FLASHPOINT

Intelligence Report

Geopolitical Iranian/Russian Overlap (Analyst Knowledge Page)

June 10, 2020

EXECUTIVE SUMMARY

Russia and Iran are economic partners, likely as a result of Western sanctions and geographic proximity. As a strong global power, Russia has provided Iran with military weaponry and nuclear material and technology.

This exchange continues into state-sponsored cyber operations, where Russia offers training and guidance for Iran's growing cyber program. Analysts have noted overlap of Russian TTPs within Iranian cyber campaigns, but a definitive link has not been established of official collaboration on cyber operations. Iran adopted Russia's tactic of creating one group of "fake" actors that then "friend" a second group of fake actors on social media to build legitimacy for their personas used for social engineering, spearphishing, etc. There are also unsubstantiated claims that the "Internet Research Agency" created some of the fake Iranian personas used in Kitten operations, but this is dubious as Iran maintains its own capability to develop online personas.

As authoritarian regimes, Iran and Russia strive to control their populations and quell dissent through information control. One step both nations are taking toward this goal is the development of national internets separated from the global domain name system.
The exact details and extent of Iran and Russia's collaboration in state-sponsored cyber operations is unknown. However, analysts assess with moderate confidence that based on overlap of infrastructure and TTPs, there is a nonadversarial and collaborative relationship between the two countries.

Furthermore, Iran and Russia cooperate closely on other issues, such as military weaponry, nuclear technology, and population control.

June 10, 2020, Updates:

General Collaboration

Cyber Collaboration

Collaboration and Exchanges in Other Domains

IRAN AND RUSSIA: GENERAL COLLABORATION

BACKGROUND AND GEOPOLITICS

[back to top]

Russia and Iran are economic partners, likely as a result of Western sanctions and geographic proximity, a relationship that dates back to the era of the USSR. Additionally, it is likely that Iran and Russia have united on similar goals, like a perceived adversarial relationship with the West as a result of economics, politics, and military operations.

Iran and Russia also share independent goals of greater inclusion on the world stage, which would involve greater defense resources. [1, 2] As recently as 2016 at the St. Petersburg economic forum, Vladimir Putin said the United States was “the only remaining superpower.” Russia is generally regarded as a major global player, but not a superpower; Putin’s intention as leader is to restore Russia to a superpower status. [3, 4] Russia effectively leverages its current influence via:

- As a permanent member of the UN Security Council
- Playing important roles in European and Middle Eastern affairs, relationships, and geopolitics
- Shaping the Syrian conflict, aiding Bashar al Assad and his supporters

However, Russia is limited in its superpower aspiration due to its limited defense resources and an underwhelming economy.

Iran comes from a position of isolation as Western governments unite against the country. In the past, Russia provided Iran with physical weaponry and played an integral part in its nuclear activities, and Russia has recently expanded into providing technological exchanges with Iran. Russia continues to value the Iranian alliance as issues concerning Syria, cyber, and the Islamic State (ISIS) unite the two countries. Due to Russia’s proximity to Iran, Moscow has a vested interest in the economics and politics of Tehran.

The multiple crises in the Middle East, civilian uprisings, and a desire to push back the US presence in the region provide the perfect platform for intensified cooperation between Russia and Iran. In the near term, Syria will likely remain the crux of their relations, but there are other regional issues upon which they could unite. Demonstrating a continued allegiance with Iran, on October 2, 2019, Russian President Vladimir Putin publicly denounced claims that Iran was responsible for a September attack on Saudi oil infrastructure. Putin’s comments occurred alongside a meeting between Russia and Iran on the nuclear deal and activities in the Strait of Hormuz. As brazen cyber actors who aren’t afraid to leave evidence of their malicious cyber activities behind, and considering the pseudo-anonymity it provides, cyber collaboration will likely continue to play a role in this evolving partnership.

IDEOLOGY

[back to top]

Despite religious and cultural differences, the Russian and Iranian approaches to controlling what they view as subversive subcultures or threats to their regimes unite the two countries. Perceived threats include: LGBTQ+ rights, media, open internet access, western culture.

While former autocratic governments of Egypt, Iraq, and Syria did not successfully quash internal rebellions and civil uprisings, Russia observes that Iran is relatively strong domestically, as it controlled the 2009 “Green Movement” uprisings and punished participants. To Russia, Iran appears as a functioning state that can advance Russian interests, as both regimes share the desire to control their population and prevent any anti-government message.

RUSSIA AND ISLAM

[back to top]

Russia has had a long and complex relationship with Islam as a religion, as well as its role in Russian foreign policy and politics. Following the collapse of the USSR, Islam became associated with separatism and terrorism in Russia due to the Chechen wars. The North Caucasus remains a hotbed of religious extremism, and Sunni jihadism and separatism have remained heavily associated with Islam in Russia's security apparatus. Before the 2014 Winter Olympics held in the Southern Russian city of Sochi, Russia passively encouraged religious extremists to leave the country for Syria in order to reduce the chances of an attack on the games. According to different estimates, at least 1,500 Russian nationals left by 2015. [5]

Russian foreign policy both before and after the collapse of the USSR has been primarily security-focused and thus maintained a commitment to "legitimise" (preference of supporting incumbent leaders over the opposition). This general principle still guides Russia's interaction with Muslim countries e.g. in the Middle East, hence the Russian government's stark opposition to the Arab Spring. Both the general opposition to the notion of the Arab Spring and the more specific opposition to the toppling of Syria's president Bashar al-Assad were conducive to a deepening of Iran-Russia security cooperation. Russia's relationship with Saudi Arabia, which has recently improved on the heels of sustained cooperation on oil markets and negotiations on Russian arms sales has a security component as well: while the relationship is cordial, the Russian government expects Saudi Arabia not to support radical Islamism in Russia. Chechen president Kadyrov's attempts to build a strong relationship with Saudi Arabia supports this interpretation.

ISLAM AND RUSSIA'S FOREIGN POLICY

[back to top]

The Soviet government was the first to recognize the Islamic Republic of Iran in 1979—with the intention of putting pressure on the United States—but the relationship remained subdued due to the Iranian leadership's opposition to atheism. In the Iraq-Iran war of 1988 the USSR supported Iraq with arms sales. The Russia-Iran relationship improved notably after the fall of the USSR as Iran and Russia signed an agreement on the construction of the Bushehr nuclear power plant in 1995 and Russia started selling weapons and military equipment to Iran. The relationship never focused on matters of religion, due to the relatively small number of Shia Muslims in Russia, most of whom belong to the Azerbaijani nationality, a sizable minority in Iran. Russia does, however, regard Iran as an important and long-term partner in fighting Sunni jihadism, separatism and American imperialism.

Scholars and experts who study Russia believe that this atheistic state aligns itself with Islamic countries for several reasons:

- One is to show its Muslim population that it is tolerant of their religion. There are only estimates of the Muslim population of Russia. In 2017, a survey by Pew Research claimed that 10 percent of the country's population practiced Islam. [6] Russia's total population was then around 140 million. According to the Kazan-based Muslim information site Islam Today, there are approximately 8,000 mosques and 80 Muslim religious schools. [7]
- Another is to show the predominantly Islamic Middle East, where Russia has a large role, that it is tolerant of Islam as well. [8, 9]

Flashpoint's Analyst Knowledge Page on Russia and Islam can be found here.

"Iranians," a Russian-language Telegram channel sharing Shia Muslim religious content, is available here.

PHYSICAL AND NUCLEAR MATERIALS

[back to top]

Historically, Russia has provided Iran with:

- T-72 tanks
- Air-to-air missiles
- MiG-29 aircraft
- Surface-to-air missile defense system (SA-15 Gauntlet)
- TOR M-1 air-defense missile systems

Moscow also upgraded Tehran's Su-24, MiG-29 aircraft, and T-72 battle tanks.

In the context of US-Iran tensions in January 2020 and the Iranian air defense's downing of a Ukrainian civil airplane near Tehran on January 8, Ukrainian defense and security commentators Yury Kolesnikov and Oleg Katkov claimed that Russia had an interest in Iran's downing of the plane and that it had the means to remotely control the Tor air defense equipment that shot down the plane. Kolesnikov said that Russia had both infiltrated Iran's Islamic Revolutionary Guard Corps (IRGC) and had the means to remotely interfere with the system that launched missiles at the plane. Katkov said Russia had considered servicing Tor equipment in Iran in 2015. This has not been confirmed by evidence. [10]

IRAN AND RUSSIA: CYBER COLLABORATION

ORIGIN OF CYBER COLLABORATION

[back to top]

Origins of the Iranian and Russian cyber overlap date back to 2009–10, when the "Iranian Cyber Army"—an Iranian hacker group thought to be sponsored by the Iranian state—purportedly paid Russian and Chinese hackers to perform targeted attacks because they had not yet acquired the capabilities. In 2015, the cyber defense system controlled by the Islamic Revolutionary Guard Corps (IRGC) became operational in Iran; it had been developed with Chinese and Russian assistance.

Analysts assess with moderate confidence that Russia has developed into a global cyber power, which likely has attracted Iran's interest. Analysts assess with high confidence that Iran aims to learn from and emulate Russian cyber capabilities in order to boost its own capabilities in cyberspace.

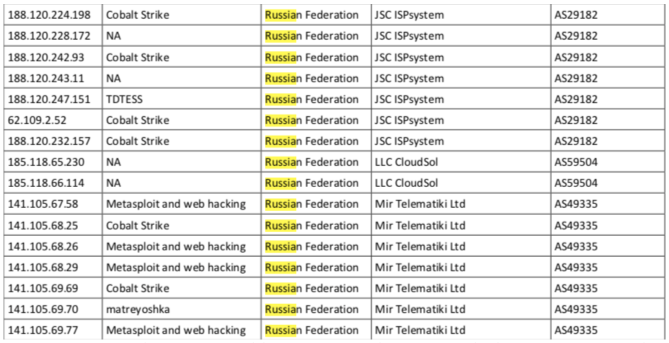
CURRENT CYBER COLLABORATION

[back to top]

Present-day evaluations and thorough study and comparison of the advanced persistent threat (APT) landscape reveal that the Iranian and Russian cyber programs clearly share common tactics, techniques, and procedures (TTPs). These include:

- Extensive social engineering campaigns on LinkedIn, Facebook, and Instagram
- Extensive spear-phishing campaigns
    - APT29/Cozy Bear
    - APT33/Refined Kitten
- Credential harvesting via spoofed websites
    - APT28/FancyBear
    - APT35/Charming Kitten

In October 2017, Iranian collective "Copy Kittens" used several Russian IP addresses in spear-phishing operations. [11] While this does not necessarily indicate conscious cooperation between Iran and Russia, it is worth noting the overlap. Iran frequently uses international infrastructure for its operations in order to obfuscate its activity, but it usually prefers European infrastructure—such as Dutch, German, or French—due to its availability. [12]



188.120.224.198	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.228.172	NA	Russian Federation	JSC ISPsystem	AS29182
188.120.242.93	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.243.11	NA	Russian Federation	JSC ISPsystem	AS29182
188.120.247.151	TDTESS	Russian Federation	JSC ISPsystem	AS29182
62.109.2.52	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.232.157	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
185.118.65.230	NA	Russian Federation	LLC CloudSol	AS59504
185.118.66.114	NA	Russian Federation	LLC CloudSol	AS59504
141.105.67.58	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.25	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.26	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.29	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.69	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.70	matreyoshka	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.77	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335

Image 1: An example of Copy Kitten's use of Russian IP addresses to conduct spear-phishing operation "Wilted Tulip." *(Source: ClearSky)*

In December 2017, the Triton/Trisis malware was used on an attack on the Petro Rabigh refinery in Saudi Arabia. Iran was suspected of carrying out this attack, partially because Iran has previously targeted Saudi Arabia with cyberattacks such as Shamoon. However, in December 2018, FireEye linked Triton to a lab at the Central Scientific Research Institute of Chemistry and Mechanics in Russia. [13, 14] This could indicate that the malware was developed by Russia and used by Iran, demonstrating further cyber cooperation between the nations.

In May 2020 the United Kingdom's National Cyber Security Centre accused both Russian and Iranian groups of targeting research institutions working on COVID-19 vaccine development. However, it was unclear whether the groups cooperated with each other. [15]

APT34 BACKGROUND INFORMATION AND RUSSIAN OVERLAP

[back to top]

The aforementioned Triton/Trisis malware was linked to Iranian APT34. Further possible overlap between APT34 and Russia surfaced in October 2019, when dozens of countries released advisories indicating overlap between Russian and Iranian state-sponsored hacking groups. The United Kingdom's National Cyber Security Centre (NCSC), together with the US National Security Agency (NSA), published an advisory warning that military establishments, government departments, scientific organizations, and universities were among the victims of an ongoing hacking campaign undertaken by "Turla."

Turla Group (also known as "Waterbug" or "Venomous Bear"), likely Russia-based, has been known to use Neuron and Nautilus implants and an ASP-based backdoor alongside the "Snake" rootkit. These tools are suspected to be Iranian in origin, with Russia aiming to identify and exploit them to further their own aims as part of a false-flag operation.

Turla is an APT, meaning its members have state backing and thus additional resources—which makes them more dangerous. The agencies believe Turla acquired access to these tools and then tested them on victims that were already compromised via the Snake rootkit. With APTs exploiting tools previously associated with other APTs, it is critical that organizations give the highest priority to mitigations and patches for vulnerabilities and destructive malware.

This incident further shows Iranian and Russian collaboration in state-sponsored cyber operations, albeit in this instance the extent of Iran's cooperation is unknown.

CRYPTOCURRENCY

[back to top]

Peyman, the domestic Iranian cryptocurrency, became available in January 2019 and is backed by four Iranian banks—Bank Pasargad, Bank Melli Iran, Parsian Bank, and Bank Mellat. Additional reports noted that the currency would be backed by gold, a shift from 2018 reports that it would be backed by the Iranian rial.

In light of Iran's exclusion from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), and its creation of a blockchain in partnership with Russia and Armenia, financial journalists hypothesized that Peyman could facilitate Iranian access to global markets. These journalists suggested that Peyman, unlike SWIFT, could remain unaffected by US sanctions. Though cryptocurrency is not necessarily related to cybercrime or state-sponsored cyber operations, Iran is likely working with Russia as a collaborative partner on new—and possibly legitimate—technologies.

PROXY COMPANIES

[back to top]

The Iranian and Russian governments frequently use proxy companies to evade sanctions, engage international partners at lower risk, and move money covertly. Furthermore, there are few, if any, freely operating cybersecurity companies within Iran or Russia. The authoritarian governments keep information about companies, operating procedures, and infrastructure held very closely. Through open platforms such as LinkedIn, GitHub, and Twitter, names, employees, and details of companies have emerged.

On July 13, 2019, Russian Federal Security Service (FSB) contractor and proxy company SyTech was breached when a group known as "0v1ru$" accessed SyTech's active directory server and defaced the website. SyTech lost 7.5 TB of data. So far, an archive with 169 MB of data has been made available to the public.

Actors then passed the information to another group of cyber threat actors, "Digital Revolution," who shared it with media outlets. Several Russian government projects were revealed and detailed by the international media. Researchers and media have called this breach one of the biggest in Russian history. **"Digital Revolution" also exposed another batch of leaked documents about FSB-sponsored projects in March 2020. These suggested that the FSB was seeking to acquire capabilities to turn infected Internet-of-Things devices into botnets.**

SEGMENTED NATIONAL INTERNETS

[back to top]

Both Russia and Iran have initiated projects to build segmented internets separate from the global domain name systems. This is likely intended as a method to control information, and possibly to protect communications in the event of a large-scale cyberattack. Few details are available about the status of Iran's attempt to build a sovereign internet. However, it is likely that this internet would be an attempt for Iran to gain more control than they have using their current National Information Network (NIN) (aka "halal" internet).

On November 1, 2019, Russia's law on "internet sovereignty" went into effect. The law, signed by Putin in May 2019, will attempt to create an alternative domain name system and strengthen overall control of the country's external access points. It also aims to isolate the country's internet architecture—commonly known as Runet—from the rest of the world.

Flashpoint analysts assess with high confidence that Russia and Iran will likely continue to push for control over their citizens' internet usage, and will likely continue to exclude and block international services that do not comply with requests to divulge users' communications and/or host content locally. Analysts further assess with moderate confidence that other countries may draw inspiration from Iran and Russia and follow in their footsteps.

COLLABORATION AND EXCHANGES IN OTHER DOMAINS

SYRIA

[back to top]

In spite of their coordinated support to Syrian President Bashar al-Assad, Russia and Iran are only allies of convenience in Syria. Russia's interference in the Syrian civil war was arguably prompted by fears that Iran would gain too much influence over a key Russian ally in the Middle East. In early 2020, when Iran's position seemed to weaken following the killing of Qassem Soleimani, Putin took an unannounced trip to Damascus, presumably to strengthen his government's position. The dominant view in the Russian security establishment currently seems to be that while Russian and Iranian interests in the Middle East may not always align, Russia cannot guarantee its own interests without taking Iran's into account.

Additionally, Russia must continuously balance its Israeli and Turkish relationships to augment its position in Syria. This is difficult as Iran and Israel are ardent enemies, and have even come into direct confrontation in Syria. In 2018, Russia helped negotiate keeping Iranian proxies away from the Israeli/Syrian border while Israel stopped air raids against Iranian positions that did not directly threaten Israeli security. When both sides of this agreement were violated, Russia threatened Iran with withdrawing Russian air support, and threatened Israel with providing air defense systems to Damascus in order to defend against Israeli air raids.

Russia relies on Israeli coordination to continue their influence in the Levant region. However, continued cooperation could strain relations between Russia and Iran, particularly if Russia were ever forced to pick a side in the event that Israel and Iran ever engaged in direct physical conflict.

LAW ENFORCEMENT

[back to top]

On October 4, 2019, Russia's foreign ministry summoned the Iranian ambassador to Moscow for a meeting, following reports that a Russian journalist had been arrested in Iran for allegedly spying on behalf of Israel. According to a release put out by the foreign ministry, they sought to "facilitate a quick clarification of the circumstances of the incident and the protection of the rights of the Russian citizen." Iran released the prisoner on October 10.

Iran's recent spate of detaining tourists as prisoners has caused tensions with multiple countries. While it generally takes years to release prisoners from Western countries, such as the United Kingdom and Australia—with some still imprisoned in Iran now—the quick resolution and release of the Russian prisoner underscores a possible working relationship between Iran and Russia. [16, 17]

NUCLEAR ACTIVITY

[back to top]

Iran revealed construction of a second nuclear reactor at the Bushehr power plant, with which Russia is assisting. The expansion was recognized with a ceremony on November 10, 2019, led by Vice President Ali Akbar Salehi, and many journalists attended. Iran then revealed plans for a third reactor. This continued effort to increase nuclear facilities, along with Russian assistance and collaboration, is a consequence of the disintegration of the 2015 nuclear deal. The international community tried to prevent Iran from reinitiating nuclear activity, but no deal has come to fruition.

As of December 5, 2019, Russia has halted work at Iranian nuclear complex Fordow due to complications with uranium compatibility. Rosatom, a Russian nuclear company, is working to modernize a nuclear unit within Fordow. This project has been ongoing since 2017. Rosatom is risking punitive sanctions from the United States due to its work with Iran, but Russia and Iran continue their congenial relationship and cooperation in nuclear technology.

ISIS

[back to top]

Moscow and Tehran could also partner to prevent the Islamic State from strengthening. As was done previously, Russia could use Iranian air bases to strike Syria. The “4+1 coalition” is an information-sharing unit in Baghdad, which Russia and Iran joined Syria, Iraq, and Hezbollah to create.

DISINFORMATION

[back to top]

Iranian disinformation campaigns lack the sophistication and reach of Russia’s disinformation infrastructure, which, although it often enjoys direct support from the state, is capable of functioning independently from it. Both Iran and Russia have engaged in coordinated inauthentic behavior on social media platforms. Infrastructures sometimes overlap, but this does not necessarily mean coordinated campaigns.

- **In February 2020 Facebook removed a large number of accounts connected to Iranian and Russian disinformation infrastructures.**
- **In March 2020 in the context of the ongoing COVID-19 pandemic a Canadian disinformation website, which had previously been linked to Russia, used material from Iranian state-linked sources to support a disinformation narrative that COVID-19 was created in a US military lab. The article was later amplified by Chinese state-linked actors in social media, and the conspiracy theory was mentioned in Russian television shows targeting domestic audiences. Russian state-linked actors did not support it.**

SOURCES

[back to top]

[1] hxxps://www[.]washingtoninstitute[.]org/policy-analysis/view/russian-arms-and-technology-transfers-to-iran-policy-challenges-for-the-uni
[2] hxxp://www[.]defencejournal[.]com/2001/august/russians[.]htm
[3] hxxps://www[.]rbth[.]com/lifestyle/330129-is-russia-superpower
[4] hxxps://qz[.]com/1331063/trump-putin-summit-why-russia-isnt-a-world-power-like-the-us-or-china/
[5] hxxp://tass[.]ru/en/society/823291
[6] hxxps://www[.]pewresearch[.]org/wp-content/uploads/sites/7/2017/05/CEUP-Overview-Russian-FOR-WEB[.]pdf
[7] hxxps://islam-today[.]ru/blogi/rafik-muhametsin/islam-v-sovremennoj-rossii/
[8] hxxps://www[.]cgpolicy[.]org/articles/russias-strategy-toward-islam-and-muslims/
[9] hxxps://www[.]wilsoncenter[.]org/article/coping-the-russian-challenge-the-middle-east-us-israeli-perspectives-and-opportunities-for
[10] hxxps://www[.]unian[.]info/world/10829891-russia-could-remotely-control-missile-launcher-that-brought-down-ps752-media[.]html
[11] hxxps://www[.]clearskysec[.]com/wp-content/uploads/2017/07/Operation_Wilted_Tulip[.]pdf
[12] hxxps://blog[.]certfa[.]com/posts/the-return-of-the-charming-kitten/
[13] hxxps://www[.]fireeye[.]com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools[.]html
[14] hxxps://www[.]fireeye[.]com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton[.]html
[15] hxxps://www[.]theguardian[.]com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency
[16] hxxps://www[.]washingtoninstitute[.]org/policy-analysis/view/russian-arms-and-technology-transfers-to-iran-policy-challenges-for-the-uni
[17] hxxps://www[.]rbth[.]com/lifestyle/330129-is-russia-superpower

=======

All Flashpoint intelligence reports, related data, and content are the property of Flashpoint, and are protected under all applicable laws. Flashpoint reports and data are intended solely for the internal use of the individual and organization to which they are addressed, and are subject to the applicable terms and conditions of your Subscription Agreement with Flashpoint and/or your NDA, as applicable. Flashpoint reports and data are Flashpoint Confidential Information, and as such, may not be shared outside of your company or disclosed publicly for any purposes without Flashpoint’s written consent; provided, however, that you may share such materials to third parties if legally required, or on a need-to-know basis, and then only to those parties who are bound by confidentiality obligations no less protective of Flashpoint than those contained in your Agreement and/or your NDA.

=======