Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

UNCLASSIFIED

INTELLIGENCE ASSESSMENT

Iran's Use of Cyber in Cognitive Warfare

Intelligence Assessments Branch
Direction de l'évaluation du renseignement

Canada

INTELLIGENCE ASSESSMENT

2023 02 20 UNCLASSIFIED CSIS IA 2022-23/100

Iran's Use of Cyber in Cognitive Warfare

"the modern concept of war is not about weapons but about influence." - NATO Innovation Hub, 2020

In recent years, NATO researchers[1] have been grappling with how the cyber domain has influenced adversaries' deployment of "cognitive warfare," defined as a tactic used to "alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision-making and hinder actions, with negative effects, both at the individual and collective levels." Psychological operations are neither new nor limited to the cyber domain; however, technological developments have exponentially augmented a state's ability to manipulate and influence adversaries at home and abroad. Iran is one of the hostile state actors[2] (HSAs) that use cyberspace to manipulate the psychology of both foreign and domestic adversaries and regime critics. The strategy is evident in the deployment of ransomware against Israel, the recent large-scale cyber attacks against Albania, and Iran's long-standing use of cyber tools to target and control dissidents.

Key Assessments

- Iran uses ransomware to impose psychological costs on its adversaries, particularly Israel, by recalibrating the traditional opportunistic, profit-driven ransomware paradigm to one that targets specific adversaries, with the goals of causing disruption, distress, and influencing decision-making abilities.

- Iran conducted disruptive cyber attacks to intimidate and embarrass the Albanian government in response to Albania's hosting of the Iranian opposition group, Mujahideen-e Khalq (MEK). They also used cyber tradecraft to influence the Albanian population by simultaneously undermining the Albanian government's ability to protect its citizens while trying to win Albanians' favour through sharing leaked government data.

- Iran uses cyber extensively as a tool for the repression and manipulation of critics at home and abroad. This is achieved through various strategies. First, Iran controls domestic access to the internet in order to influence citizens' psychology and actions. Next, they use cyber as a social engineering tool to manipulate targets into installing malware, handing over credentials, or believing a false narrative. Finally, Iran uses cyber tools more directly to surveil and target dissidents, sometimes combined with real world targeting.

[1] Research community where experts and innovators collaborate to tackle NATO challenges. See https://www.innovationhub-act.org/about
[2] This tactic is also used by Russia and China. See "Cognitive Warfare: First NATO scientific meeting on Cognitive Warfare" (June 2021); "The future of China's Cognitive Warfare: Lessons from the War in Ukraine" (July 2022)

Canada

INTELLIGENCE ASSESSMENT

Ransomware campaigns against Israel

1. While a typical ransomware attack induces stress as part of the overall strategy to extract funds from the victim, Iran's objective in targeting Israel via ransomware incorporates psychological elements intended to induce fear and to influence the populations' perception of their government. An Israeli think tank has observed that "the use of ransomware attacks for the purpose of influence operations rather than for an economic purpose is a singular phenomenon … unique to the framework of the conflict between Israel and Iran or its supporters."

2. A case in point is the BlackShadow campaign against Israeli hosting provider Cyberserve in 2021, which included data theft from an Israeli gay and lesbian dating website. Threatening to release Cyberserve's data, which included the website users' personal information, sexual orientation details and HIV status, BlackShadow put those individuals at risk—both physically and psychologically.

3. Moses Staff is another suspected Iran-linked ransomware actor that prioritizes political-psychological objectives over financial gain. Their attacks did not include a request for ransom and target selection was not random. Instead, throughout 2021, they used ransomware tools and techniques[3] to induce fear and overwhelm their victims. They claimed to have acquired the identities of members of Israel's 8200 Intelligence Unit, compromised the Israeli Defence Ministry, Israeli media and engineering firms. The attackers encrypted victims' systems, thereby rendering them inaccessible, while combining attacks with aggressive, intimidating messaging. The group used their Telegram channel to pronounce statements like, "Fight against the resistance and expose the crimes of the Zionists in the occupied territories," or "We've kept an eye on you for many years," and "we will strike you". Media coverage of Moses Staff activity included phrases that highlighted the far-reaching, disruptive nature of the attacks, thereby indicating that they attempted to "create noise," "cause chaos" and "wreak havoc on Israel". This tactic of "overwhelming" the victim is a component of cognitive warfare designed to exhaust the psychological bandwidth of the victim in order to influence (and impair) decision-making capabilities.

> *"The revolution in information technology has enabled cognitive manipulations of a new kind, on an unprecedented and highly elaborate scale."* –NATO Innovation Hub, 2020

Attacks against Albania

4. From July to September of 2022, the Government of Iran (GOI) conducted coordinated cyberattacks that disrupted Albanian government services. These attacks included ransomware, hack-and-leaks, bulk-text messages of intimidation sent to the public, and data-wiper campaigns. Impacts included temporary suspensions of Albania's public services portal. The attacks were very likely in response to Albania's ongoing hosting of MEK conferences,[4] as indicated by the anti-MEK messages left on the screens of compromised computers. Similar to the other ransomware campaigns previously highlighted, this multi-pronged attack was designed to intimidate and overwhelm the victim.

5. Some ransomware experts have observed that ransomware victims care less about the culpability of the attackers and more about the impacts of ransomware attacks. For example, unemployment could result when companies are

[3] Media reports indicate Moses Staff exploits known vulnerabilities for initial access, Powershell for lateral movement and open-source encryption tools. They also use a Tor-based data leak site to announce their victims, much like other ransomware groups.
[4] MEK is an Iranian opposition group. Albania has hosted MEK conferences, with the support of the United States and Israel, since 2013.

unable to recover. This, in turn, leads to people experiencing heightened levels of stress, suspiciousness, and an erosion of confidence in businesses and government. Similarly, on a geopolitical level, key objectives of cognitive warfare include the erosion of trust that underpins society and the alteration of worldviews. Just as the Iranian ransomware attacks against Israeli entities was likely used, at least in part, to cause the Israeli population to lose faith in their government's ability to protect them, the multi-faceted, sustained attacks against Albania likely had the same objective: to make the Albanian population feel less secure and erode its trust and confidence in their government, particularly with respect to the presence of the MEK.

6. Erosion of trust in the domestic government can also be coupled with cyber tactics that are designed to win support for the adversary. As part of the attacks against Albania, cyber actors used their Telegram channel to solicit input from Albanians about which stolen government data—including the Prime Minister's emails—they wanted to see first. NATO researchers have suggested that "[s]ocial engineering always starts with a deep dive into the human environment of the target. The goal is to understand the psychology of the targeted people. This phase is more important than any other, as it allows not only the precise targeting of the right people, but also to anticipate reactions, and to develop empathy." Instead of representing themselves as the enemy for this part of the campaign, the threat actors likely sought to win empathy—or at least curry favour from—the population, reframing themselves as a Robin Hood-type hero.

Targeting and Control of Regime Critics

7. Iran uses cyber extensively as a tool for the repression and manipulation of critics at home and abroad. Control of the internet and access to communications platforms limits the population's ability to communicate and organize, and it induces fear. There have been numerous documented instances of Iran throttling internet infrastructure and access to platforms like WhatsApp and Instagram during periods of unrest.

8. In a study conducted on populations in India that are subject to internet shutdowns, psychological impacts varied. While some had increased mistrust in the government, others accepted government actions as necessary to stop "misinformation." There were reports of panic, increased stress, feelings of isolation and, in some cases, behavioural changes—people did not leave their homes for fear they would lose contact with family members. CSIS assesses that a similar range of impacts would be experienced by Iranians from internet shutdowns. While not extensively studied, media coverage of the state-imposed internet filtering in the wake of the protests around Mahsa Amini's death highlights the psychological impact and effects on behaviour. One person interviewed said they felt "more brave" initially and were motivated to do something about the injustice they saw in the online coverage of protests. By contrast, when the GOI severed internet access, that same individual said that they felt alone. Actions taken by the government in this case contributed to feelings of isolation, and also effectively curbed retaliatory action by protesters.

9. Another strategy deployed by Iran involves using the online space for social engineering;[5] a key component of cognitive warfare. Researchers have suggested that Iran is becoming increasingly adept at leveraging social media

[5] According to the Canadian Centre for Cyber Security, malicious actors use social engineering to take advantage of people using information technology by exploiting human traits such as carelessness and trust. Threat actors use social engineering to trick individuals into providing

platforms to "convince a target to download malware, hand over credentials, or believe a false narrative." In this way, the victims are unaware that they are being coerced into clicking, making decisions they would not have otherwise made naturally, or they pursue a line of thought or adopt an ideology that has been orchestrated by the threat actor. This tactic is not limited to targeting Iranians; it has been observed in efforts to sow discord in the West. For example, in 2020, Iranians impersonated the Proud Boys right-wing extremist group online in an attempt to intimidate registered Democrats in the United States.

10. Iranian cyber actors also conduct more direct forms of control and influence using cyber tools. Iranian cyber actors use cyber platforms to monitor and harass opponents of the regime. In 2020, the United States imposed sanctions against the Rana Intelligence Computer Company, a front company for Iran's civilian intelligence service, for their use of malicious cyber intrusion tools to target and monitor Iranian citizens, particularly dissidents, Iranian journalists, former government employees, environmentalists, refugees, university students and faculty, foreign governments, and employees at international nongovernmental organizations. In some cases, the cyber surveillance facilitated real-world operations, as some of these individuals were subjected to arrest and physical and psychological intimidation by the intelligence service.

Outlook

11. The GOI seeks to ensure regime stability. To achieve that goal, Iran uses cyber as a "neuroweapon" that integrates psychological, and social engineering capabilities. Cyber is a low cost but effective tool that can be—and has been—one that Iran has used to sow doubt and induce other emotional responses, such as fear, to coerce certain actions or force inaction. Iran uses cyber tools to monitor and control dissent, and create mistrust of adversary ideologies and governments. This increasingly poses a threat to Western democracies because cyber-enabled cognitive warfare is not always easy to detect, to attribute, and it is certainly not easy to regulate or stop. Given the ubiquity of technology, particularly internet access and communication platforms, Iran will highly likely continue to exploit these avenues to achieve its national goals within and outside its borders.

sensitive information or inadvertently allowing access to a system, network, or device. Social engineering is also often used in combination with vulnerability exploitation.

INTELLIGENCE ASSESSMENT

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS