EXECUTIVE SUMMARY

Iran was one of the first states to formulate a coherent national cyber strategy, including the establishment of the necessary state institutions and development of the requisite technological capabilities. Its interest in the cyber realm was first sparked by two primary developments: first, the effective use that the opposition made of the internet to foment and sustain the mass demonstrations following the rigged presidential elections in 2009, and second, the dramatic Stuxnet attack against Iran's nuclear program in 2010, reportedly a joint US–Israeli operation. Ever since, Iran's cyber capabilities have grown steadily, and it is now commonly ranked at the top of the second tier of global cyber powers.

This memorandum presents a comprehensive and up-to-date analysis of Iran's cyber strategy, institutions, and especially praxis. In the absence of a formal statement of Iran's cyber strategy, the study draws on the limited open-source information available, some partial statements by Iranian officials, the broader literature on Iran's national security, and its observable behavior in both the cyber and kinetic realms. To this end, the memorandum presents a detailed account of essentially all the significant cyber operations that Iran has conducted from 2010 through December 2023.

For Iran, the cyber realm poses both major challenges and important advantages. Iran views the cyber realm with concern, as a subversive means of propagating Western values and empowering domestic opposition, and thus posing a threat to the regime. Conversely, it has also proven to be an effective means of shaping public opinion and exerting popular control.

In contrast with Israel's Arab adversaries in the past, Iran does not seek Israel's defeat in the near-term, which it knows is beyond its capabilities. Instead, Iran has adopted a long-term strategy of attrition, designed to sap Israel's military strength, erode its international standing, and undermine its societal resilience, thereby leading to its ultimate collapse. Iran similarly recognizes that it cannot pose a significant conventional threat to the United

States and other actors. Cyber has thus come to constitute an increasingly important component of Iran's strategy of asymmetric conflict. It is also particularly suited to Iran's strategic culture, which emphasizes ambiguity, deniability, and the use of proxies.

Iran conducts cyber operations both separately and in tandem with more traditional means of asymmetric conflict, such as terrorism and guerrilla warfare, to offset the advantages of its more powerful adversaries and to further augment and amplify its use of these asymmetric means. Cyber is a particularly important instrument for Iran, because its leading adversaries are far more dependent on the cyber realm than it is and therefore more vulnerable to attack.

Israel and the United States are Iran's primary adversaries in the cyber realm, and it conducts an ongoing, largely below-the-radar, cyber conflict against them. Iran's cyber operations also attack countries throughout Europe, the Middle East and beyond and has attacked targets of virtually every type. Iran has further adopted a full spectrum and flexible military doctrine; in other words, Iran reserves the right to take both offensive and defensive action, by whatever means it deems appropriate—kinetic or cyber. Iran's cyber operations constitute a complementary capability, not a stand-alone one, designed to buttress its diplomatic, economic, and military capabilities, and to strengthen its deterrence.

Iranian enmity toward the United States, Saudi Arabia, and others is deep; in Israel's case, it is fundamental and likely immutable. Without detracting from the depth of this enmity, much of Iran's cyber activity, like its behavior in other realms, has been reactive. As noted, Iran first built up its cyber capabilities largely in response to the Stuxnet attack; it prepared and conducted a number of attacks before and after the 2015 nuclear deal, using cyber means to respond to the assassination of Qassem Suleimani, a senior leader of the Revolutionary Guard, by the United States in 2020; and reportedly engaged in an ongoing exchange of cyber blows with Israel in recent years.

To assess the effectiveness of Iranian cyber operations to date, they have been divided into four primary categories: disruptive/destructive attacks, espionage operations, information operations, and mixed attacks, which combine some or all of the different types.

Disruptive/destructive attacks: Iran has already demonstrated its ability to cause significant economic disruption and to potentially damage critical national infrastructure in Israel, the United States, Europe, the Middle East, and elsewhere. Attacks against Israel's water supply and air traffic control systems have demonstrated the potential for lethal harm.

However, most of the disruptive/destructive attacks that Iran has conducted to date have been unsophisticated, and the defenses put into place have usually proven sufficient to prevent significant damage. Indeed, Iran has focused most of its attacks on poorly defended targets, thereby indicating that it may believe that important Israeli and Western targets are defended at a level beyond its capabilities. Conversely, the unsophisticated website defacement and disruption attacks, which constitute the bulk of Iranian attacks, have caused considerable inconvenience and have incurred significant financial costs.

Iran's ability to conduct effective and sustained military cyber operations cannot be adequately assessed based on its public record, and Iran has yet to manifest cyber capabilities at a systemic level. It may, however, be withholding its most advanced capabilities for the "appropriate" circumstances. What is clear is that the cyber realm does provide Iran with an important toolkit for conducting under the radar, disruptive, and destructive operations, which are harder to attribute to it.

Espionage operations: The very nature of espionage makes it difficult to draw clear-cut conclusions regarding the effectiveness of Iran's cyber operations in this area. At a minimum, they have been numerous and, in some cases, have yielded considerable classified information. Some attacks have collected intelligence regarding various states' defense industries, weapons

development programs, military capabilities, and more specifically about Israel's nuclear policy and US, Western and Israeli political and strategic thinking. Iran has also conducted cyber espionage operations for purposes of terrorism or in preparation for future destructive or information attacks.

Iran has also made particularly effective use of cyber operations for political surveillance and suppression, targeting dissidents both in Iran and abroad. Control of Iran's cyber realm has helped the regime suppress repeated rounds of demonstrations and ensure its ongoing stability.

Information operations: Cyber information operations are an integral and growing part of the regime's ongoing efforts to disseminate propaganda and gain support for its theocratic beliefs and policies, within Iran, the region, and worldwide. Cyber information operations have provided Iran and its proxies with a variety of platforms for reaching vast numbers of people directly, instantly, and at minimal cost.

Some of these operations have sought to create and exacerbate domestic divisions among Iran's adversaries, affect electoral processes, and undermine societal resilience of the targeted states. Iran's repeated cyberattacks against the US elections in 2020 are a case in point. Some operations have been designed to disrupt relations between foreign states and foment potentially severe crises; in one case, an Iranian website that disseminates false information even sought to create a nuclear crisis between Israel and Pakistan. Still other Iranian cyber information operations have caused financial and reputational damage to a variety of governments and firms around the world.

Cyber information operations have contributed to the ability of Iran and its proxies to create international pressure on Israel to prematurely halt or curtail military operations, before it can achieve its objectives. As such, these operations have adversely affected Israel's ability to conduct effective military operations and maintain its international standing.

Combined attacks: Most of the attacks that Iran has launched since 2020 have combined elements of disruption or destruction, with espionage and

information operations, and have often been disguised as ransomware attacks. Iran has leveraged these attacks to further amplify its offensive cyber capabilities, or compensate for their shortcomings, and their growing use has yielded higher payoffs. The use of ransomware attacks primarily for purposes of information operations, as opposed to financial gain, is unique to Iran's confrontation with Israel.

Iran's cyber praxis, to date, sheds light on three critical quandaries of interest to both cyber practitioners and theorists. First, cyber has proven to be not just an effective means of asymmetric warfare for Iran but also has been conducted with little risk of escalation. As evinced by the numerous cyberattacks detailed throughout this study, Iran's adversaries have rarely chosen to escalate in response to them.

Second, the contention that most Western and Israeli targets of importance may be defended at a level that is beyond Iran's capabilities—if, indeed, true—lends support to those who have maintained that the cyber realm is increasingly becoming defense, rather than offense dominant. Some even believe that Iran's ability to cause significant harm to sophisticated cyber actors has actually diminished. Be that as it may, advanced countries make effective use of some of the same asymmetric military advantages that cyber proffers to Iran, while also wielding their more powerful kinetic capabilities, thus enjoying the advantages of both worlds.

Third, whereas one school of thought contends that the cyber realm strengthens weaker actors, by providing them with additional asymmetric means to counterbalance the superior power of their adversaries, another posits that the sophisticated technological capabilities required for effective cyber operations have actually strengthened the advanced states even more. Iran has certainly made growing use of its cyber capabilities, but Israel, the United States, and other Western countries appear to wield cyber tools with greater socioeconomic and military efficacy. The Iranian experience seems

to lend more weight to the latter viewpoint. The bottom line may be a net overall gain in state power for already advanced actors.

Iran's praxis further demonstrates that it has not adopted a policy of "no first use" in the cyber realm. Conversely, there is no indication that Iran has integrated its cyber and nuclear strategies, that it believes that systemic cyberattacks constitute an escalatory rung below the nuclear level, and that it considers both to be a part of one overall national security strategy.

The number of Iran's cyber operations and their degree of sophistication have grown, and Iran has demonstrated the ability to disrupt, destroy, distort, sabotage, or undermine critical national infrastructure, commercial interests, military capabilities, domestic politics, societal resilience, and international diplomacy. Iran's capabilities will likely continue to improve, both due to its own indigenous capabilities as well as Russian and Chinese assistance. If one assesses the Iranian cyber threat according to the number of important and successful attacks that have taken place to date and their actual consequences, the threat should be considered significant, albeit limited. If, however, one bases the assessment on the potential for future disruption and damage, a growing threat should not be discounted.

Israel's public and private sector cyber strategy was one of the first of its kind, based on decisions adopted between 2011–2015. Much has changed in the interim, however, and a significant update is warranted. The Israel Defense Forces formulated an operational cyber doctrine, but not an overall military cyber strategy, and it has been now eight years since it decided to establish a unified cyber command, which was then suspended, pending further review. No statutory forum today below the cabinet is actively responsible for determining and coordinating military and intelligence cyber priorities and integrating the civil and military cyber strategies. These issues must be rectified if Israel is to maximize its cyber capabilities.

Stand-alone defeat of an adversary, in the traditional sense of preventing it from continuing to wage a conflict or undermining its psychological will

to do so, is not usually achievable in the cyber realm. Instead, Israel should seek "cyber superiority"; that is, the ability to impose a level of disruption or damage on an adversary that it cannot tolerate, or to reduce the severity of attacks against Israel to a level at which Israel can continue to function without significant disruption. To achieve cyber superiority, Israel will have to pursue a cumulative mixed-domain advantage through the gradual, additive application of the full range of capabilities available to it (cyber, kinetic, diplomatic, and economic). It also means cultivating a national pool of highly talented cyber professionals, of which Israel suffers from a considerable shortage. Israel must also formulate a national strategy to counter Iranian cyber information operations. The United States, United Kingdom, and France, among other democracies, have begun addressing this threat, and Israel can learn from their experience.

The Iranian nuclear program remains the greatest military threat to Israel's national security. The "Begin Doctrine," the preventive component of Israel's counter-proliferation strategy, has not been implemented to date against Iran, at least not in the classic sense of an air strike. The numerous kinetic and cyberattacks that Israel has reportedly conducted to sabotage the Iranian program may be a new means of implementing the doctrine. One way or the other, Israel must ensure that it has the kinetic and cyber capabilities to prevent Iran from ever gaining an operational nuclear capability.

Finally, the United States is Israel's primary partner in the cyber realm. Unlike most areas of bilateral military cooperation, Israel's cyber capabilities are primarily homegrown, and it has much to offer the United States, beyond just gain. It is important that Israel seek to expand its cyber cooperation with the United States to the extent possible, but in a manner that minimizes the risks to its freedom of independent action. Cyber dialogue should be formalized in new and expanded memoranda of understanding.