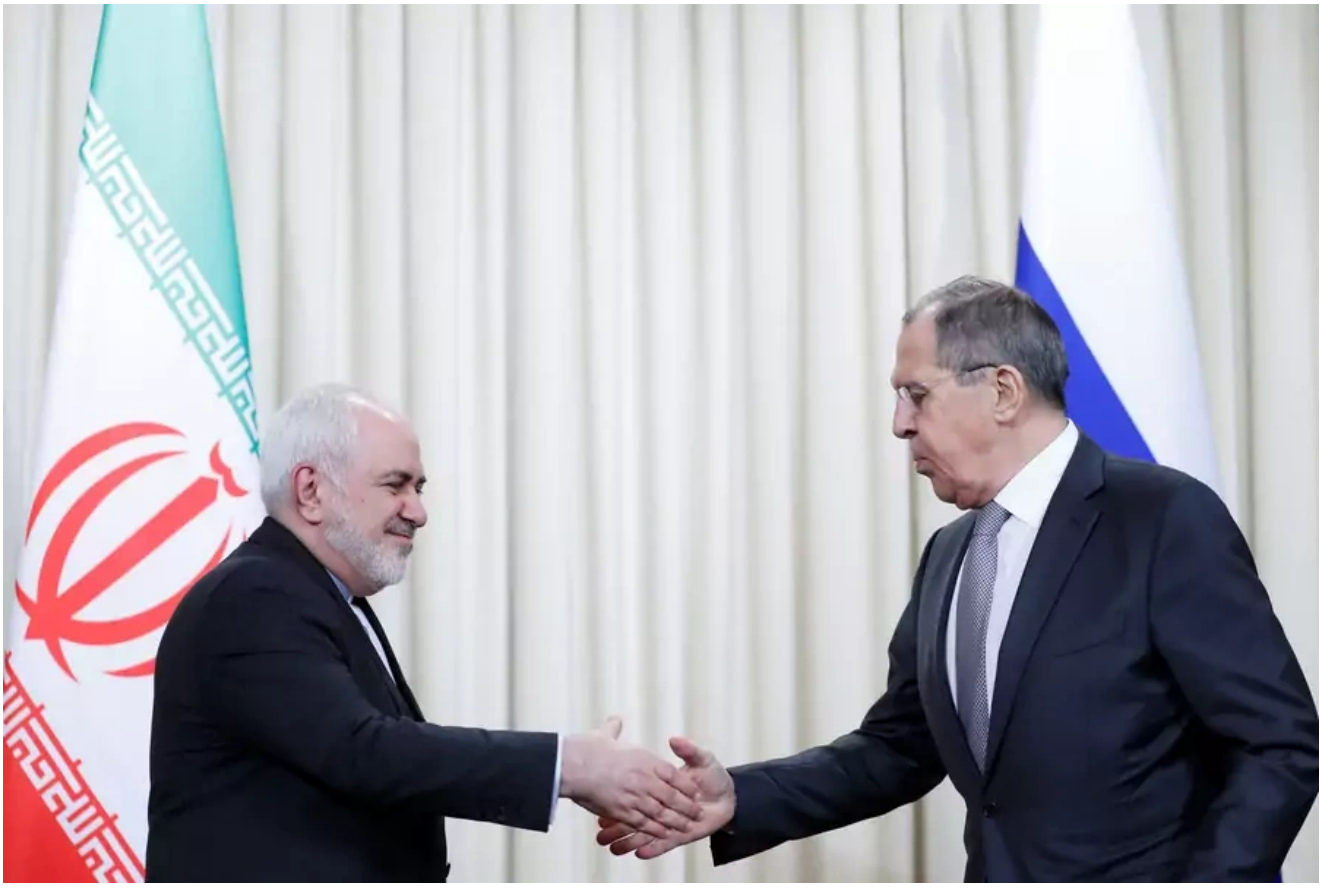
The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East

cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east

The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East

from Digital and Cyberspace Policy Program and Net Politics
The new cooperation agreement between Russia and Iran on cybersecurity and information technology is likely to create new hurdles for the United States and its allies in the Middle East.



Iran's Foreign Minister Mohammad Javad Zarif shakes hands with Russia's Foreign Minister Sergei Lavrov. REUTERS/Evgenia Novozhenina

Blog Post by Guest Blogger for Net Politics

March 15, 2021 2:28 pm (EST)

Omree Wechsler is a senior researcher at the Yuval Ne'eman Workshop for Science, Technology, and Security at Tel Aviv University.

This January, Russian Foreign Minister Sergey Lavrov and his Iranian counterpart Javad Zarif signed a cooperation agreement on cybersecurity and information and communications technology (ICT). The agreement includes cybersecurity cooperation, technology transfer, combined training, and coordination at multilateral forums, like the United Nations.

More on:

Cybersecurity

Iran

Russia

Security Alliances

Although the cooperation with Moscow outlined in the agreement could upgrade Tehran's offensive cyber capabilities, the agreement is largely defensive, motivated by the countries' shared animus toward the United States and U.S. influence in the Middle East as well as a desire to reduce dependence on Western technology. There are limits, however, to how closely the two sides can be expected to work together. The relationship between Russia and Iran has long suffered from mutual suspicion, ideological differences, and competition. Moreover, in the past, Russian and Iranian operators have operated at cross purposes. For example, in October 2019, British and U.S. officials revealed that the Russian threat actor Turla had hijacked Iranian hacking infrastructure as part of a false-flag operation.

Due to suspicion and conflicting objectives, Cyber cooperation between Moscow and Tehran is likely to be focused on intelligence sharing and improving cyber defenses, rather than sharing offensive capabilities. Nonetheless, the agreement could pose four challenges to U.S. cyber operations. First, Russia could help Iran obtain stronger cyber defense systems. Harvard's Belfer Center's National Cyber Power Index 2020 [PDF] lists Iran as the lowest-scoring nation for cyber defense capabilities, with Russia ranked in the middle of the

countries surveyed. If Tehran addresses these defensive deficiencies with the help of Russian technology and training, it could make U.S. initiatives like defend forward [PDF] more challenging and costly.

Second, Iran-Russia cyber cooperation could entail Russian cyber teams deploying to Iran to monitor Iranian networks in order to collect insights and identify U.S. malware, similar to U.S. Cyber Command's "Hunt Forward" operations. Acquiring and analyzing Cyber Command or National Security Agency hacking tools and techniques could help improve Russian and Iranian defenses, thwart future U.S. cyber operations, and force U.S. hackers to develop new exploits sooner than they hoped.

Third, if able to access Iranian defense systems, Russian hackers could acquire and reverse engineer U.S. or Israeli malware that has been used against Iran. This occurred with the Stuxnet worm, which targeted Iran's nuclear facilities in 2010 and was attributed to the United States and Israel. Since then, numerous cyber actors have developed over 22 million pieces of malware that used Stuxnet's blueprint to target organizations around the world. Stuxnet eventually infected thousands of networks globally, so hackers had access to lots of samples, but an attack that did not become as widely known could still be repurposed if Russia is able to access Iranian networks.

Fourth, technologies and techniques that Iran acquires from Russia could be provided to Iran's proxies around the Middle East, including Hezbollah and militias in Iraq and Yemen. Some of these groups have already shown considerable hacking capabilities. In January, security firm ClearSky revealed that a Hezbollah-affiliated hacking group named Lebanese Cedar was involved in an extensive campaign that targeted telecoms and internet service providers in the United States, Europe, and Middle East. Equipping Iranian proxies with advanced Russian cyber capabilities could allow them to threaten government agencies, businesses, and U.S. operations in the Middle East. It could also hamper investigations into cyber operations conducted by Iranian proxies and lead to misattributing them to Russia, possibly causing unintended escalation.

More on:

Cybersecurity

Iran

Russia

Security Alliances

Although the agreement between Moscow and Tehran could pose challenges for U.S. cyber strategy, some of its disruptive implications can be mitigated. To minimize the risk of their hacking tools being repurposed for use against them, the United States and its allies should establish a unified vulnerability disclosure mechanism to share vulnerabilities, including

those that have already been exploited, with each other and vendors. While the United States already has a vulnerability equities process, other allies seem to have only varying degrees of similar processes, if at all. Because victims are likely to patch vulnerabilities once they've been targeted, the attacking country can disclose the vulnerabilities it used after they've been exploited without weakening its offensive capabilities. Furthermore, the United States could promote the responsible development of offensive capabilities by adding self-destruct code modules to prevent them from being analyzed by adversaries. These modules have been deployed as part of highly sophisticated malware campaigns in the past and are designed to overwrite their own file data in order to prevent forensic analysis.

Establishing a standardized vulnerabilities disclosure mechanism could take place as part of a broader effort to strengthen intelligence sharing and security ties between the United States, Israel, the Gulf States, and possibly other actors in the region. As cyber cooperation between Russia and Iran grows, leaving it unchallenged could pose new threats to U.S. security and strategy in the Middle East.