Mehrotra, and William Turton, "Iran's Cyber Attack on Billionaire Adelson Provides Lesson on Strategy," ***Claims Journal***, January 6, 2020, https://www.claimsjournal.com/news/national/2020/01/06/294849.htm.

COLUMBIA UNIVERSITY | SIPA — CAPSTONE REPORT
Published in April 2021