FULCRUM GLOBAL

The publishing arm of the Society for Defense and Strategic Studies (SDSS)
at American Military University (APUS)

INTELLIGENCE BRIEF #8

NAME OF PRIMARY ANALYST: Dustin Oaks

SUBJECT: Iranian Relations, Cyberwar, and Trade deals with China

COUNTRY/REGION: Iran

BACKGROUND OF SUBJECT:

The U.S. reinstatement of the Iran nuclear ban has resulted in renewed hostilities in U.S.-Iranian relations. This has resulted in Iran taking a systematic course of action against the United States and allies in defiance of the West, and this has great implications on the oil Industry and the trade agreements with China.

CUSTOMER QUESTIONS:

1. Can Iran sustain a cyber war with the United States?
2. Is Iran seeking a negotiation similar to North Korea in terms of threatening nuclear attacks and attacking American Troops in the region?
    a. Economic assistance needed?
3. Can Iran survive sanctions?
4. Can Iran form a blockade in the Strait of Hormuz and would the U.S. survive it?
    a. Economic Impact on the oil Industry?
5. How will enhanced conflict between the U.S. and Iran impact China's strategic interests and the ongoing U.S.-China trade war dispute?

CURRENT ASSESSMENT:

Iran's Cyber Operations

The Stuxnet malware/virus that attacked the internal network of the Iranian Natanz nuclear reactor plant resulted in an upgraded policy shift that initiated a targeted cyberwarfare offensive strategy that was focused on the U.S. and other members of the international community. The Iranians began their cyber operations in 2011 by compromising certificates of

Comodo and DigiNotar. The next stage of their cyberwarfare offensive known as Operation Cleaver targeted the critical infrastructures of sixteen nations. The United States was the most heavily targeted nation as the following industries were highly emphasized: airlines; education; chemicals; transportation; energy and utilities; military and government; and the defense industrial base.[1]

A new cyber threat group called the Advanced Persistent Threat (APT)-33, 34 and APT39 came after the Cleaver team by targeting and exploiting the networks of multiple organizations. APT33 (Elfin) became active around late 2015 to early 2016 and attacked over 50 organizations between Saudi Arabia, United States, and various other countries.[2] This group specializes in scanning website vulnerabilities and exposing them for potential targets to either attack, or create, command and control (C&C) infrastructure. Targets include governments and organizations tied to research, chemicals, engineering, manufacturing, consulting, finance, telecoms, and several other sectors. They have also targeted Saudi Arabia 42% of the time and the United States 34% of the time between 2016 and 2019. The U.S. attacks are mostly centered on supply chain operations interference.

APT34 is an Iran-nexus cluster responsible for cyber espionage and is reportedly active since 2014. The group utilizes both public and non-public tools in order to collect strategic information beneficial to nation-state interests that pertain to geopolitical and economic needs.[3] The group is known to target decision makers and key organizations that they feel capable of furthering Iran's economic and national security goals. It is believed that the organization's interest lay in gaining access to financial, energy, and government entities.

APT39 is an Iranian cyber espionage group that is responsible for the widespread theft of personal information, which is also linked to influence operations and disruptive attacks, since 2014.[4] This group focuses on the personal information in order to support the monitoring, tracking, and even surveillance operations that better serve Iran's national priorities, or potentially create additional accesses and vectors to facilitate future campaigns. Their original focus was on the telecommunications and travel industries which aligns with the surveillance and monitoring of specified individuals in order to potentially collect proprietary or customer data. This is for either commercial, or operational purposes, of strategic requirements for the national priorities as well as developing future vectors for campaigns. The groups targeting of government entities and personnel shows its intent to exploit and steal geopolitical data that may benefit decision-makers within nation-states.

Adopting North Korea's Nuclear Negotiation Tactics

Iran's stance on enriching uranium and building nuclear weapons is the same one that the North Korean government has utilized for several years. The Democratic People's Republic of Korea (DPRK) for decades has continued to threaten both the South Korean and United States governments with nuclear attacks if certain demands were not met. Over the years, different delegations attempted to meet with the reluctant leadership until the current leaders were able to generate a dialogue and initiate serious negotiations. The Iranian regime has been

at odds with the United States since the Iranian Revolution in 1979 that resulted in the capture of the U.S. embassy in Tehran. Iran's current government is taking actions that mimic the DPRK's in an attempt to maintain a dominant stance while wanting to negotiate through a rhetoric of threats.

The Joint Comprehensive Plan of Action (JCPOA) Agreement

The Joint Comprehensive Plan of Action (JCPOA), enforced by the United Nations Security Council was enacted on January 16, 2016. The plan was agreed by the U.S., United Kingdom, France, Russia, China, and Germany (P5+1) and it discussed the constraints needed to ensure that Iran's nuclear program can be utilized for purely peaceful purposes in exchange for lifting the broad sanctions of the U.S. and European Union (EU) and United Nations (UN).[5] The issues pertaining to this agreement is that it gives Iran additional resources in order to conduct "malign activities" in the region, as well as enabling Iran's ability to develop ballistic missiles. Resolution 2231, adopted in July 2015, only prohibited arms transfers to or from Iran for five years and contains a voluntary restriction on Iran's development of nuclear-capable ballistic missiles for up to eight years.

Iranian Influence in Iraq During the ISIS Campaign

This creates tension in the region and impacts economic growth. The Iranian military and their militias, have fought the Islamic State of Iraq and Syria (ISIS) throughout Western Iraq all the way to the outskirts of Baghdad, has enabled a much stronger Iranian influence deep within Iraqi society, particularly in their military and parliament. This was previously minimized by the U.S. military. Iran's Islamic Revolutionary Guard Corps, also known as the IRGC, is now able to funnel weapons and explosives deep into the country and target political outposts. This enables the Iranian government's capability to influence anti-American militias while creating a staging ground for attacking U.S. interests, as well as forcing the hand of the American negotiating stance.

Decline in Iranian Oil and Economic Performance

Iran's oil production and Gross Domestic Production (GDP) growth are all collapsing, their currency is weakening, and inflation is picking up.[6] Iran has been exploiting loopholes in the sanctions by utilizing domestic "private companies" to act as middlemen and sell oil to normal purchasers such as China. The International Monetary Fund (IMF) forecasts a contraction in the Iranian economy in 2018 of 1.8 percent and then another 3.6 percent throughout 2019, which is a reversal of their prediction of a 4 percent growth over the two year span. Exportation of Iranian oil has fallen from 2.7 million barrels per day (b/d) in June of 2018 to between 1.7 million b/d and 1.9 million b/d in September of the same year. This number is expected to grow as companies do not wish to chance losing access to the business markets in the United States. In addition, the country is experiencing enhanced unemployment levels among younger generations as well as an inflation rate of 31.4 percent in September of 2018. Also, sources indicate that inflation number will continue to increase. To cap this economic

struggle off, the Iranian Rial, has lost over two-thirds of its value in the unofficial market since January 1, 2018. The P5+1 has jointly disapproved with the U.S. sanctions and the withdrawal from the JCPOA and since agreed to develop a special purpose vehicle (SPV) to facilitate trade with Iran and mitigate the sanctions put in place by the United States. This SPV would be a clearing house for the business transactions with Iran in Euros.[7]

Status of Iranian Navy in the Strait of Hormuz

Iran's naval fleet currently consists of 8 Active ship classes for the Islamic Republic of Iran Navy (IRIN) and included is two diesel-powered submarine classes, one replenishment ship (Iranian Kharg 431), 4 Fast Attack Missile Boats Classes with 9 ships in the Sina-class, seven Frigate warships. Within the Kilo-class submarine section, there are 57 submarines that originated in 1982 from the Soviet Union (USSR). The newest commissioned submarines called the Fateh-class (Conqueror-class) have two diesel power submarines in that class.

Given the amount of ships and submarines officially listed in the Iranian Navy and the width of the Strait of Hormuz being between thirty-five to sixty miles wide at the widest part, the Iranian Navy will have no difficulty in controlling access to the Strait of Hormuz where one-third of the world's crude and fuel passes through it.[9] The impact it has on the oil market increases since actions like tankers being attacked or being taken over increases operational costs such as $28,000 per day for chartering the largest class of tankers. Also, insurance premiums for the shipping area rise and as of 2018, operators were charging $50,000 per day.[10]

This does not impact the U.S. as much as expected since it has increased domestic production by seventeen percent last year and natural gas output increased by twelve percent as well. Over the last decade, the U.S. roughly added six million barrels per day of oil, which is an equivalent of combined production between the United Arab Emirates (UAE) and Kuwait. With recent actions in the Strait of Hormuz, crude oil prices have only risen five percent, which is not considered being much of an impact for the United States and other OPEC nations.

Illegal Deals Between Iran and China

Iran's business deals with China in arms deals has fallen from roughly $300 million between 2004 and 2007 to below $50 million between 2008 and 2011.[11] The United States has indicted Chinese Businessman Li Fangwei back in 2013 by the New York County District Attorney. It was reported that he continued to earn in excess of $10 million from illegal sales to Iran since the sanctions were put into effect.[12] The Chinese Foreign Minister's spokeswoman, Hua Chunying, stated that the U.S. measure had "seriously violated the norms of international relations and harms China's interests", and she urged the United States to revoke the "irrational sanctions".

The Chinese telecom firm, Huawei, is at the forefront of the international investigation being conducted by U.S. authorities that are seeking to charge their Chief Financial Officer, Meng Wanzhou, with espionage and violation of sanctions with Iran. Huawei controls Skycom

Tech Co Ltd and another shell company called Canicula Holdings Ltd. The importance of this case is that Huawei has been using Skycom Ltd to shield sales of telecommunications equipment to Iran and Syria. The U.S. investigators found documents that link a high-level Huawei executive as being their Iranian manager. They also list three additional Chinese-named individuals as having the ability to sign on behalf of Huawei and Skycom bank accounts within Iran. These deals all but violate sanctions with Iran and have played a significant role in fueling an escalated cyberwar between the United States, Iran, and China.[13]

ANALYSIS OF ASSESSMENT:

Given the continual progression of the Iranian cyber army and their sophistication of attacks, one should expect to see an increase in spear phishing campaigns and exploitation of government employees and contractors as they move throughout the Middle East. Focus of indications of compromise should be around the defense industry, especially throughout Iraq and Afghanistan. The utilization of newer defense technology is actively tested throughout these two countries, to include sophisticated tracking satellites and unmanned aerial vehicles, both armed and unarmed. The reverse engineering of these technologies has been a constant issue when dealing with Iran and will continue to have an impact on military and geopolitical issues.

Expect more military interference throughout the Strait of Hormuz directly targeting allies of the United States and the United States itself. The Iranian navy paired with Iranian cyber military members can be expected to board ships and implant malware within their ship's electronic systems with the intention of exploiting connection to additional networks at other ports of entries and the host country (i.e. United Kingdom, United States, and Saudi Arabia). As a result, one can expect the P5+1 to continue to mitigate the sanctions with Iran and the continuing business deals with China, both on oil and telecommunications, to better assist the Iranian influencing strategy.

Sanctions on Iran will continue until a deal can be brokered that is beneficial to the United States and ensure the safety of the civilians and interests in the region. This can mimic aid such as with DPRK since the inflation and unemployment rates are increasing with a devalued monetary currency. Until this happens one can expect increased and maintained cyberwarfare with Iranian units and those that sympathize with the regime.

LIST OF SOURCES AND REFERENCES:

1.) "Operation Cleaver." Operation Cleaver. Accessed July 24, 2019. https://www.cylance.com/operation-cleaver.

2.) Security Response Attack Investigation Team. "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S." Symantec. March 27, 2019. Accessed July 24, 2019. https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

3.) Bromiley, Matt. "Hard Pass: Declining APT34's Invite to Join Their Professional Network « Hard Pass: Declining APT34's Invite to Join Their Professional Network." FireEye. July 18, 2019. Accessed July 24, 2019. https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html.

4.) Hawley, Sarah. "APT39: An Iranian Cyber Espionage Group Focused on Personal Information APT39: An Iranian Cyber Espionage Group Focused on Personal Information." FireEye. January 29, 2019. Accessed July 24, 2019. https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html.

5.) Kerr, Paul K., and Kenneth Katzman. Iran Nuclear Agreement and U.S. Exit. Report no. 7-5700/ R43333. Congressional Research Service. July 20, 2018. Accessed July 24, 2019. https://fas.org/sgp/crs/nuke/R43333.pdf.

6.) Segal, Stephanie, and Dylan Gerstel. "The Economic Impact of Iran Sanctions." The Economic Impact of Iran Sanctions | Center for Strategic and International Studies. November 5, 2018. Accessed July 24, 2019. https://www.csis.org/analysis/economic-impact-iran-sanctions.

7.) Segal, Stephanie, and Dylan Gerstel. "The Economic Impact of Iran Sanctions." The Economic Impact of Iran Sanctions | Center for Strategic and International Studies. November 5, 2018. Accessed July 24, 2019. https://www.csis.org/analysis/economic-impact-iran-sanctions.

8.) Military Factor. "Active Iranian Navy Ships (2019)." Military Weapons. Accessed July 24, 2019. https://www.militaryfactory.com/modern-navy/islamic-republic-of-iran-navy.asp.

9.) Davis, Tina. "Iran Says It Doesn't Want to Blockade the Strait of Hormuz." News | Al Jazeera. July 18, 2019. Accessed July 24, 2019. https://www.aljazeera.com/ajimpact/iran-doesn-blockade-strait-hormuz-190717115940801.html.

10.) Reed, Stanley. "The Oil Market Shows It Can Take a Punch." The New York Times. June 21, 2019. Accessed July 24, 2019. https://www.nytimes.com/2019/06/21/business/oil-prices-us-iran.html.

11.) Maclean, William, and Ben Blanchard. "Exclusive: Chinese Trader Accused of Busting Iran Missile Embargo." Reuters. March 01, 2013. Accessed July 19, 2019. https://www.reuters.com/article/us-china-iran-trader/exclusive-chinese-trader-accused-of-busting-iran-missile-embargo-idUSBRE9200BI20130301.

12.) Maclean, William, and Ben Blanchard. "Exclusive: Chinese Trader Accused of Busting Iran Missile Embargo." Reuters. March 01, 2013. Accessed July 19, 2019. https://www.reuters.com/article/us-china-iran-trader/exclusive-chinese-trader-accused-of-busting-iran-missile-embargo-idUSBRE9200BI20130301.

13.) Stecklow, Steve. "Exclusive: New Documents Link Huawei to Suspected Front Companies..." Reuters. January 09, 2019. Accessed July 24, 2019. https://www.reuters.com/article/us-huawei-iran-exclusive/exclusive-new-documents-link-huawei-to-suspected-front-companies-in-iran-syria-idUSKCN1P21MH

FINAL DATE OF ANALYSIS AND SUBMISSION:
December 10, 2019

EDITING TEAM:
Sam Kessler - Chief and Managing Editor
Lorinda Rosario - Senior Editor

PEER REVIEW TEAM:
Cameron Grischott
Ron Brooks
Brian Moody
Allen Cline
Alyssa LeVasseur

WEBSITE:
www.fulcrumglobal.us

SOCIAL MEDIA PAGES:
Fulcrum Global Facebook: https://www.facebook.com/Fulcrum-Global-1398490850246444/
SDSS Facebook: https://www.facebook.com/groups/APUS.SDSS/
SDSS Twitter: https://twitter.com/sdss_apus
SDSS LinkedIn: https://www.linkedin.com/in/society-for-defense-and-strategic-studies-022182196/