**Translation section**

API key not valid

**Page 1**

A Report of the CSIS Intelligence, National Security, and Technology Program  
Julia Dickson Emily Harding  
A Playbook for Winning   
the Cyber War  
Part 4: Evaluating Iran’s Cyber Strategy  
SEPTEMBER 2025

**Page 2**

A Playbook for Winning   
the Cyber War  
Part 4: Evaluating Iran’s Cyber Strategy  
AUTHORS  
Julia Dickson  
Emily Harding  
SEPTEMBER 2025  
A Report of the CSIS Intelligence, National Security, and Technology Program

**Page 3**

A Playbook for Winning the Cyber War | II  
About CSIS  
The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research   
organization dedicated to advancing practical ideas to address the world’s greatest challenges.  
Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former   
U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as   
president and chief executive officer since 2000.  
CSIS’s purpose is to define the future of national security. We are guided by a distinct set of   
values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship,   
integrity and professionalism, and talent development. CSIS’s values work in concert toward the   
goal of making real-world impact.  
CSIS scholars bring their policy expertise, judgment, and robust networks to their research,   
analysis, and recommendations. We organize conferences, publish, lecture, and make media   
appearances that aim to increase the knowledge, awareness, and salience of policy issues with   
relevant stakeholders and the interested public.  
CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the   
thinking of key influencers. We work toward a vision of a safer and more prosperous world.  
CSIS does not take specific policy positions; accordingly, all views expressed herein should be   
understood to be solely those of the author(s).  
© 2025 by the Center for Strategic and International Studies. All rights reserved.  
Center for Strategic & International Studies  
1616 Rhode Island Avenue, NW  
Washington, DC 20036  
202-887-0200 | www.csis.org

**Page 4**

Julia Dickson and Emily Harding | III  
Acknowledgments  
The authors would like to extend their gratitude to those who agreed to be interviewed and to their   
foreign partners who contributed valuable insights from the front lines of this fight. The authors   
would also like to thank Rex Booth and Dana Stroul for graciously providing valuable feedback,   
Susan Hines for helping with the project contract, and the CSIS iDeas Lab for offering their   
design expertise.   
This report is made possible by project support from the Smith Richardson Foundation.

**Page 5**

A Playbook for Winning the Cyber War | IV  
Contents  
Authors’ Note about the Series   
1  
Overview of Iran’s Cyber Playbook   
2  
Core Elements of Iran’s Strategy   
5  
How Cyber Strategy Fits into Foreign Policy   
8  
How Iran Approaches Deniability   
10  
Implementation: Campaigns or Opportunism?   
11  
Organization of Capabilities   
13  
Who Are the Fighters?   
13  
Case Study 1: Deserts vs. Sands   
29  
Case Study 2: Tehran Targets Tirana   
31  
Case Study 3: Iranian Cyberattacks During the Israel-Hamas War   
34  
About the Authors   
37  
Endnotes   
39

**Page 6**

Authors’ Note About  
the Series   
T  
his report is part of a series on the future of cyber warfare. This section examines how Iran   
fights in the cyber domain, including the core elements of Tehran’s strategy for conducting   
cyber operations, how that strategy fits in a larger foreign policy context, and who the   
frontline fighters are in this new mode of conflict.   
Part 1 of this series offers a broad introduction to the report, covers key takeaways from the   
comparative studies and wargames, and summarizes the authors’ recommendations. Part 2, 3, and   
4 examine how Russia, China, and Iran, respectively, fight in the cyber domain, and Part 5 examines   
U.S. cyber practices. Part 6 tests how U.S. policymakers view cyber operations as part of the spectrum   
of war, peace, and irregular warfare, illuminated by a set of wargames. Finally, Part 7 fully explains   
the new playbook that will close the gap between how the United States and its adversaries fight and   
succeed in the cyber domain.  
Julia Dickson and Emily Harding | 1  
Photo Source: Emanuele Mazzoni/Adobe Stock

**Page 7**

A Playbook for Winning the Cyber War | 2  
Overview of Iran’s   
Cyber Playbook  
I  
n July 2022, Albanian government networks began to crash. Ransom notes appeared from   
“HomeLand Justice,” but it was clear the attackers were not Albanian. The attackers collected   
and then either deleted or leaked classified information, including the identities of undercover   
intelligence officers and emails from the director of intelligence. As Foreign Policy put it at the   
time: “all aspects of the lives of Albanian citizens, from births to marriages to deaths, were thrown   
into disarray.”1  
Iran, angry at Albania’s hosting of an Iranian opposition group that it classifies as a terrorist   
organization, had used an intensive cyberattack to coerce and punish the country. Though Albania’s   
systems largely were restored within weeks, Iran hit Tirana again in September 2022 and a third   
time in December 2023. By the December attack, Albania had learned hard lessons and was resilient   
enough to avoid severe consequences.2  
Iran can fairly be described as a rising, aggressive cyber actor. Persistent cyber operations for   
domestic surveillance as well as years of constant confrontation with Israel and Saudi Arabia have   
given Tehran significant experience in this domain. Two key events catalyzed Iran’s cyber focus:   
(1) a set of regime-threatening protests in 2009 called the Green Movement, and (2) the discovery   
of the Stuxnet virus, which targeted Iran’s nuclear program.3 More recently, Iran has shown a   
willingness to escalate dramatically and to engage in high-profile attacks. In addition to the attack   
on Albania in 2022, for instance, Iran attempted to interfere in the 2020 and 2024 U.S. elections and   
attacked water infrastructure in the United States in 2013 and again in 2023.4

**Page 8**

Julia Dickson and Emily Harding | 3  
In the wake of the Green Movement, also known as “Iran’s Twitter Revolution,” Tehran found   
it necessary to develop cyber capabilities in order to maintain the strength of the regime. As   
millions of Iranians took to the streets to protest the presidential elections, protestors also   
gathered on social media sites and conducted distributed denial of service (DDoS) attacks against   
government websites.5 According to analysis by the Carnegie Endowment for International   
Peace, the government became acutely aware that the internet “could be used as an instrument   
of mass mobilization and represented a significant challenge to the regime’s long-held   
information monopoly.”6  
In response to the protests, the regime developed tools to control its domestic cyberspace and   
surveil its population. Government-affiliated groups defaced websites associated with the political   
opposition, Israeli businesses, and social media sites. Official government groups also conducted   
DDoS attacks against critical websites and spied on government critics. The surveillance and   
censorship eventually paralyzed the Green Movement, and the strategy, tools, and threat actors that   
developed during this period laid the groundwork for Iran’s modern cyber operations.7  
Likewise, the discovery of the Stuxnet attack may have encouraged Tehran’s development of   
offensive, retaliatory tools. Stuxnet, a series of exploits that infected Iran’s nuclear facilities around   
2009, caused not only digital problems but also physical damage. Centrifuges, in particular, seem   
to have been affected by the code.8 Not long after, in 2011, Iran launched attacks against at least   
six big American banks and a small dam in New York.9 The country then hit Saudi Aramco, the   
largest Saudi oil company, in 2012, destroying an estimated 35,000 computers.10 Since then, Iranian   
hackers have conducted thousands of cyberattacks, primarily against Israel, the United States,   
and Saudi Arabia.11  
Tehran has committed millions of dollars to developing its cyber capabilities. According to a report   
by the Institute for National Security Studies at Tel Aviv University, “some 18 percent of Iranian   
university students were reportedly studying computer science” by the late 2010s and “Iran’s cyber   
budget jumped twelvefold between 2013–2021.”12 The regime uses compulsory military service to   
channel these technologically knowledgeable graduates into the state security apparatus, including   
the two components best known for carrying out cyberattacks: the Islamic Revolutionary Guard   
Corps (IRGC) and the Ministry of Intelligence ( ).13  
Cooperation with other countries has also contributed to Iran’s cyber capabilities. Tehran and   
Moscow have signed numerous cyber cooperation agreements, starting with a preliminary   
agreement in 2015.14 In 2017, the two countries signed a memorandum of understanding for   
cooperation on information technology and communications-related issues, including “internet   
governance [and] network security.”15 Further, they signed an updated agreement in 2021 to   
share information related to “the fight against crimes committed with the use of information and   
communications technology,” which includes cooperation in detecting cyber intrusions, technology   
transfer, and combined training.16 Moscow is also supplying Tehran with technology. For example,   
in 2023, the Kremlin provided Tehran with powerful communications-surveillance capabilities and   
advanced software for hacking dissidents’ systems and phones.17

**Page 9**

A Playbook for Winning the Cyber War | 4  
China has also contributed to Iran’s defensive cyber capabilities. In 2021, the two countries signed   
a 25-year strategic agreement, which was leaked on social media and published by Iranian news   
sites. It includes both military and cybersecurity cooperation, and as part of this agreement,   
Beijing will help Tehran build its 5G telecommunications infrastructure and assert greater control   
over its cyberspace by sharing knowledge and technologies related to digital surveillance and   
online censorship.18  
While Tehran is rapidly improving its cyber capabilities, they somewhat lag behind other advanced   
cyber actors. In 2017, an Israeli general assessed that Iran is “not state of the art” nor the “strongest   
superpower in the cyber dimension,” but is nonetheless quickly improving its cyber capabilities.19   
Iranian leaders are known to oversell the nation’s offensive cyber capabilities as part of their   
military propaganda, and Tehran lacks an advanced and organized security apparatus, so the   
most sophisticated kinds of cyberattack (such as Stuxnet or the Russian actions in Ukraine) are still   
beyond Iranian capabilities.20  
Although Tehran is not yet as advanced as Russia or China, the United States and its allies should   
not underestimate this adversary. Tehran has demonstrated a brazen willingness to attack civilian   
critical infrastructure and will likely continue to reach for destructive tools. Poorly defended targets   
in the United States (of which there are many) are vulnerable; they include smaller banks or local   
power companies, or poorly secured pipeline control systems. Further, Iran conflates Israel and   
the United States, viewing the latter as a legitimate target in retaliation for Israeli actions. As the   
2023 Annual Threat Assessment from the Office of the Director of National Intelligence states: “Iran’s   
growing expertise and willingness to conduct aggressive cyber operations make it a major threat to   
the security of the U.S. and allied networks and data.”21  
Although Tehran is not yet as advanced as Russia or China,   
the United States and its allies should not underestimate this   
adversary. Tehran has demonstrated a brazen willingness to   
attack civilian critical infrastructure and will likely continue to   
reach for destructive tools.

**Page 10**

Julia Dickson and Emily Harding | 5  
Core Elements of   
Iran’s Strategy  
I  
ran has emerged as an aggressive cyber actor unburdened by concerns about norms and   
international law. In developing its offensive and defensive cyber capabilities, the country has   
two main goals: (1) to create a “technological envelope” to protect its critical and sensitive   
infrastructure from cyberattacks, and (2) to counter adversaries in cyberspace.22 Central to   
the second goal is “forward defense,” a concept holding that militarily confronting adversaries   
outside of Iran’s borders is preferable to fighting them within Iran.23 Offensive cyber operations   
are an important component of this hybrid strategy, suggesting that Iran will continue to invest in   
developing its cyber capabilities.24  
This section will cover several key features of Iran’s cyber strategy: sophisticated social engineering   
campaigns to gain access to networks, cyber-enabled influence operations, disruptive and   
destructive attacks, and the use of proxies to carry out these various methods of attack.  
As part of their cyber operations, Iranians have become particularly adept at crafting sophisticated   
social engineering campaigns. According to a 2022 report by Insikt Group, Iranian hackers are   
capable of social engineering in ways that are similarly as advanced as Russia’s advanced persistent   
threat (APT) groups, demonstrating the capability to understand and dissect foreign societies,   
political systems, and languages. Iranian APTs “use many of the studied ‘principles of influence’   
and overlap with human intelligence (HUMINT) recruitment processes” to target their victims. They   
are known for employing a variety of approaches such as using “charismatic sock puppets” and   
creating fake prospective job opportunities to connect with victims.25 They also pose as journalists

**Page 11**

A Playbook for Winning the Cyber War | 6  
and think tank experts seeking comments on a particular topic.26 Some examples of advanced social   
media campaigns include the following:  
    
▪  
An Iranian APT known as Imperial Kitten used the social media persona “Marcella Flores”   
to engage with a subsidiary of an aerospace defense contractor. The APT friended the victim   
on Facebook in 2019, if not before, and actively had conversations with the victim on both   
corporate and personal communication platforms in 2020. In early June 2021, Imperial   
Kitten delivered a malicious email in an attempt to infect the victim’s system with malware.   
In mid-July, Facebook announced that it removed a network of fake users, including Marcella   
Flores, from its platform.27   
    
▪  
Israel’s Shin Bet internal intelligence agency announced in late July 2023 that Iranian hackers   
created fake LinkedIn profiles and initiated conversations with Israeli citizens, specifically   
civil servants and researchers, eventually moving to email. The Israeli agency managed to   
thwart the campaign.28  
Another key component of Iran’s recent cyber strategy is the use of cyber-enabled influence   
operations. These operations have become significantly more common since mid-2022 and surged   
in particular as the Israel–Hamas conflict broke out in October 2023. They “combine offensive   
computer operations with messaging and amplification in a coordinated and manipulative fashion   
to shift [victims’] perceptions, behaviors, or decisions” and further the regime’s strategic objectives,   
according to Microsoft.29 Tactics include leaking sensitive data to undermine public trust in   
institutions and posting hacked material to social media pages to drive fear in Iranian adversaries   
and boast about Iran’s capabilities. Iranian threat actors adopted this technique as a way to boost,   
exaggerate, and compensate for Iran’s lower level of technical capability.30  
Table 1: Cyber-Enabled Influence Operation Methods  
Cyber Method  
    
▪Stealing data  
    
▪Website defacement  
    
▪Ransomware  
    
▪DDoS attacks  
Influence Method  
    
▪Data leaks  
    
▪Sharing stolen data on social media or   
via SMS and email  
    
▪Impersonating victims  
    
▪Sock puppets  
Source: “Iran turning to cyber-enabled influence operations for greater effect,” Microsoft Threat Intelligence, May 2, 2024, https://  
www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-turning-to-cyber-enabled-influence-operations-for-g  
reater-effect.

**Page 12**

Julia Dickson and Emily Harding | 7  
Throughout Israel’s war in Gaza, Iranian APTs have used cyber-enabled influence operations to   
intimidate Israelis and criticize the Israeli government’s military strategy and handling of hostages,   
with the ultimate goal of polarizing Israeli society and eventually destabilizing the country. Iran also   
uses this technique against Israel’s allies to undermine support for Israel’s military campaigns.31 In   
one instance, Emennet Pasargad, an Iranian-state-affiliated front company, interrupted multiple   
broadcast channels in the United Arab Emirates, the United Kingdom, and Canada. The front   
company accessed the news stations’ internal networks and used this access to broadcast their own   
content. Their video began with an AI-generated newscaster reading a message saying, “We had no   
choice but to deliver this to you,” before showing unverified graphic images of Palestinians killed or   
injured by the Israeli military.32  
In early July 2024, then-Director of National Intelligence Avril Haines issued a formal statement   
about Iranian influence operations directed at Americans. She warned:  
In recent weeks, Iranian government actors have sought to opportunistically take advantage   
of ongoing protests regarding the war in Gaza, using a playbook we’ve seen other actors use   
over the years. We have observed actors tied to Iran’s government posing as activists online,   
seeking to encourage protests, and even providing financial support to protesters.33  
Haines also stated that Americans were protesting to express their authentic views on the war in   
Gaza and highlighted that expressing those opinions is a core part of being a democracy. However,   
Iran-backed hackers interrupt news broadcasting with AI-generated content.  
Source: “Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence, February 26, 2024,   
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-i  
n-support-of-hamas.

**Page 13**

A Playbook for Winning the Cyber War | 8  
her larger warning was that Iran was hiding its true identity, pushing additional protest action, and   
seeking to foment unrest through these campaigns.  
Tehran’s willingness to conduct disruptive, even destructive, attacks against civilian targets makes it   
a cyber adversary requiring additional focus. In short, Tehran is predictably aggressive, but against   
unpredictable targets, and its attacks can range from feckless to highly destructive. In 2012, for   
example, Tehran targeted one of the world’s largest oil companies, Saudi Aramco, using a phishing   
email and a wiper to partially wipe or completely destroy an estimated 35,000 computers in a few   
hours. While the attack failed to impact oil production, it froze all payment systems and prevented   
gasoline tank trucks from processing payments. CNN reported in a deep dive on the attack that   
“Managing supplies, shipping, contracts with governments and business partners—all of that was   
forced to happen on paper. . . . After 17 days, the corporation relented and started giving oil away   
for free to keep it flowing within Saudi Arabia” and to ensure the country had a sufficient supply as   
Saudi Aramco worked to bring the systems back online.34  
The use of proxies and front organizations is another important component of Iranian strategy   
that allows the country to maintain a level of plausible deniability. For instance, a group called   
“Cutting Sword of Justice” claimed responsibility for the attack on Saudi Aramco, citing it as an   
act of retaliation for supporting the Al Saud regime and its crimes and atrocities against citizens   
in Syria, Lebanon, and Egypt, amongst others. Iran denied any involvement in the attack, but U.S.   
intelligence attributed it to Tehran.35 For more about proxies and front organizations, see page 23.  
How Cyber Strategy Fits into Foreign Policy  
Iran views cyber as a cost-effective, low-risk tool for harassing its adversaries abroad. Iran uses   
cyberattacks as one tool in its asymmetric tool kit, enabling a less risky way to challenge nations that   
it could not compete with in a conventional armed conflict. Using cyber tools, Tehran can damage   
conventionally stronger opponents and quickly collect intelligence on a variety of strategically   
valuable targets while maintaining a level of deniability. The intended outcomes of the attacks range   
from espionage and embarrassment of an adversary to real, lasting damage against an enemy that is   
conventionally stronger.36  
Iran also uses cyber operations as a defense mechanism for maintaining stability at home,   
specifically to ensure regime survival. Domestic surveillance is a strong focus of the regime’s cyber   
operations. Iranian threat actors, for example, frequently target current Iranian government   
officials (such as diplomats) and their families as well as reformist politicians and journalists. Tehran   
collects personal information and monitors the political and personal networks of these individuals   
who are of strategic interest to the Iranian government. This allows the regime to watch for   
potential rivals and obtain sensitive information that can later be used for blackmail.37  
Another key component of Tehran’s strategy is to control its domestic information space to prevent   
Western values and culture from “corrupting” Iranian society. Iran views cyberspace as “a cultural   
battlefield between Iran and the Western world.” The IRGC persistently blocks international news   
sites, social media sites such as Facebook and Twitter, and other popular media sites such as

**Page 14**

Julia Dickson and Emily Harding | 9  
YouTube and Netflix, with the aim of “block[ing] the West’s use of cultural and political ideals to   
subvert the Iranian State.”38 In February 2024, Tehran implemented a partial ban on the use of   
virtual private networks (VPNs), an escalation in enforcement following the 2022 decision to punish   
the purchase and sale of VPNs.39  
To further control its information space, Iran is developing the National Information Network (NIN),   
a local intranet entirely supported by domestic infrastructure. According to the U.S. Department of   
the Treasury, the NIN is “being used to disconnect the Iranian people from the global internet.”40   
As it will be completely under government control, the NIN, once operational, will allow the   
government to keep critical infrastructure online when it imposes internet blackouts to silence   
criticism. Such control is already evident; in 2019, as protests erupted over a petrol-rationing   
scheme that significantly raised oil prices, the Iranian government imposed an internet blackout   
that cut access for most of the country for a week. Services such as banking transactions were able   
to continue, and local versions of other internet-based tools such as a navigation app and a search   
engine also remained online and even gained customers.41 When the NIN becomes fully operational,   
the government will have full control over the information available to the Iranian population,   
limiting the accessibility of foreign news and reducing Iran’s vulnerability to cyberattacks.42  
While many cyber intrusions are used to monitor and control the Iranian population and thus   
maintain the strength of the regime, Iran also conducts destructive cyberattacks. Tehran notably   
does not make a discernible distinction between operations carried out against domestic and   
foreign adversaries. The same cyber tools developed and used against domestic organizations and   
Iranian citizens have since been used against adversaries as disparate as the U.S. defense industry,   
Persian-language women’s development programs, and Saudi government institutions. The same   
threat actors also target both domestic and international organizations and individuals.43  
The same cyber tools developed and used against domestic   
organizations and Iranian citizens have since been used   
against adversaries as disparate as the U.S. defense industry,   
Persian-language women’s development programs, and Saudi   
government institutions. The same threat actors also target both   
domestic and international organizations and individuals.  
In conducting destructive cyberattacks, Iran tends to portray itself as a victim that is simply   
responding to an attack on its own infrastructure to “deflect attention away from its own actions.”44   
For example, upon discovery of the Stuxnet intrusion against its nuclear facilities in 2010, Iran   
launched a series of attacks against U.S. assets, including against dozens of U.S. banks and a small   
dam in New York.45 Similarly, in 2020 following a fire at its Natanz power plant that Iranian officials   
attributed to a cyberattack, Iran’s head of civilian defense said that Iran would retaliate against any   
country that carries out cyberattacks against its nuclear sites.46

**Page 15**

A Playbook for Winning the Cyber War | 10  
In its offensive operations, Iran’s brazenness and disregard for international norms makes the   
country a particularly dangerous adversary. Tehran does not shy away from targeting civilian critical   
infrastructure, having already attacked the financial sector, pipelines, dams, and water facilities,   
which “can enable actions that harm the public and cause devastating humanitarian consequences.”47   
While Iran has increasingly turned to cyber operations as a tool in its tool kit for irregular conflict,   
Tehran may not be ready to fully integrate cyber into active conflict operations. Tehran continues   
to support groups involved in conflicts in Gaza, Iraq, Yemen, and Syria, but cyber operations have   
not featured in those wars. Part of the reason is likely the difficulty of executing tactical cyber   
operations, which requires intensive coordination and seamless communication. Instead, Iran has   
continued to pursue cyber-enabled influence operations and cyber operations on the margins of   
conflict. Although past attacks in these conflicts have not been particularly damaging, Tehran’s   
rapidly developing tool kit may lead to more destabilizing and escalatory attacks in the future.  
Throughout the war in Gaza, a complex Iranian influence campaign called Emerald Divide has   
sought to “psychologically manipulate Israeli citizens to take real-world actions that exacerbate   
ideological divisions within Israeli society and undermine the Israeli government,” according to   
Sean Minor, a senior threat intelligence analyst at Insikt Group.48 While Emerald Divide has been   
operational since at least 2021, the group has focused on the ongoing conflict in Gaza since the   
attacks on October 7, 2023. One such effort, the “Tears of War” Telegram channel, posts content   
related to the Hamas-captured hostages and Israeli victims to encourage Israelis to partake in   
anti-government protests and raise internal conflict.49   
How Iran Approaches Deniability  
Tehran rarely claims responsibility for cyber operations and instead tends to emphasize its   
defensive capabilities while touting claims of victimhood.50 Overall, Iran provides conflicting   
information about its offensive cyber operations—it simultaneously burnishes its capabilities while   
consistently denying involvement in attacks.51  
Just as it does in other warfare domains, Tehran relies on proxies and front organizations to   
maintain a degree of separation and plausible deniability, which emboldens the government to   
vehemently deny involvement in cyber operations. In general, the use of proxies has been a key   
aspect of Iran’s military strategy since the Iranian Revolution. Tehran has a robust network of   
proxies such as Hezbollah and Hamas that it uses as channels for action in conflicts throughout   
the Middle East.52 Similarly, Tehran conducts many of its cyber operations using cyber proxies that   
disguise themselves as hacktivists or pan-Islamists. By doing so, Iran avoids definite attribution,   
preserving its claims of victimhood. However, cyber defenders have increasingly been able to   
identify hallmarks of IRGC and MOIS campaigns. For more information about proxy and front   
organizations, see page 23.

**Page 16**

Julia Dickson and Emily Harding | 11  
Implementation: Campaigns or Opportunism?  
While Iranian actors tend to be reactive, exploiting opportunities for cyberattacks as they arise,   
they are patient and persistent in their social engineering campaigns. Many of Iran’s cyber efforts   
are designed to be splashy and public, both making a political statement and causing actual   
damage. Those are generally presented as retaliatory attacks—activism attempting to right a social   
wrong. It is not clear, however, how far in advance Iran attempts to establish these accesses for   
later exploitation. In other words, which comes first, the desire to retaliate or the capability,   
held in reserve?  
Following Israel’s invasion of Gaza, Iran demonstrated its opportunistic tendencies to quickly react   
in support of Gaza. In one such attack, Malek Team, an Iranian actor likely associated with the   
MOIS, leaked personal data from an Israeli university. When publishing the data on Twitter, Malek   
Team used hashtags to support Hamas and later shifted messaging to belittle Israeli prime minister   
Benjamin Netanyahu. The group either took advantage of any vulnerability it found quickly or   
repurposed existing access to support its campaign against Israel, regardless of the relevance of the   
data or victim to the conflict.53 For more information about Iranian attacks during the war in Gaza,   
see the case study on page 36.  
Similarly, the 2023 Annual Threat Assessment of the U.S. Intelligence Community highlighted that   
“Iran’s opportunistic approach to cyberattacks makes critical infrastructure owners in the United   
States susceptible to being targeted by Tehran.”54 This warning came to fruition in November   
2023 when an Iranian cyber persona linked with the IRGC Cyber–Electronic Command targeted   
a programmable logic controller manufactured by Unitronics (an Israeli company) at a water   
utility in Pennsylvania. The group, known as CyberAv3ngers, left a warning on the screen of the   
device: “Every equipment ‘made in Israel’ is CyberAv3ngers legal target.” While the water utility   
has no intrinsic value to Iran, all poorly defended systems in adversary countries are potential   
targets, allowing Tehran to engage with adversaries without spending a significant amount of time   
carefully crafting a campaign. Even partially successful attacks that result in no significant damage   
or disruption of services are used in Iranian propaganda to further its strategic agenda.55 In this   
case, the extent of the attackers’ access prompted the water facility managers to switch to manual   
operations out of concern that safety was compromised.  
U.S. election infrastructure is another critical sector that Tehran has targeted in furtherance of its   
strategic goals. Similar to its initial attacks in support of Gaza, Iran’s 2020 campaign against U.S.   
election systems attempted to advance Tehran’s long-term strategic goals—to undermine Americans’   
faith in the U.S. electoral system, sow discord in American society, and “undercut the reelection   
prospects of President Trump,” according to an unclassified report by the U.S. National Intelligence   
Council.56 A press release published by the U.S. Department of the Treasury stated that Iranian   
hackers attempted to compromise 11 state voter websites but were only successful in exploiting one.   
Despite failing 10 times, Tehran’s single success had the potential to spread fear and undermine   
faith in electoral systems; it also allowed the country to download the personal information of over   
100,000 voters. Posing as a far-right group, hackers subsequently sent emails to tens of thousands   
of Democratic voters, including many whose data had been stolen from the successful attack,

**Page 17**

A Playbook for Winning the Cyber War | 12  
threatening violence if they did not vote for Trump.57 Iran has shown the capability to adapt and   
advance its tactics in other domains, suggesting that it will continue to learn from failures and grow   
their cyber capabilities.  
In addition, Iranian hackers claiming to be Proud Boys volunteers sent Facebook messages and   
emails to Republican members of Congress as well as people associated with the Trump campaign.   
According to the U.S. Department of the Treasury, the messages claimed that the Democratic Party   
was “planning to exploit ‘serious security vulnerabilities’ in state voter registration websites to ‘edit   
mail-in ballots or even register non-existent voters.’” The hackers also sent a video purporting to   
show someone fraudulently casting ballots via the Federal Voting Assistance Program for military   
and overseas voters.58 The fraud, however, never actually took place.  
While most attacks are opportunistic, Iranian hackers are known to invest considerable time and   
resources into developing advanced social engineering campaigns. Mandiant Intelligence, for   
instance, reported that to gain access to victims’ email accounts or install Android malware on their   
mobile devices, APT42 “uses highly targeted spear-phishing and social engineering techniques   
designed to build trust and rapport with their victims.”59 In May 2024, Mandiant reported that the   
group was “posing as journalists and event organizers . . . to deliver invitations to conferences   
or legitimate documents,” which allowed the APT to harvest credentials and gain access to   
cloud environments.60  
Cybersecurity researchers have also witnessed increased collaboration between Iranian-state   
affiliated actors, suggesting a degree of pre-planning. Two groups that Microsoft tracks as   
Storm-0861 and Storm-0842 collaborated on destructive cyberattacks in Israel and Albania. In both   
attacks, Storm-0861 provided initial access and Storm-0842 executed wiper malware. Similarly,   
Microsoft reported collaboration between an MOIS-affiliated group, Argius (Pink Sandstorm), and   
Hezbollah cyber units.61

**Page 18**

Julia Dickson and Emily Harding | 13  
Organization   
of Capabilities  
Who Are the Fighters?  
Two main organizations lead offensive cyber operations for the Iranian regime: the IRGC and the   
MOIS. The following section will discuss the IRGC, MOIS, and the APTs associated with each. This   
is not an exhaustive list, given that researchers have identified as many as 40 separate APTs, and   
it is still unclear how much their activities and personnel overlap. There is more publicly available   
information about the groups discussed below, many of which have conducted some of Iran’s more   
high-profile attacks.  
Figure 1: Iranian Offensive Cyber Actors  
Source: CSIS research.  
Pioneer Kitten  
Agruis  
Chrono  
Kitten  
Remix  
Kitten  
Static  
Kitten  
Helix  
Kitten  
Charming   
Kitten  
Reﬁned  
Kitten  
Imperial  
Kitten  
APT42  
Islamic Revolutionary Guard Corps  
(IRGC)  
Ministry of Intelligence and Security  
(MOIS)

**Page 19**

A Playbook for Winning the Cyber War | 14  
IRANIAN REVOLUTIONARY GUARD CORPS (IRGC)  
The IRGC is a branch of the Iranian armed forces that was established after the Iranian Revolution   
in 1979 to protect the new Islamic political system and regime. Since its establishment, the IRGC has   
taken on an exceedingly large role in executing Iran’s foreign policy, particularly via Iran’s covert,   
asymmetric operations abroad. The IRGC has ties to regional armed groups, including Hezbollah   
in Lebanon, militant groups in Iraq, and Hamas in Gaza. It has considerable influence in domestic   
politics as well because key positions are appointed by the country’s supreme leader, Ali Khamenei,   
and are answerable to him, bypassing the president’s office.62 The United States designated the IRGC   
as a terrorist organization in 2019.63  
The IRGC is composed of ground, naval, land, and air forces as well as cyber-focused units,   
which have conducted cyberattacks against many targets in Israel, the United States, and Saudi   
Arabia, among others. The IRGC also is the parent organization of the Basij, a civilian paramilitary   
organization that manages a legion of cyberwar volunteers recruited from universities and   
religious schools who also act as a proxy hacker force. While the exact number is unknown, Iranian   
leadership claims to have 120,000 basij cyber warriors. The volunteers are sometimes referred to as   
“cyber war commandos.”64  
APTs associated with the IRGC include Refined Kitten, Charming Kitten, Imperial Kitten, APT42,   
and Pioneer Kitten, each of which are detailed below.  
Refined Kitten  
Refined Kitten has been active since at least 2013 and is likely tied to the IRGC, according to   
CrowdStrike.65 The group is known for gathering intelligence on companies in the United States,   
Saudi Arabia, and South Korea, with a particular interest in the military and commercial aviation   
sectors and the energy sector, especially companies with ties to petrochemical production.66 These   
targets are in line with Iranian strategic interests, which include gaining insights into Saudi military   
aviation capabilities, supporting Iranian decisionmaking regarding Saudi Arabia, and expanding   
Iran’s petrochemical production to grow its competitiveness within the region. Although the group’s   
activities mainly focus on intelligence gathering, there have been suspected links between Refined   
Kitten and destructive attacks such as the Shamoon wiper-malware attacks in 2018.67  
Refined Kitten is known for using relatively sophisticated tactics, including custom-built malware   
and advanced social engineering strategies. This adversary often uses targeted spear-phishing   
campaigns to gain initial access. In one instance, Refined Kitten sent recruitment themed emails   
to employees of aviation-related organizations that contained links to malicious application files.   
Table 2: Aliases of Refined Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Refined Kitten  
APT33  
HOLMIUM  
Peach   
Sandstorm  
Cobalt Trinity  
Elfin

**Page 20**

Julia Dickson and Emily Harding | 15  
These files also contained job descriptions and links to legitimate job postings that were relevant to   
the targeted individuals.68  
Notable attacks by Refined Kitten include the following:  
    
▪  
In 2023, Microsoft reported that Refined Kitten was carrying out password spray activity   
against thousands of organizations in the satellite, defense, and pharmaceutical sectors,   
which was likely an attempt to gain initial access and collect intelligence in line with   
Iranian strategic interests. When these campaigns were successful, Refined Kitten used “a   
combination of publicly available and custom tools for discovery, persistence, and lateral   
movement,” with a few instances of data exfiltration reported.69   
    
▪  
From mid-2016 to 2017, Refined Kitten compromised a U.S. aerospace organization and   
targeted a Saudi corporation with aviation holdings, according to Mandiant. To do so, the   
group sent targeted spear-phishing emails and registered domains that masqueraded as   
Saudi aviation and Western organizations.70  
    
▪  
According to a 2018 report by McAfee, Refined Kitten is responsible for Shamoon Version   
3 wiper-malware attacks in December 2018 that used a supply chain attack to target   
organizations in the Middle East through their suppliers in Europe. To gain initial access,   
Refined Kitten hackers created websites that closely resembled legitimate job-posting   
websites, many of which were related to the Middle Eastern energy sector. Some of the   
websites contained malicious application files, while others had victims log in using their   
corporate credentials.71 Similarly, in September 2017, Mandiant (then FireEye) assessed that   
Refined Kitten likely has ties to earlier uses of Shamoon malware.72  
Charming Kitten  
Charming Kitten is an Iranian APT, likely affiliated with the IRGC, that is known for targeting   
military, diplomatic, and government personnel; private companies in the media, energy, and   
telecommunications sectors; and organizations and companies in the defense industrial base.73   
The group has been active since at least 2014 and typically conducts long-term, resource-intensive   
operations to collect intelligence and surveil Iranians and foreign citizens who have strategic value.74  
According to Mandiant, Charming Kitten has “historically relied on marginally sophisticated tools   
. . . suggesting a relatively nascent development capability. However, the breadth and scope of [its]   
operations, particularly as it relates to its complex social engineering efforts, likely indicates that   
the group is well resourced in other areas.”75 The group relies on spear phishing to gain initial access   
Table 3: Aliases of Charming Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Charming   
Kitten  
APT35  
PHOSPHORUS  
Mint Sandstorm  
Cobalt Illusion  
Magic Hound

**Page 21**

A Playbook for Winning the Cyber War | 16  
and occasionally utilizes strategic web compromises and password spray attacks against externally   
facing web applications.  
Attacks attributed to Charming Kitten include the following:  
    
▪  
In February 2017, Palo Alto Networks reported that Charming Kitten targeted organizations   
that are either based in Saudi Arabia or have interests in Riyadh in the energy, government,   
and technology sectors. The campaign, dating to mid-2016, was focused on espionage.76   
Charming Kitten disguised malicious files as holiday greeting cards, job offers, and   
government documents from Saudi Arabia’s Ministry of Health and Ministry of Commerce   
and used custom tools, including “droppers, downloaders, executable loaders, document   
loaders, and IRC bots,” to carry out the campaign.77   
    
▪  
In 2020, the group targeted medical research organizations in Israel, focusing particularly on   
targets in oncology, genetics, and neurology.78  
    
▪  
In September 2020, Microsoft reported that Charming Kitten “continued to attack the   
personal accounts of people associated with the Donald J. Trump for President campaign.”   
Between May and June 2020, the threat actor attempted to sign in to administration officials’   
and campaign staffs’ personal or work accounts but was unsuccessful.79  
    
▪  
In January 2023, Germany’s Federal Office for the Protection of the Constitution warned that,   
since the end of 2022, Charming Kitten had been conducting cyberattacks against Iranian   
dissident organizations and individuals such as lawyers and human rights activists residing   
both inside and outside of Iran.80 The group used advanced spear-phishing tactics to gain   
access to targets’ accounts.81  
Nemesis Kitten is generally classified as a sub-group of Charming Kitten. For more information   
about Nemesis Kitten, see the section on Najee Technology and Afkar Systems on page 25.  
Imperial Kitten  
Imperial Kitten has been active since at least 2017 and, according to CrowdStrike, is affiliated with   
the IRGC. Mandiant tracks Imperial Kitten’s activity under APT35 (the same as Charming Kitten)   
and UNC1549. Microsoft also tracks this threat actor under two different names, Crimson Sandstorm   
and Smoke Sandstorm.82 Imperial Kitten’s activity is characterized by its use of social engineering   
techniques, specifically creating false social media profiles and using job recruitment–themed   
content to deliver custom malware. This APT has targeted multiple industries, including defense,   
Table 4: Aliases of Imperial Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Imperial Kitten  
APT35,   
UNC1549  
CURIUM,   
BOHRIUM  
Crimson   
Sandstorm,   
Smoke   
Sandstorm  
Cobalt Fireside  
Tortoiseshell

**Page 22**

Julia Dickson and Emily Harding | 17  
technology, telecommunications, maritime, energy, and consulting companies.83 Examples of such   
activities include the following:  
    
▪  
In November 2023, CrowdStrike reported that Imperial Kitten conducted a series of   
cyberattacks against organizations in the transportation, logistics, and technology   
sectors the month prior. These attacks utilized public scanning tools, one-day exploits,   
SQL injection, and stolen VPN credentials for initial access before moving laterally and   
exfiltrating data. Similarly, between 2022 and 2023, Imperial Kitten conducted strategic web   
compromise operations, targeting organizations in the same sectors.84  
    
▪  
In February 2024, Mandiant reported that Imperial Kitten was targeting the aerospace,   
aviation, and defense industries of countries in the Middle East, including Israel and   
the United Arab Emirates, as well as potentially Turkey, India, and Albania. The threat   
group used a fake recruiting website hosting a malicious payload to do so. According to   
Mandiant, the link between these attacks and the IRGC is “noteworthy given the focus on   
defense-related entities and the recent tensions with Iran in light of the Israel-Hamas war.”85  
APT42  
APT42 has been active since at least 2015 and is responsible for at least 30 confirmed operations.   
Mandiant previously tracked APT42 as UNC788 and assesses with moderate confidence that the   
group operates on behalf of the IRGC Intelligence Organization. Other cybersecurity researchers   
combine Charming Kitten’s (APT35) activity with that of APT42, but Mandiant assesses with   
moderate confidence that Charming Kitten and APT42 are separate groups that both “operate   
on behalf of the IRGC but originate from different missions and contracts or contractors based   
on substantial differences in their respective targeting patterns and tactics, techniques and   
procedures.” Similarly, though Microsoft reports a connection between Nemesis Kitten (UNC2448)   
and APT42, Mandiant “has not observed any technical overlaps between APT42 and UNC2448.”86  
APT42 has targeted the personal and corporate email accounts of current and former Iranian   
government officials, policymakers, political figures, members of the Iranian diaspora, opposition   
groups, journalists, and academics. It also targets organizations in the following sectors: civil   
society, education, government, healthcare, legal, manufacturing, media, entertainment, and   
pharmaceutical. However, unlike other groups associated with the IRGC, APT42 does not target the   
defense industrial base or focus on the collection of personally identifiable information. Instead,   
it seeks out “enemies or opponents of the regime, specifically gaining access to their personal and   
mobile devices.” The group relies primarily on highly targeted social engineering efforts to build   
trust with their victims. APT42 has targeted organizations and individuals in at least 14 countries,   
Table 5: Aliases of APT42  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Charming   
Kitten  
APT42  
PHOSPHORUS  
Mint   
Sandstorm  
Cobalt Illusion  
Damselfly, Crooked   
Charms

**Page 23**

A Playbook for Winning the Cyber War | 18  
including Australia and the United States, as well as countries in the Middle East and Europe.87   
Notable attacks include the following:  
    
▪  
In May 2024, Mandiant reported that APT42 was observed masquerading as journalists and event   
organizers. The group spent considerable time building rapport with their victims, typically   
individuals perceived as being a threat to the regime, such as NGO leaders and human rights   
activists. APT42 eventually sent a link to a legitimate conference invitation or other document,   
which prompted victims to enter credentials. Upon harvesting credentials, the group gained   
access to cloud environments and covertly exfiltrated data of strategic value to Iran.88  
    
▪  
In another campaign beginning in 2021, APT42 impersonated news sources such as the   
Washington Post, The Economist, and the Jerusalem Post to target journalists and researchers   
with spear-phishing campaigns.89  
MINISTRY OF INTELLIGENCE AND SECURITY (MOIS)  
The MOIS (VEVAK in Farsi) is one of the two most powerful intelligence branches in Iran, alongside   
the IRGC Intelligence Organization. The MOIS is the primary civilian intelligence organization, and   
all other intelligence services are required to share information with the MOIS. Notably, the MOIS   
reports to the president rather than the supreme leader and “is assessed to be more technical and   
less ideology-driven than IRGC leaders.”90  
The MOIS’s main priority is to collect domestic intelligence. To do so it “spies on Iranians   
abroad, collects intelligence on other governments, counters foreign intelligence plots, and   
works with allied intelligence agencies.”91 The organization is known to be responsible for signals   
intelligence and collecting information from electronic communications.  
APTs associated with the MOIS include Static Kitten, Helix Kitten, Remix Kitten, Agrius, and Chrono   
Kitten. The section below details these APTs.  
Static Kitten   
Static Kitten has been active since at least 2017. In January 2022, U.S. Cyber Command reported   
that this APT is a “subordinate element” within the MOIS.92 This adversary is known for targeting   
organizations located in the Middle East and Eurasia, including telecommunications, local   
government, defense, oil, and natural gas companies. Static Kitten is most known for cyber   
espionage campaigns and intellectual property (IP) theft but is believed to occasionally deploy   
ransomware, perhaps to cover its tracks.93 According to Microsoft, Static Kitten has collaborated   
with another threat actor, tracked as DEV-1084 (also known as Storm-1084 and as the DarkBit   
persona); Static Kitten gains initial access before DEV-1084 carries out destructive actions.94 Static   
Table 6: Aliases of Static Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Static Kitten  
UNC3313  
TEMP.Zargos  
MERCURY  
Mango   
Sandstorm  
Cobalt Ulster  
MuddyWater

**Page 24**

Julia Dickson and Emily Harding | 19  
Kitten typically exploits publicly reported vulnerabilities and mainly uses open-source tools and   
strategies.95 Notable attacks by Static Kitten include the following:  
    
▪  
In February 2022, Static Kitten attacked what Mandiant describes as a “Middle Eastern   
government.” According to Mandiant, Static Kitten gained access to the system through a   
targeted phishing email. The group moved quickly and used new, targeted malware that also   
possessed backdoor functionalities and publicly available remote-access software. Mandiant   
assessed that Static Kitten “conducts surveillance and collects strategic information to   
support Iranian interests and decision-making.”96  
    
▪  
In early November 2023, Deep Instinct’s Threat Research Team reported that Static Kitten   
unleashed a new social engineering campaign aimed at Israeli organizations. The group   
targeted two Israeli organizations with spear-phishing emails and used subsequent access to   
conduct reconnaissance.97  
Helix Kitten  
Helix Kitten has been active since at least 2015 and is known to target organizations in the   
aerospace, energy, financial, government, hospitality, and telecommunications industries across   
the Middle Eastern region, mostly for espionage purposes. According to the Cybersecurity and   
Infrastructure Security Agency (CISA), Helix Kitten works on behalf of the Iranian government,   
likely the MOIS.98 According to a Palo Alto Networks report, Helix Kitten attacks are “not   
particularly sophisticated” but are “extremely persistent in the pursuit of their mission objective,”   
and have become more sophisticated over time, following the general trend of Iranian cyber   
capabilities.99 Notable attacks by Helix Kitten include the following:  
    
▪  
In an interesting attack in 2019, Venomous Bear, a Russian APT that has been attributed to   
the Russia’s Federal Security Service (FSB), hijacked Helix Kitten’s infrastructure and used   
it to deliver malware against a target in the Middle East. Symantec found no evidence to   
suggest that the two groups were collaborating and instead assessed that Venomous Bear’s   
use of Helix Kitten’s infrastructure “appears to have been a hostile takeover.”100  
    
▪  
During the 2023 annual Cyber Security Weekend for the Middle East, Türkiye, and Africa,   
Kaspersky researchers warned of increased IT supply chain attacks by Helix Kitten that   
targeted high-profile government entities to collect credentials and sensitive data about   
their targets. The APT used social engineering techniques and exploited software and other   
technical vulnerabilities to gain initial access, and Kaspersky reported that “the group has   
updated their arsenal, resorting to persistent, stealthier ways of infiltrating their targets   
through third-party IT companies.”101  
Table 7: Aliases of Helix Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Helix Kitten  
APT34  
EUROPIUM  
Hazel   
Sandstorm  
Cobalt Gypsy  
OilRig

**Page 25**

A Playbook for Winning the Cyber War | 20  
    
▪  
In August 2023, Helix Kitten attempted to use a supply chain attack to gain access to targets   
within the government of the United Arab Emirates (UAE). The group created a fake IT   
company website and sent a malicious job recruitment form to a target IT company; the   
form, when opened, deployed malware to collect sensitive information. From there, Helix   
Kitten looked to target government clients, “using the victim IT group’s email infrastructure   
for command-and-control communication and data exfiltration.”102  
Remix Kitten   
Remix Kitten is an Iranian APT known to target the Middle East and the United States. The group   
has been active since at least 2014 and has a particular focus on the telecommunications sector   
as well as the travel and hospitality industries. Remix Kitten has engaged in the widespread theft   
of personally identifiable information in order to “perform monitoring, tracking, or surveillance   
operations against individuals, collect proprietary or customer data for commercial or operational   
purposes that serve strategic requirements related to national priorities, or create additional   
accesses and vectors to facilitate future campaigns.”103 According to the U.S. Department of the   
Treasury, Remix Kitten is “owned or controlled” by the MOIS.104 Notable attacks by Remix Kitten   
include the following:  
    
▪  
According to Symantec, Remix Kitten compromised a major telecommunications services   
provider in the Middle East in 2017 and likely attempted to attack a major travel reservations   
firm. The same year, Remix Kitten attacked nine organizations in Israel, Jordan, the UAE,   
Saudi Arabia, and Türkiye using seven new tools. The attacks hit airlines, aircraft services,   
document management software, software and IT services companies working with the   
air and sea transport sectors, engineering consultancies, and payroll services to “facilitate   
widescale surveillance of targets.”105  
    
▪  
Remix Kitten targeted air transportation organizations and government entities in Kuwait   
and Saudi Arabia in a campaign that began in 2018. Researchers believe Remix Kitten gained   
initial access through a social engineering campaign, and the attacks used custom-built tools   
and living-off-the-land tactics. The attacks on Kuwait were more sophisticated, as the hackers   
were able to move laterally.106  
Table 8: Aliases of Remix Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)   
Microsoft (new)  
Secureworks  
Other  
Remix Kitten  
APT39  
DEV-0589  
Storm-0589  
Cobalt Hickman  
Chafer

**Page 26**

Julia Dickson and Emily Harding | 21  
Agrius  
Agrius has been active since 2020 and is known for conducting destructive wiper and fake   
ransomware attacks, mainly against Israeli organizations. It has been attributed to the MOIS.107   
According to Palo Alto Networks, Agrius steals sensitive information, posts it on Telegram   
and Instagram channels, and wipes as many endpoints as possible. This adversary has both   
developed custom tools and used known hacking techniques.108 Notable attacks by Agrius   
include the following:  
    
▪  
Palto Alto Networks found that Agrius targeted the Israeli higher education and technology   
sectors throughout 2023, stealing personal information such as intellectual property   
and personally identifiable information and disabling endpoints using custom wipers.   
The group then posted the stolen data on social media and Telegram channels. Agrius   
hackers exploited internet-facing web servers, then deployed multiple web shells to get a   
foothold in a network.109  
Chrono Kitten  
Chrono Kitten has been active since at least 2018 and is known for targeting oil, gas, and   
telecommunications companies in Africa and the Middle East for espionage purposes. While some   
cybersecurity researchers combine this group with Helix Kitten, according to MITRE ATT&CK,   
this group’s tactics, techniques, and procedures are similar to those used by Helix Kitten and   
Refined Kitten, but it is tracked separately due to differences in victims and tools.110 Notable attacks   
include the following:  
    
▪  
In 2019, Secureworks reported that Chrono Kitten focused on South African targets   
in mid-2018, and the group launched a campaign against Middle Eastern oil and gas   
organizations in May 2019. Chrono Kitten gains initial access using account credentials   
obtained through password spraying or brute-force attacks. The group then sends   
spear-phishing emails with malicious Excel attachments from the compromised accounts.111  
    
▪  
In August 2021, ClearSky, an Israeli cybersecurity company, reported a campaign by Chrono   
Kitten focusing on Israeli IT companies.112  
Table 9: Aliases of Agrius  
Microsoft (old)  
Microsoft (new)  
Other  
AMERICUM  
DEV-0022  
Pink Sandstorm  
Agrius, Agonizing Serpens  
Table 10: Aliases of Chrono Kitten  
CrowdStrike  
Microsoft (old)  
Microsoft (new)  
Secureworks  
Others  
Chrono Kitten  
DEV-0133  
Storm-0133  
Cobalt Lyceum  
Siamese Kitten,   
Lyceum, HEXANE

**Page 27**

A Playbook for Winning the Cyber War | 22  
UNCLEAR IRANIAN GOVERNMENT AFFILIATION  
Pioneer Kitten  
Pioneer Kitten has been active since at least 2017, targeting mainly North American and Israeli   
organizations in the “technology, government, defense, healthcare, aviation, media, academic,   
engineering, consulting and professional services, chemical, manufacturing, financial services,   
insurance, and retail” sectors. Pioneer Kitten is likely connected to the Iranian government, but   
cybersecurity researchers from CrowdStrike assess that this APT is most likely a “contract element   
operating in support of the Iranian government, rather than one operated by the government itself”   
due to certain behaviors and traits. Pioneer Kitten potentially overlaps with the IRGC’s Refined   
Kitten as well as the MOIS’s Helix Kitten and Remix Kitten, but “CrowdStrike intelligence considers   
these claims to be circumstantial and lacking in sufficient corroborative data to enable confirmation   
of such relationships.”113 Attacks by Pioneer Kitten include the following:  
    
▪  
In September 2020, CISA reported that Pioneer Kitten targeted U.S. organizations in the   
information technology, government, healthcare, financial, insurance, and media sectors.   
The group “conducts mass-scanning tools . . . to identify open ports . . . [then] exploits CVEs   
[common vulnerabilities and exposures] related to VPN infrastructure to gain initial access   
to a targeted network.” The threat actor then exfiltrated data and has been observed selling   
stolen data on an online hacker forum.114  
    
▪  
Pioneer Kitten is likely responsible for a 2020 attack on a local government website that was   
to report the 2020 election results. The U.S. military discovered the breach. and disrupted   
the attack before the results were finalized.115  
OTHER GOVERNMENT ENTITIES  
Other government entities that have a role in Tehran’s defensive cyber operations   
include the following:  
    
▪  
Supreme Council of Cyberspace (SCC): Established by Supreme Leader Ayatollah Ali   
Khamenei in 2013, the SCC is responsible for managing cyberspace policy, coordinating   
offensive and defensive cyber operations, and blocking websites, including social media   
sites. It also has a role in various censorship efforts.116 All state agencies are required to   
cooperate with the SCC, so it has almost complete control over Iran’s domestic cyberspace.117   
    
▪  
National Cyberspace Center: The National Cyberspace Center is owned or controlled by   
the SCC and is responsible for developing tactics to control Iran’s domestic information   
space and “preparing for a cultural war” between Iran and the West.118 It has prevented   
Iranians from using VPNs to access blocked content.119  
Table 11: Aliases of Pioneer Kitten  
CrowdStrike  
Mandiant  
Microsoft (old)  
Microsoft   
(new)  
Secureworks  
Other  
Pioneer Kitten  
UNC757  
RUBIDIUM  
Lemon   
Sandstorm  
Cobalt   
Foxglove  
Fox Kitten

**Page 28**

Julia Dickson and Emily Harding | 23  
    
▪  
National Passive Defense Organization: A quasi-military body, the National Passive   
Defense Organization (NPDO) is in charge of making Iran’s critical infrastructure more   
resilient. One of the NPDO’s main roles is to use “all national cyber and non-cyber resources   
to deter, prevent, deny, identify, and effectively counter any cyberattack against . . . Iran’s   
national infrastructure by either hostile foreign states or groups supported by them.” In   
addition to defense, the NPDO also helps coordinate citizen surveillance and supposedly   
works with the IRGC to conduct offensive cyberattacks.120  
NONGOVERNMENTAL  
In conducting computer network operations, Tehran often relies on a diverse ecosystem of cyber   
actors that act on behalf of the Iranian government. A proxy-based approach is a feature of Iranian   
cyber operations and reflects Tehran’s approach in conflict zones like Syria and Yemen, where Iran   
employs both direct and indirect means to exert influence on decisionmaking. Assessments of the   
Iranian state’s control over its cyber proxies point to cases where the groups operate without strict   
restraints. The means and logistics of a cyber response are often as much determined by the proxies   
as they are by the state.121 The use of proxies provides Iran with a level of deniability and the ability   
to maintain that it is a victim in the global cyberwar.122  
Proxies and Front Organizations  
Iranian companies are known to have perpetrated attacks, in affiliation with the IRGC and MOIS,   
against a range of targets, including universities, election apparatuses, and critical infrastructure.   
The section below describes several proxy organizations that have been responsible for   
high-profile hacks.  
mabna institute  
Since its founding in 2013, the Mabna Institute has helped Iranian universities and other research   
institutions steal foreign scientific resources. The Mabna Institute employs and hires individuals that   
use cyber operations to steal intellectual property, academic research, emails, and other sensitive   
information on behalf of both the Iranian government and private companies. In March 2018, the   
U.S. Department of Justice indicted nine individuals working at the Mabna Institute for conducting   
cyber operations on behalf of the IRGC. They are believed to have hacked 144 universities and 36   
private companies in the United States, 176 foreign universities in 21 different countries, and 11   
foreign private companies.123

**Page 29**

A Playbook for Winning the Cyber War | 24  
Mabna hackers wanted by the Federal Bureau of Investigation.  
Source: “Iranian Mabna Hackers,” Federal Bureau of Investigation, March 23, 2018, https://www.fbi.gov/wanted/cyber/  
iranian-mabna-hackers.

**Page 30**

Julia Dickson and Emily Harding | 25  
najee technology hooshman fater llc and afkar system yazd company  
The U.S. Department of the Treasury sanctioned both Najee Technology and Akfar System in   
September 2022 for “their roles in conducting malicious cyber acts, including ransomware   
activity” in affiliation with the IRGC Intelligence Organization. According to the press release, these   
cyber actors had been active in the United States and other countries, particularly in the Middle   
East, since at least 2020. They have launched campaigns against personnel working in defense,   
diplomacy, and government as well as private companies in the media, energy, business services,   
and telecommunications sectors.124  
Microsoft Threat Intelligence tracks these two companies under the name DEV-0270—also known   
as Nemesis Kitten and UNC2448—and it is thought to be a sub-actor of Charming Kitten. According   
to Microsoft, while Nemesis Kitten conducts cyberattacks on behalf of the government of Iran,   
“judging from their geographic and sectorial targeting, which often lacked a strategic value for the   
regime,” some of their attacks are likely “a form of moonlighting for personal or company-specific   
revenue generation.”125 Notable attacks by the group include the following:  
    
▪  
In February 2021, cyber actors hacked a New Jersey municipality. After gaining access,   
employees from the two companies created unauthorized accounts, escalated their   
privileges, and moved laterally to other parts of the network. They also established   
persistent remote access to a domain registered by the owner, managing director, and   
chairman of the board of Najee Technology.  
    
▪  
In March and April 2021, hackers affiliated with the companies launched their first known   
ransomware activities against several small businesses, including a law firm, an accounting   
firm, and a construction contractor.  
    
▪  
In June 2021, a group, composed of employees of the two companies, gained access to   
a hospital’s supervisory control and data acquisition systems. They exfiltrated data and   
encrypted at least one device. U.S. government law enforcement partners were able to notify   
the hospital of the attack before it impacted patient care.126  
emennet pasargad  
Emennet Pasargad is an Iranian cyber company that was formerly known as Eeleyanet Gostar   
and Net Peygard Samavat Company. Microsoft tracks the company as Cotton Sandstorm (formerly   
NEPTUNIUM). In 2019, the U.S. Department of the Treasury sanctioned the Net Peygard Samavat   
Company for its involvement in a malicious cyber campaign that aimed to gain access to and   
implant malware on the systems of U.S. counterintelligence agents. At that time, the company was   
noted to work with the MOIS and the IRGC Cyber Electronic Command (IRGC-CEC). The company   
subsequently rebranded to Emennet Pasargad in an attempt to evade U.S. sanctions.127  
Since at least 2020, Emennet Pasargad has targeted companies, primarily in Israel, using   
cyber-enabled information operations, including data theft and the subsequent leak of data,   
sometimes followed by the deployment of destructive encryption malware. To avoid attribution,   
Emennet Pasargad conducted these campaigns under fake personas, including posing as hacktivist   
or cybercriminal groups. For example, between 2020 and 2022, Emennet Pasargad operated under

**Page 31**

A Playbook for Winning the Cyber War | 26  
the persona “Hackers of Savior” in multiple campaigns against Israel. In 2021, the group used the   
persona “Deus” while targeting an Israeli call service center.128  
In 2021, the Treasury Department sanctioned Emennet Pasargad for its attempts to interfere in   
the 2020 U.S. elections on behalf of the Iranian government. Between August and November   
2020, the company “executed an online operation to intimidate and influence American voters,   
and to undermine voter confidence and sow discord.” Hackers obtained voter information, sent   
threatening emails to voters, and created disinformation campaigns related to election security.   
They also obtained access to accounts of media entities, which gave them the ability to edit and   
create fake content, but the Federal Bureau of Investigation managed to thwart that access before it   
was used.129 Emennet Pasargad actors also claimed affiliation with the Proud Boys.130  
Other notable companies include the following:  
    
▪  
Rana Intelligence Computing Company: The government of Iran used this front company   
to target Iranian dissidents, journalists, and international companies in the travel sector as   
well as the government networks of Iran’s neighboring countries and foreign organizations in   
the academic, travel, and telecommunications sectors. Individuals working at Rana provided   
support for MOIS cyberattacks.131  
    
▪  
ITSecTeam and MERSAD: Seven Iranian individuals who worked at these two companies   
were indicted in March 2016 on computer hacking charges. They performed work for the   
Iranian government, including the IRGC, and were indicted for their involvement in an   
extensive campaign that included over 176 days of DDoS attacks primarily against targets   
in the U.S. financial sector. The campaign began in December 2011, with attacks occurring   
sporadically until September 2012, when hackers began conducting attacks almost every   
week. The campaign lasted until mid-2013 and was able to disable bank websites and prevent   
customers from accessing their accounts online.132  
    
▪  
Ravin Academy: The Ravin Academy is a cybersecurity and hacking training school from   
which the MOIS recruits. It also assists the MOIS with a range of needs such as information   
security training, threat hunting, digital forensics, malware analysis, penetration training,   
and reverse engineering.133  
Hacktivist Groups  
Iran’s hacktivist network is constantly evolving and growing. In particular, since Hamas’s attack   
on Israel on October 7, 2023, and Israel’s subsequent invasion of Gaza, Iranian hacktivists have   
been increasing their attacks against both Israeli and non-Israeli targets, especially targets in the   
United States. The Iranian government hides behind hacktivist organizations as they do with front   
organizations. The section below details some of the most well-known hacktivist groups.  
cyberav3ngers  
CyberAv3ngers is a hacktivist group that has been active since at least February 2022 but came to   
the fore during the Israel-Hamas conflict. While most cybersecurity researchers track this group as a   
hacktivist group, CISA classifies CyberAv3ngers as an IRGC-affiliated APT.134 The group is particularly   
active on social media and has claimed several attacks against critical infrastructure sectors,

**Page 32**

Julia Dickson and Emily Harding | 27  
often publicizing both actual and overstated successes. For example, some of their claims about   
compromising Israeli infrastructure have been proven false.135  
In a notable attack in November 2023, CyberAv3ngers targeted a municipal water authority in   
Pennsylvania. The hackers shut down a device that monitors and regulates water pressure at a   
pumping station, claiming the attack was meant to target the Israeli company, Unitronics, the maker   
of the industrial control system. Luckily, the staff switched to manual pumping quickly, and there   
was no impact on the water supply or on the health of the residents who rely on the company’s   
water and sewer services. CyberAv3ngers has also reportedly targeted a brewery in Pittsburgh, an   
aquarium, Israel’s railway infrastructure, and several Israeli water facilities.136  
haghjoyan  
Haghjoyan is another Iranian hacktivist group that emerged during the Israel-Gaza conflict. The   
group self-identifies as “Iran’s cyber army” on their popular Telegram channel, which had over   
40,000 subscribers at one point (see the images on page 28). Haghjoyan’s early attacks primarily   
targeted Israel, but the group’s focus has expanded to include the United States. The group is   
known for focusing on data leaks, defacement attacks, and propaganda. In one notable attack,   
Haghjoyan claimed to have targeted several Israeli water pumps, electricity distribution units, and   
virtual network computing systems at gas stations, highlighting the dangerous reality that this group   
could disrupt critical infrastructure.137  
cyber toufan al-aqsa  
Cyber Toufan Al-Aqsa (“Toufan” means flood in Arabic and is very likely a reference to Hamas’s   
October 7th attack on Israel, known as “Toufan Al-Aqsa”) is a relatively new hacktivist group that   
only recently emerged, in November 2023, but has already managed to attack more than 100   
Israeli organizations. According to SOCRadar, the group’s operations “bear the hallmarks of a   
sophisticated entity, potentially state-sponsored.”138 Cyber Toufan has been able to rapidly rise in   
notoriety and carry out complex cyberattacks that “suggest a level of support and resources that   
are not typically available to independent hacker collectives.”139 The group has leaked sensitive   
data from private companies and Israeli government targets, including the Ministry of Health, the   
Ministry of Welfare and Social Security, and Max Security (an Israeli cybersecurity company); Israeli   
branches of multinational companies such as Ikea, ACE Hardware, and Toyota; and companies that   
did business with Israeli companies such as Berkshire eSupply and SpaceX.140 Cyber Toufan’s wiper   
malware has caused significant damage to many of these organizations, and the group is known for   
spreading follow-on attacks down the supply chain.  
The vast array of these actors is telling. Iran has a variety of tools to choose from and is willing to   
deploy a range of tools and actors against several consistent targets: the United States, Israel, and   
the Gulf states. These attacks also show determination and persistence in the tactics, techniques,   
and procedures of these actors.

**Page 33**

A Playbook for Winning the Cyber War | 28  
Screenshots of Haghjoyan’s Telegram distributing stolen data of alleged CIA and Mossad employees.  
Source: Haghjoyan, Telegram, Screenshot, Haghjoyan distributes CIA and Mossad personnel data. February 16, 2024.

**Page 34**

Case Study 1  
Deserts vs. Sands   
“Do you see that desert out there? I want to show you something.” You pick up your cell   
phone and you call somewhere in Nebraska and you say, “Ok let it go.” So there’s an   
atomic weapon, goes over ballistic missiles, the middle of the [Iranian] desert, that doesn’t   
hurt a soul. . . . Then you say, “See? The next one is in the middle of Tehran. So, we mean   
business. You want to be wiped out? Go ahead and take a tough position and continue   
with your nuclear development.”  
—Sheldon Adelstein, 2013141  
These comments from Sheldon Adelstein, the owner of the Sands Casino in Las Vegas, from a 2013   
panel sparked outrage in Tehran. Adelstein had been asked how he would handle the ongoing talks   
with Iran about its nuclear program, to which he casually proposed that the United States launch   
a nuclear weapon at Iran, instead of pursuing diplomatic negotiations, to send a message and get   
the country to stop pursuing its own nuclear program.142 A few months later, in early 2014, Tehran   
retaliated with a malware bomb aimed at his casino.143  
The attack on the Sands Casino was not particularly sophisticated—it was a brute force password   
attack on a smaller casino. Tehran then used that access to find the credentials of a systems   
engineer and plant the malware. The attack destroyed about three-quarters of the casino’s   
Las Vegas servers, and cost the company an estimated $40 million.144 A year later, Director   
of National Intelligence James Clapper attributed the hack to the Iranian government in a   
congressional testimony.145  
Julia Dickson and Emily Harding | 29

**Page 35**

A Playbook for Winning the Cyber War | 30  
This attack set a dangerous precedent, demonstrating Iran’s willingness to target privately   
held companies, similar to North Korea’s attacks on Sony Pictures only a year later.146 The U.S.   
government was not the cavalry, coming to help. Adelstein’s comments were his own, and even   
though the attacker was a nation-state, the U.S. government did not view protecting the Sands   
Casino as its responsibility. The business recovered, but Tehran was able to exact a heavy cost.  
In 2013, Iran’s cyber capability was still new. In the years since, however, Tehran’s cyber activity   
has grown bolder and more ambitious, from DDoS attacks to wiper malware to an attempt to   
undermine the 2020 and 2024 U.S. elections.

**Page 36**

Case Study 2  
Tehran Targets Tirana  
I  
n 2022, Tehran hit Albania with perhaps the most aggressive and disruptive cyberattacks   
against a foreign government during peacetime to date. In response, Tirana made the   
unprecedented decision to fully sever diplomatic ties with Tehran.147 The attacks, part of Iran’s   
larger foreign policy strategy, aimed to retaliate against Albania for offering refuge to thousands of   
members of the People’s Mujahedeen of Iran (Mujahedeen-e-Khalq, or MEK), an Iranian opposition   
movement that Tehran considers a terrorist organization and a potential threat to the regime.   
Tirana’s 2013 offer of refuge entangled Tirana in the geopolitical standoff between the United States   
and Iran.148 In its devastating cyberattacks on Albania, Tehran sent a clear signal that it would seek   
revenge against those who act against its interests.  
On July 15, 2022, Iranian cyber actors calling themselves HomeLand Justice hit the government of   
Albania with a destructive cyberattack that shut down government services and websites, including   
the e-Albania portal which then offered 1,225 electronic services to Albanian citizens.149 Several   
groups, all of which Microsoft linked to MOIS-affiliated Helix Kitten, conducted the attack. A group   
Microsoft tracks as DEV-0861 gained initial access to the network in May 2021 and maintained   
continuous network access for over a year. Throughout that time, DEV-0861 and DEV-0166 accessed   
and exfiltrated data and harvested credentials from Albanian government networks while moving   
laterally. Another MOIS-affiliated group, which Microsoft tracks as DEV-0842, deployed both the   
ransomware and wiper malware (See Figure 2 on page 33). The ransomware image contained   
an anti-MEK political ransom note, which “closely mirrored the messaging used in cyberattacks   
against Iran . . . suggesting an intent to signal the attack as a form of retaliation” for earlier attacks.150   
Further, the MEK was planning to host a “Free Iran World Summit” on July 23–24, 2022, in Durrës,   
Julia Dickson and Emily Harding | 31

**Page 37**

A Playbook for Winning the Cyber War | 32  
HomeLand Justice ransom note.  
Source: Mandiant, “ROADSWEEP Ransomware-Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity   
Against Albanian Government Organizations,” Google Cloud Blog, August 4, 2022, https://www.microsoft.com/en-us/security/  
blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government.  
Leading up to the destructive attack, HomeLand Justice had created a website and various social   
media profiles on which they circulated anti-MEK messages. Following the attack, the group   
officially claimed credit and posted videos of the attack on their website. They also leaked Albanian   
government data between late July and mid-August on the group’s social media accounts.152  
Despite the severity of the attack, Tirana was able to recover relatively quickly. An Albanian   
government official highlighted that Iran had aimed to completely paralyze Albania’s government   
infrastructure, but that Albania was able to prevent the spread of the ransomware and recover   
most of the data from a backup within a matter of days.153 On August 12, 2022, the government   
reported, “All the online public services for the citizens and businesses and government websites   
in Albania have been fully restored and are normally accessible after almost four weeks of intense   
counterattacks against a massive and synchronized cyber attack.” The report indicated that 1,214 of   
the 1,225 services provided on the e-Albania platform were fully accessible, with a few others, such   
as the ability to issue diplomas, not yet restored.154  
Albania. The ransom note referenced Durrës, saying “Why should our taxes be spent on the benefit   
of DURRES terrorists?”151

**Page 38**

Only a few months later, Tehran targeted Tirana once more. The September 2022 attacks used similar   
tactics, techniques, and procedures and were “likely done in retaliation for public attribution of the   
cyber attacks in July.”155 The second attack targeted the Albanian police force’s Total Information   
Management System (TIMS), which stores information about people entering and leaving the country.   
The attack forced police departments across the country to take the TIMS offline for 24 hours.   
Albania benefited from its strong partnerships with the United States and NATO in recovering from   
these attack; both the U.S. government and private sector partners came to Tirana to help with the   
investigation and recovery.156 Albanian Prime Minister Edi Rama tweeted on July 24: “the good news is   
that the aggression was successfully repelled by an Albanian-American super team, that no data was   
deleted, that public services are back to work!”157   
In response to these attack, the Albanian government fully cut diplomatic ties with Tehran, forcing   
Iranian embassy staff to leave the country within 24 hours.158 Ties have not been restored. The United   
States also condemned the attack because it “violated the peacetime norm of not damaging critical   
infrastructure that the public relied on.”159  
In December 2023, Iran, again posing as HomeLand Justice, attacked the Albanian parliament,   
ONE Albania, and Air Albania. The attackers used the hashtag #DestroyDurresMilitaryCamp.160 In   
February 2024, they attacked the Albanian Institute of Statistics.161  
These attacks exemplify many tactics commonly associated with Iranian hacking groups, including   
their use of fake personae to avoid attribution and retaliatory messaging, but they also represent an   
“aggressive escalatory step,” according to Mandiant’s vice president of intelligence, John Hultquist.   
Prior to this attack, Iran had only conducted disruptive cyberattacks in the Middle East, suggesting   
that the country’s risk tolerance for using destructive cyber tools against its adversaries, including   
those outside of the region, may be increasing. Hultquist also emphasized “whatever deterrents   
we believe exist between us and them may not exist at all.” 162 So, as Tehran continues to increase   
its cyber capabilities, it will likely be willing to target the United States and its allies with similarly   
destructive and disruptive cyberattacks.   
Julia Dickson and Emily Harding | 33  
Figure 2: MOIS-Affiliated Groups Involved in the July 2022 Cyberattack  
    
▪  
DEV-0842 deployed the   
ransomware and wiper   
malware.  
    
▪  
DEV-0861 gained initial access   
and exfiltrated data.  
    
▪  
DEV-0166 exfiltrated data.  
    
▪  
DEV-0133 probed victim   
infrastructure.

**Page 39**

A Playbook for Winning the Cyber War | 34  
Case Study 3  
Iranian Cyberattacks During the Israel-Hamas War  
B  
efore Hamas attacked Israel on October 7, 2023, and Israel subsequently invaded Gaza,   
Israel was already a top target of Iranian cyberattacks. Following the war’s commencement,   
Iranian actors seemed to use existing accesses to make a statement, even if the connection   
between the target and the war was slim at best. Iran soon increased the frequency and   
sophistication of its cyberattacks in order to undercut support for the war and collect intelligence   
on key decisionmakers.163 At first, attacks mainly aimed at quickly stirring public discord, but   
eventually they became more targeted and focused on disruption. Iran’s tactics in Israel and against   
Israeli allies demonstrate key components of its evolving cyber strategy, including its opportunistic   
operations, use of advanced social engineering campaigns, increasing use of cyber-enabled   
influence operations, and reliance on proxies.  
Immediately following October 7, Iranian threat actors conducted a series of clearly opportunistic   
cyberattacks combined with influence operations designed to mislead and exaggerate Iranian   
capabilities and access. Iranian hackers quickly boosted their cyber operations in support of Gaza,   
utilizing pre-existing access and re-leaking old data. For instance, on October 8, Malek Team—  
likely an MOIS-affiliated cyber persona—leaked personal data from an Israeli university on Twitter.   
Without any clear link to the Israel-Hamas conflict, Microsoft Threat Intelligence concluded that the   
attack was most likely based on preexisting access and was opportunistic in nature; Malek Team saw   
a new opportunity within its existing capabilities and took it.164  
Iran also re-leaked old data and published ambiguous details and false information about   
supposedly successful cyberattacks in state media. For instance, Tasnim News Agency, a news

**Page 40**

outlet affiliated with the IRGC, stated on Twitter that the CyberAv3ngers attacked Israel’s Dorad   
powerplant “at the same time as the ‘Al-Aqsa Storm,’” but the group already had claimed to have   
conducted a cyberattack against an Israeli electricity company the evening before Hamas’s attack.   
Further, a Kaspersky report found that the images posted on CyberAv3nger’s Telegram were   
from a 2022 attack by Moses Staff, another Iranian group, which has no known affiliation with   
CyberAv3ngers.165 The confusing information and false claims of Iran’s successes are part of Iran’s   
broader influence operations that seek to intimidate Israel by overstating Iran’s capabilities. These   
attacks—both real and exaggerated—aimed to affect Israeli citizens’ and allies’ beliefs about the   
conflict, and thereby their behavior, but did not actually cause significant disruption or damage.  
As the war progressed, however, a growing number of groups shifted their focus to Israel, and   
attacks moved from being opportunistic or fabricated to being more carefully planned and   
somewhat destructive. Microsoft Threat Intelligence found that 9 groups were targeting Israel   
during the first week of the war, increasing to 14 groups after two weeks of conflict; the number   
of attacks more than doubled in the first month. Further, multiple groups affiliated with the   
IRGC and MOIS focused on the same targets, “suggesting coordination, common objectives set in   
Tehran, or both.”166  
During this second phase of the war from mid- to late October 2023, Iranian groups conducted   
more disruptive attacks while continuing to publish misleading and false information and rely on   
influence activity to exaggerate the effects of their attacks and abilities. For instance, on October 18,   
the IRGC’s Shahid Kaveh Group used custom ransomware to target Israeli security cameras. Soldiers   
of Solomon, one of Iran’s cyber personas, then claimed it had hacked security cameras and stolen   
data from the Nevatim air base. In actuality, the footage was from nowhere near the military base; it   
was from a town north of Tel Aviv with a street named Nevatim.167  
Throughout this period, Iran-linked threat actors continued to use advanced social engineering   
campaigns to target individuals of strategic interest to the Iranian government. In one instance,   
Charming Kitten sent emails to a series of targets, pretending to be a notable individual. The   
group posed as a journalist from a well-known news outlet reporting on the conflict in Gaza. After   
building rapport, Charming Kitten sent a follow-up email, including a link to a malicious domain.   
These campaigns targeted research and academic institutions in Belgium, France, Gaza, the United   
Kingdom, and the United States, and they were first spotted in November 2023.168  
As the war continued to progress, so too did the scope of Iran’s activities. By late November,   
Iranian groups had begun targeting countries that Iran perceives as supporting Israel, as well as   
Israeli-made systems in countries around the world. These destructive attacks highlight Tehran’s   
willingness to attack civilian critical infrastructure, its general disregard for international norms,   
and its willingness to conduct potentially escalatory acts when operating in the cyber domain.   
In December 2023, the Iranian front HomeLand Justice used wiper malware against Albania’s   
parliament, two local telecommunications companies, and Air Albania (a local airline).169 Microsoft   
Threat Intelligence assesses that two MOIS-affiliated groups collaborated on this destructive   
attack: One provided access to the network and the other executed wiper malware. See the case   
study on page 32 for more about Iran’s attacks on Albania.170 In another instance, IRGC-affiliated   
Julia Dickson and Emily Harding | 35

**Page 41**

A Playbook for Winning the Cyber War | 36  
CyberAv3ngers targeted and compromised programmable logic controllers made by Israeli   
company, Unitronics. The group hacked a small western Pennsylvania water authority using this   
Israeli system, warning that “every equipment made in Israel is CyberAv3ngers legal target.”171  
At the same time, Iran’s cyber-enabled influence operations also grew more sophisticated, utilizing   
new advanced techniques. In February 2024, Iranian hackers used artificial intelligence (AI) for the   
first time as a key component of a cyber-enabled influence campaign. State-backed actor Emennet   
Pasargad interrupted multiple broadcast channels to broadcast this deepfake. See page 25 for   
more information about this attack.172 The threat from Iran is likely to grow as its operations and   
capabilities continue to advance, becoming more carefully targeted and destructive and utilizing   
emerging technologies.

**Page 42**

About the Authors  
 Julia Dickson is a research associate with the Intelligence, National Security, and Technology   
(INT) Program at CSIS. Her research interests include cybersecurity and cybercrime and the   
role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and   
spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant   
at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center,   
and a communications and outreach intern at the International Crisis Group. She holds a BA in   
international studies with a minor in French from the Johns Hopkins University.  
Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program   
and vice president of the Defense and Security Department at CSIS. As the head of the INT Program,   
she provides thought leadership on the most critical issues facing intelligence professionals and   
on the future of intelligence work. She also serves as vice president of the Defense and Security   
Department, where she is responsible for leading a team of world-renowned scholars providing   
policy solutions that shape national security. Drawing on her decades of experience in national   
security, Emily has established herself as an expert on how technology is revolutionizing national   
security work. Harding has served in a series of high-profile national security positions at critical   
moments. While serving as deputy staff director on the Senate Select Committee on Intelligence,   
she led the committee’s investigation into Russian interference in the 2016 elections, which was   
lauded for its bipartisanship. At CIA, she led analysts and analytic programs through moments of   
crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a   
tour at the National Security Council, she served as director for Iran. After leaving the White House,   
her team ran the first Office of the Director of National Intelligence-led presidential transition,   
Julia Dickson and Emily Harding | 37

**Page 43**

A Playbook for Winning the Cyber War | 38  
where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer   
at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the   
Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. Harding holds a master’s degree   
from Harvard University’s Kennedy School of Government and a bachelor’s degree from the   
University of Virginia.

**Page 44**

Endnotes  
1   
Ayman Oghanna, “How Albania Became a Target for Cyberattacks,” Foreign Policy, July 24, 2024, https://  
foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.  
2   
“A Cyberattack Targets Albanian Parliament’s Data System, Halting Its Work,” AP News, December 26,   
2023, https://apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1ab­  
c0f7.  
3   
Alex Campbell et al., “How Does Iran Conceive of Cyber as Part of Its National Strategy?,” Columbia   
School of International Public Affairs, 2019, https://www.sipa.columbia.edu/how-does-iran-conceiv  
e-cyber-part-its-national-strategy.  
4   
Mark Thompson, “Iranian Cyber Attack on New York Dam Shows Future of War,” TIME, March 24, 2016,   
https://time.com/4270728/iran-cyber-attack-dam-fbi/.  
5   
James P. Farwell and Darby Arkelian, “What Does Iran’s Cyber Capability Mean for Future Conflict?,”   
Whitehead Journal of Diplomacy and International Relations (Winter/Spring 2013), https://ciaotest.cc.co­  
lumbia.edu/journals/shjdir/v14i1/f\_0028742\_23336.pdf.  
6   
Colin Anderson and Karim Sadjadpour, Iran’s Cyber Threat: Espionage, Sabotage, and Revernge (Wash­  
ington, DC: Carnegie Endowment for International Peace, 2018), https://carnegieendowment.org/files/  
Iran\_Cyber\_Final\_Full\_v2.pdf.  
7   
Ibid.  
8   
Kim Zetter, “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon,” Wired, November 3,   
2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.  
Julia Dickson and Emily Harding | 39

**Page 45**

A Playbook for Winning the Cyber War | 40  
9   
Nicole Perlroth, “Attacks on 6 Banks Frustrate Customers,” New York Times, September 30, 2012, https://  
www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html;   
and Thompson, “Iranian Cyber Attack on New York Dam Shows Future of War.”  
10   
“Connect the Dots on State-Sponsored Cyber Incidents - Compromise of Saudi Aramco and RasGas,”   
Council on Foreign Relations, accessed July 25, 2024, https://www.cfr.org/cyber-operations/compromis  
e-saudi-aramco-and-rasgas; and Nicole Perlroth, “In Cyberattack on Saudi Firm, U.S. Sees Iran Fir­  
ing Back,” New York Times, October 24, 2012, https://www.nytimes.com/2012/10/24/business/global/  
cyberattack-on-saudi-oil-firm-disquiets-us.html.  
11   
David E. Sanger, “U.S. Indicts 7 Iranians in Cyberattack on Banks and a Dam,” New York Times, March 24,   
2016, https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-  
banks-and-a-dam.html; “Iran Cyber Threat Overview,” Sekoia (blog), June 5, 2023, https://blog.sekoia.io/  
iran-cyber-threat-overview/.  
12   
Chuck Freilich, “Part 2: Iran’s Cyber Strategy, Institutions, and Capabilities,” in The Iranian Cyber Threat:   
The Institutions and Praxis of Iran’s Cyber Strategy (Washington, DC: Institute for National Security Stud­  
ies, February 2024), https://www.inss.org.il/wp-content/uploads/2024/02/Part-2.pdf.  
13   
Clint Watts, “Iran Accelerates cyber ops against Israel from chaotic start,” Microsoft Threat Analysis   
Center, February 6, 2024, https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cybe  
r-ops-against-israel/.  
14   
“Iran, Russia Agree on Cyber-Defense Cooperation: Official,” Tasnim News Agency, June 13, 2015,   
https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defens  
e-cooperation-official.  
15   
“Россия и Иран подписали меморандум о сотрудничестве в области связи и ИТ” [Russia and   
Iran signed a memorandum of cooperation in the field of communications and IT], Министерство   
цифрового развития, связи и массовых коммуникаций Российской Федерации [Ministry of   
Digital Development, Communications, and Mass Comunications of the Russian Federation], March 28,   
2017, https://digital.gov.ru/ru/events/36659/.  
16   
“Iran, Russia Sign Information Security Cooperation Pact,” Ministry of Foreign Affairs of the Islamic   
Republic of Iran, January 26, 2021, https://en.mfa.ir/portal/NewsView/625777.  
17   
Dov Lieber, “Russia Supplies Iran with Cyber Weapons as Military Cooperation Grows,” Wall Street   
Journal, March 27, 2023, https://www.wsj.com/articles/russia-supplies-iran-with-cyber-weapons-as-milita  
ry-cooperation-grows-b14b94cd.  
18   
Golnaz Esfandiari, “Iran to Work With China to Create National Internet System,” Radio Free Eu­  
rope Radio Library, September 4, 2020, https://www.rferl.org/a/iran-china-national-internet-syste  
m-censorship/30820857.html.  
19   
James Andrew Lewis, “Iran and Cyber Power,” CSIS, Commentary, June 25, 2019, https://www.csis.org/  
analysis/iran-and-cyber-power.  
20   
Campbell et al., “How Does Iran Conceive of Cyber as Part of Its National Strategy?”  
21   
“Iran Cyber Threat Overview and Advisories,” Cybersecurity and Infrastrure Agency (CISA), accessed   
August 24, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/  
iran.  
22   
Gabi Siboni and Sami Kronenfeld, “Iran’s Cyber Warfare,” Institute for National Security Studies, INSS   
Insight, no. 375 October 15, 2012, https://www.files.ethz.ch/isn/154842/No375\_15OCT2012.pdf.

**Page 46**

23   
Alex Vatanka, “Whither the IRGC of the 2020s? Is Iran’s Proxy Warfare Strategy of Forward Defense   
Sustainable?,” New America, January 15, 2021, https://www.newamerica.org/future-security/reports/  
whither-irgc-2020s/ii-introduction.  
24   
Amr Yossef, “Upgrading Iean’s Military Doctrine: An Offensive ‘Forward Defense’,” Middle East In­  
stitute, December 10, 2019, https://www.mei.edu/publications/upgrading-irans-military-doctrin  
e-offensive-forward-defense.  
25   
A sock puppet is a false online identity. Iranian hackers are known for creating fake social media profiles   
and emails to have elaborate conversations with their victims. After building trust, the sock puppet   
sends a malicious link or attachment.  
26   
“Social Engineering Remains Key Tradecraft for Iranian APTs,” Insikt Group, March 30, 2022, https://  
www.recordedfuture.com/blog/social-engineering-remains-key-tradecraft-for-iranian-apts.  
27   
Ionut Arghire, “Iranian Spies Maintained Social Media Persona for Years Before Targeting Defense   
Contractor,” SecurityWeek, July 28, 2021, https://www.securityweek.com/iranian-spies-maintained-socia  
l-media-persona-years-targeting-defense-contractor/.  
28   
“Israel Busts Iran’s Phishing Network Active in LinkedIn,” Iran International, July 31, 2023, https://www.  
iranintl.com/en/202307308905.  
29   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence,   
February 26, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/ira  
n-surges-cyber-enabled-influence-operations-in-support-of-hamas.  
30   
“Iran and the Rise of Cyber-Enabled Influence Operations,” Dark Reading, August 16, 2023, https://www.  
darkreading.com/cybersecurity-operations/iran-and-the-rise-of-cyber-enabled-influence-operations-.  
31   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
32   
Kat Duffy, Kyle Fendorf, and Cecilia Marrinan, “Cyber Week in Review: February 16, 2024,” Council on   
Foreign Relations, February 16, 2024, https://www.cfr.org/blog/cyber-week-review-february-16-2024.  
33   
“Statement from Director of National Intelligence Avril Haines on Recent Iranian Influence Efforts,”   
Office of the Director of National Intelligence, July 9, 2024, https://www.dni.gov/index.php/newsroom/  
press-releases/press-releases-2024/3842-statement-from-director-of-national-intelligence-avril-haine  
s-on-recent-iranian-influence-efforts.  
34   
Jose Pagliery, “The inside Story of the Biggest Hack in History,” CNN Money, August 5, 2015, https://mon­  
ey.cnn.com/2015/08/05/technology/aramco-hack/index.html.  
35   
“Shamoon (2012),” Cyber Law toolkit, September 17, 2021, https://cyberlaw.ccdcoe.org/wiki/Shamoon\_  
(2012).  
36   
Center for Security Studies, Hotspot Analysis: Iranian cyber-activities in the context of regional rival­  
ries and international tensions (Zurich: ETH Zurich, May 2019), https://css.ethz.ch/content/dam/ethz/  
special-interest/gess/cis/center-for-securities-studies/pdfs/20190507\_MB\_HS\_IRN%20V1\_rev.pdf.  
37   
Anderson and Sadjadpour, Iran’s Cyber Threat.  
38   
“Iran,” Freedom House, 2022, https://freedomhouse.org/country/iran/freedom-net/2022; and Paul   
Bucala and Caitlin Shayda Pendleton, “Iranian Cyber Strategy: A View from the Iranian Military,” Critical   
Threats, November 24, 2015, https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-fro  
m-the-iranian-military.  
Julia Dickson and Emily Harding | 41

**Page 47**

A Playbook for Winning the Cyber War | 42  
39   
Maziar Motamedi, “Iran unveiled plan for tighter internet rules to promote local platforms,” Al Jazeera,   
February 24, 2024, https://www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-  
rules-to-promote-local-platforms.  
40   
“Treasury Sanctions Iranian Company Aiding in Internet Censorship,” U.S. Department of the Treasury,   
June 2, 2023, https://home.treasury.gov/news/press-releases/jy1518.  
41   
“After internet blackout, Iranians take stock,” Al Jazeera, November 27, 2019, https://www.aljazeera.com/  
economy/2019/11/27/after-internet-blackout-iranians-take-stock.  
42   
Raksha Kumar, “As the world focuses on Ukraine, Iran is on the verge of becoming an internet black   
hole,” Reuters Institute for the Study of Journalism, April 5, 2022, https://reutersinstitute.politics.ox.ac.  
uk/news/world-focuses-ukraine-iran-verge-becoming-internet-black-hole.  
43   
Anderson and Sadjadpour, Iran’s Cyber Threat.  
44   
Ibid.  
45   
David E. Sanger, “U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam,” New York Times, March   
24, 2016, https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberat­  
tacks-on-banks-and-a-dam.html?module=inline; and  
“Iran Cyber Threat Overview,” Sekoia (blog), June 5, 2023, https://blog.sekoia.io/iran-cyber-threat-overview/.  
46   
“Iran threatens retaliation after what it calls possible cyber attacl on nuclear site,” Reuters, July 3, 2020,   
https://www.reuters.com/article/idUSKBN24424H/.  
47   
“Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure,” U.S.   
Department of the Treasury, February 2, 2024, https://home.treasury.gov/news/press-releases/jy2072.   
48   
A. J. Vicens, “How an Iranian-Linked Influence Campaign Pivoted after Oct. 7 Attack on Israel,” Cyber­  
Scoop (blog), May 8, 2024, https://cyberscoop.com/how-an-iranian-linked-influence-campaign-pivoted-a  
fter-oct-7-attack-on-israel/.  
49   
Ibid.  
50   
Anderson and Sadjadpour, Iran’s Cyber Threat.  
51   
Anderson and Sadjadpour, Iran’s Cyber Threat.  
52   
Ashley Lane, “Iran’s Islamist Proxies in the Middle East,” Wilson Center, September 12, 2023, https://  
www.wilsoncenter.org/article/irans-islamist-proxies.  
53   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
54   
“Iran Cyber Threat Overview and Advisories,” CISA, accessed August 26, 2024, https://www.cisa.gov/top­  
ics/cyber-threats-and-advisories/advanced-persistent-threats/iran.  
55   
Erika Stanish, “Municipal Water Authority of Aliquippa hacked by Iran-backed cyber group,” CBS News,   
November 23, 2023, https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliqui  
ppa-hacked-iranian-backed-cyber-group/.  
56   
“Foreign Threats to the 2020 US Federal Elections,” National Intelligence Council, March 10, 2021,   
https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.  
57   
“Treasury Sanctions Iraian Cyber Actors for Attempting to Influence the 2020 U.S. Presidential   
Election,” U.S. Department of the Treasury, November 18, 2021, https://home.treasury.gov/news/  
press-releases/jy0494.

**Page 48**

58   
Office of Public Affairs,, “Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat   
Campaign Designed to Influence the 2020 U.S. Presidential Election,” U.S. Department of Justice,   
November 18, 2021, https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-  
disinformation-and-threat-campaign-designed.  
59   
Mandiant, “APT42: Crooked Charms, Cons, and Compromises,” Google Cloud, September 7, 2022,   
https://www.mandiant.com/resources/blog/apt42-charms-cons-compromises.  
60   
Ofir Rozmann et al., “Uncharmed: Untangling Iran’s APT42 Operations,” Mandiant, Google Cloud, May 1,   
2024, https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations.  
61   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
62   
“Iran’s Revolutionary Guards,” Council on Foreign Relations, April 17, 2024, https://www.cfr.org/back­  
grounder/irans-revolutionary-guards.  
63   
“Islamic Revolution Guard Corps (IRGC),” National Counterterrorism Center, March 2022, https://www.  
dni.gov/nctc/ftos/irgc\_fto.html.  
64   
Lewis, “Iran and Cyber Power.”  
65   
Adam Meyers, “Who is REFINED KITTEN?,” CrowdStrike (blog), December 12, 2019, https://www.crowd­  
strike.com/blog/who-is-refined-kitten/.  
66   
Jacqueline O’Leary et al., “Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy   
Sectors and has Ties to Destructive Malware,” Mandiant, September 20, 2017, https://www.mandiant.  
com/resources/blog/apt33-insights-into-iranian-cyber-espionage.  
67   
“APT33,” Council on Foreign Relations, accessed August 26, 2024, https://www.cfr.org/cyber-operations/  
apt-33.  
68   
Meyers, “Who is REFINED KITTEN?”  
69   
“Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets,”   
Microsoft Threat Intelligence, September 14, 2023, https://www.microsoft.com/en-us/security/  
blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-v  
alue-targets/.  
70   
Jacqueline O’Leary et al., “Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy   
Sectors and has Ties to Destructive Malware,” Mandiant, September 20, 2017, https://www.mandiant.  
com/resources/blog/apt33-insights-into-iranian-cyber-espionage.  
71   
Thomas Roccia, “Shamoon Attackers Employ New Tool Kit to Wipe Infected Systems,” McAfee, Decem­  
ber 19, 2018, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-attackers-employ-ne  
w-tool-kit-to-wipe-infected-systems/.  
72   
O’Leary et al., “Insights into Iranian Cyber Espionage.”  
73   
“Charming Kitten,” CrowdStrike, accessed August 26, 2024, https://www.crowdstrike.com/adversaries/  
charming-kitten/.  
74   
“Magic Hound,” MITRE Corporation, last updated January 8, 2024, https://attack.mitre.org/groups/  
G0059/.  
75   
“Advanced Persistent Threats (APTs),” Mandiant, accessed August 26, 2024, https://www.mandiant.com/  
resources/insights/apt-groups.   
Julia Dickson and Emily Harding | 43

**Page 49**

A Playbook for Winning the Cyber War | 44  
76   
Bryan Lee and Robert Falcone, “Magic Hound Campaign Attacks Saudi Targets,” Unit 42 by Palo Alto   
Networks, February 15, 2017, https://unit42.paloaltonetworks.com/unit42-magic-hound-campaig  
n-attacks-saudi-targets/.  
77   
Eduard Kovacs, “Iranian Spies Target Saudi Arabia in ‘Magic Hound’ Attacks,” SecurityWeek, February   
16, 2017, https://www.securityweek.com/iranian-spies-target-saudi-arabia-magic-hound-attacks/.  
78   
“Advanced Persistent Threats (APTs),” Mandiant.  
79   
Tom Burt, “New cyberattacks targeting U.S. elections,” Microsoft, September 10, 2020, https://blogs.mic­  
rosoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.  
80   
“Advisory on cyber espionage against critics of the Iranian regime in Germany,” Federal Office for the   
Protection of the Constitution, BfV Cyber-Brief Nr. 01/2023, August 10, 2023, https://www.verfassungss­  
chutz.de/SharedDocs/kurzmeldungen/DE/2023/2023-08-10-cyber-brief-01-2023.html?nn=679196#Start.  
81   
“Germany says Charming Kitten Hackers target Iran dissidents,” Deutsche Welle, August 10, 2023, https://  
www.dw.com/en/germany-says-charming-kitten-hackers-target-iran-dissidents/a-66493687.  
82   
“Imperial Kitten,” CrowdStrike, accessed August 26, 2024, https://www.crowdstrike.com/adversaries/  
imperial-kitten/; And “Charming Kitten,” CrowdStrike, accessed August 26, 2024, https://www.crowd­  
strike.com/adversaries/charming-kitten/.  
83   
“IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations,” CrowdStrike   
(blog), November 9, 2023, https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malwar  
e-families/.  
84   
Ibid.  
85   
Ofir Rozmann, Chen Evgi, and Jonathan Leathery, “When Cats Fly: Suspected Iranian Treat Actor   
UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors,” Mandiant, Google Cloud,   
February 27, 2024, https://cloud.google.com/blog/topics/threat-intelligence/suspected-iranian-unc154  
9-targets-israel-middle-east.  
86   
Mandiant, “APT42: Crooked Charms, Cons, and Compromises,” Google Cloud, September 7, 2022,   
https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises.  
87   
Ibid.  
88   
Rozmann et al., “Uncharmed.”.  
89   
Ibid.  
90   
Connor Bradbury, “Profiles: Iran’s Intelligence Agencies,” The Iran Primer, April 5, 2023, https://iran­  
primer.usip.org/blog/2023/apr/05/profiles-iran%E2%80%99s-intelligence-agencies.  
91   
Maxime A. and Sekoia TDR, “Iranian Cyber Threat Overview,” Sekoia (blog), June 5, 2023, https://blog.  
sekoia.io/iran-cyber-threat-overview.  
92   
“Iranian intel cyber suite of malware uses open source tools,” U.S. Cyber Command, January   
12, 2022, https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-o  
f-malware-uses-open-source-tools/.  
93   
“MuddyWater,” SOCRadar, January 2, 2023, https://socradar.io/dark-web-profile-muddywater-ap  
t-group/.  
94   
“MERCURY and DEV-1084: Destructive attack on hybrid environment,” Microsoft Threat Intelligence,   
April 7, 2023, https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-108  
4-destructive-attack-on-hybrid-environment/.

**Page 50**

95   
“MuddyWater,” SOCRadar, January 2, 2023, https://socradar.io/dark-web-profile-muddywater-ap  
t-group/.  
96   
Ryan Tomcik, Emiel Haeghebaert, and Tufail Ahmen, “Left on Read: Telegram Malware Spotted in Lat­  
est Iranian Cyber Espionage Activity,” Mandiant, Google Cloud, February 24, 2022, https://cloud.google.  
com/blog/topics/threat-intelligence/telegram-malware-iranian-espionage/.  
97   
Simon Kenin, “MiddyWater eN-Able spear-phishing with new TTPs,” Deep Instinct Threat Lab, Novem­  
ber 1, 2023, https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps.  
98   
“Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations,” CISA,   
February 24, 2022, https://www.cisa.gov/news-events/alerts/2022/02/24/iranian-government-sponsore  
d-muddywater-actors-conducting-malicious.  
99   
Bryan Lee and Robert Falcone, “Behind the Scenes with OilRig,” Unit42, April 30, 2019, https://unit42.  
paloaltonetworks.com/behind-the-scenes-with-oilrig/.  
100   
“Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attack Against Governments,” Syman­  
tec, June 20, 2019, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbu  
g-espionage-governments.  
101   
“Kaspersky experts warn of increase IT supply chain attacks by OilRig APT in the Middle East and Turki­  
ye,” Kaspersky, May 8, 2023, https://me-en.kaspersky.com/about/press-releases/2023\_kaspersky-expert  
s-warn-of-increased-it-supply-chain-attacks-by-oilrig-apt-in-the-middle-east-and-turkiye.  
102   
Dan Raywood, “Iran’s APT34 Hits UAE With Supply Chain Attack,” Dark Reading, August 2, 2023, https://  
www.darkreading.com/cyberattacks-data-breaches/iran-apt34-uae-supply-chain-attack.  
103   
“Advanced Persistent Threats (APTs),” Mandiant.  
104   
“Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities,” U.S. De­  
partment of the Treasury, September 9, 2022, https://home.treasury.gov/news/press-releases/jy0941.  
105   
“Chafer: Latest Attacks Reveal Heightened Ambitions,” Symantec, February 28, 2018, https://  
symantec-enterprise-blogs.security.com/threat-intelligence/chafer-latest-attacks-revea  
l-heightened-ambitions.  
106   
Liviu Arsene, “Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi   
Arabia,” Bitdefender, May 21, 2020, https://www.bitdefender.com/blog/labs/iranian-chafer-apt-targete  
d-air-transportation-and-government-in-kuwait-and-saudi-arabia/.  
107   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
108   
Or Chechik et al., “Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sec­  
tors,” Unit 42 at Palo Alto Networks, November 6, 2023, https://unit42.paloaltonetworks.com/agonizin  
g-serpens-targets-israeli-tech-higher-ed-sectors/.  
109   
Dan Raywood, “Iran-Linked Agrius APT Group Targets Israeli Education, Tech Sectors,” Dark Reading,   
November 7, 2023, https://www.darkreading.com/cyberattacks-data-breaches/iran-linked-agrius-ap  
t-group-israeli-education-tech-sectors.  
110   
“Hexane,” Mitre Corporation, accessed August 26, 2024, https://attack.mitre.org/groups/G1001/.  
111   
“Lyceum takes Center Stage in Middle East Campaign,” Secureworks, August 27, 2019, https://www.  
secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign.  
112   
“New Iranian Espionage Campaign by ‘Siamesekitten’—Lyceum,” ClearSky, August 17, 2021, https://www.  
clearskysec.com/siamesekitten/.  
Julia Dickson and Emily Harding | 45

**Page 51**

A Playbook for Winning the Cyber War | 46  
113   
Alex Orleans, “Who Is PIONEER KITTEN?,” CrowdStrike, August 31, 2020, https://www.crowdstrike.  
com/blog/who-is-pioneer-kitten/.  
114   
“Iran Based Threat Actor Exploits VPN Vulnerabilities,” CISA, September 15, 2020, https://www.cisa.gov/  
news-events/cybersecurity-advisories/aa20-259a.  
115   
Joseph Menn, “Oiran gained access to election result website in 2020, military reveals,” Washington Post,   
April 24, 2020, https://www.washingtonpost.com/technology/2023/04/24/election-2020-iran-hacking/.   
AJ Vicens, “Microsoft says Iranian hackers combined influence ops with hacking for maxi­  
mum impact,” Cyberscoop, May 2, 2023, https://cyberscoop.com/iranian-information-operation  
s-hacking-microsoft-report/.  
116   
“Treasury Sanctions Senior Iranian Officials Overseeing Violent Protest Suppression and Censorship,”   
U.S. Department of the Treasury, April 24, 2023, https://home.treasury.gov/news/press-releases/jy1436.  
“Supreme Council of Cyberspace,” United Against Nuclear Iran, accessed August 26, 2024, https://www.united­  
againstnucleariran.com/sanctioned-person/supreme-council-of-cyberspace-scc.”  
117   
“Iran,” Center for Internet and Society at Stanford Law School, accessed August 26, 2024, https://wil­  
map.stanford.edu/country/iran.  
118   
Catherine A. Theohary, “Iranian Offensive Cyber Attack Capabilities,” Congressional Research Service,   
IF11406, January 13, 2020, https://sgp.fas.org/crs/mideast/IF11406.pdf.  
119   
“Treasury Sanction Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Sup­  
port to Sanctioned Weapons Proliferators,” U.S. Department of the Treasury, January 12, 2018, https://  
home.treasury.gov/news/press-releases/sm0250.  
120   
Farzin Nadimi, “Iran’s Passive Defense Organization: Another Target for Sanctions,” Washington Insti­  
tution for Near East Policy, August 16, 2018, https://www.washingtoninstitute.org/policy-analysis/iran  
s-passive-defense-organization-another-target-sanctions.  
121   
Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power (Cambridge: Cambridge University   
Press, 2018).  
122   
Campbell et al., “How Does Iran Conceive of Cyber as Part of Its National Strategy?”  
123   
“Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds   
of University,” U.S. Department of the Treasury, March 23, 2018, https://home.treasury.gov/news/  
press-releases/sm0332.  
124   
“Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity,” U.S. Department of   
the Treasury, September 14, 2022, https://home.treasury.gov/news/press-releases/jy0948.  
125   
“Profiling DEV-0270: PHOSPHORUS’ ransomware operations,” Microsoft Threat Intelligence, Septem­  
ber 7, 2022, https://www.microsoft.com/en-us/security/blog/2022/09/07/profiling-dev-0270-phosphoru  
s-ransomware-operations/.  
126   
“Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity,” the U.S. Depart­  
ment of the Treasury, September 14, 2022, https://home.treasury.gov/news/press-releases/jy0948.  
127   
“U.S. Sanctions Iran for Election Hacking,” U.S. Institute of Peace, The Iran Primer, November 19, 2021,   
https://iranprimer.usip.org/blog/2021/nov/18/us-sanctions-iran-election-hacking.  
128   
“Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Perso­  
nas,” Federal Bureau of Investigation, October 20, 2022, https://www.ic3.gov/Media/News/2022/221020.  
pdf.

**Page 52**

129   
“Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election,”   
U.S. Department of the Treasury, November 18, 2021, https://home.treasury.gov/news/press-releases/  
jy0494.  
130   
Catalin Cimpanu, “US charges Iranian hackers for spoofed Proud Boys emails threatening US voters,”   
The Record, November 17, 2021, https://therecord.media/us-charges-iranian-hackers-for-spoofed  
-proud-boys-emails-threatening-us-voters.  
131   
“FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissi­  
dents and Travel and Telecommunicaitons Companies,” Federal Bureau of Investigation, September 17,   
2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-releases-cybersecurit  
y-advisory-on-previously-undisclosed-iranian-malware-used-to-monitor-dissidents-and-travel-and-t  
elecommunications-companies.  
132   
“Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Con­  
ducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector,” U.S. Department of the   
Treasury, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutiona  
ry-guard-corps-affiliated-entities-charged.  
133   
“Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and   
Internet Censorship,” U.S. Department of the Treasury, October 26, 2022, https://home.treasury.gov/  
news/press-releases/jy1048.  
134   
“IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater   
Systems Facilities,” CISA, December 1, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/  
aa23-335a.  
135   
“Dark Web Profile: CyberAv3ngers,” SOCRadar, December 22, 2023, https://socradar.io/dark-web-profil  
e-cyber-av3ngers/.  
136   
AJ Vicens, “U.S. government sanctions Iranian officials over Pennsylvania water facility hack,” Cyber­  
scoop, February 2, 2024, https://cyberscoop.com/u-s-government-sanctions-iranian-officials-over-penn­  
sylvania-water-facility-hack/.  
137   
“Dark Web Profile: Haghjoyan,” SOCRadar, December 28, 2023, https://socradar.io/  
dark-web-profile-haghjoyan/.  
138   
“Dark Web Profile: Cyber Toufan Al-aqsa,” SOCRadar, December 28, 2023, https://socradar.io/dark-we  
b-profile-cyber-toufan-al-aqsa/; “Claims of cyberattack on Israeli power plant found to be false: Re­  
port,” The Hindu, October 18, 2023, https://www.thehindu.com/sci-tech/technology/gadgets/claims-o  
f-cyberattack-israeli-power-plant-false/article67433778.ece.  
139   
“Dark Web Profile: Cyber Toufan Al-aqsa,” SOCRadar, December 28, 2023, https://socradar.io/dark-we  
b-profile-cyber-toufan-al-aqsa/.  
140   
Nate Nelson, “’Cyber Toufan’ Hacktivists Leaked 100-Plus Israeli Orgs in One Month,” Dark Reading,   
January 4, 2024, https://www.darkreading.com/cyberattacks-data-breaches/-cyber-toufan-hacktivists-l  
eaked-100-plus-israeli-orgs-in-one-month.  
141   
Connor Simpson, “Sheldon Adelson Has an Idea: Lob a Nuclear Bomb in the Iranian Desert,” The Atlan­  
tic, October 23, 2013, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charg  
ed-conspiracy-conduct-multiple-cyber-attacks-and.  
142   
Ibid.  
Julia Dickson and Emily Harding | 47

**Page 53**

A Playbook for Winning the Cyber War | 48  
143   
Sean Gallagher, “Iranian Hackers Used Visual Basic Malware to Wipe Vegas Casino’s Network,” Ars Tech­  
nica, December 12, 2014, https://arstechnica.com/information-technology/2014/12/iranian-hackers-use  
d-visual-basic-malware-to-wipe-vegas-casinos-network/.  
144   
“Iran’s Cyber Attack on Billionaire Adelson Provides Lesson on Strategy,” Claims Journal, January 6,   
2020, https://www.claimsjournal.com/news/national/2020/01/06/294849.htm.  
145   
Jose Pagliery, “Iran Hacked an American Casino, U.S. Says,” CNN Money, February 27, 2015, https://mon­  
ey.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html.  
146   
“North Korean Regime-Backed Programmer Charged With Conspiract to Conduct Multiple Cyber Attacks   
and Intrusions,” Office of Public Affairs, U.S. Department of Justice, September 6, 2018, https://www.  
justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-c  
yber-attacks-and.  
147   
Ayman Oghanna, “How Albania Became a Target for Cyberattacks,” Foreign Policy, March 25, 2023,   
https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.  
148   
Harun Karclc, “How Albania Ended Up in Iran’s Cyber Crosshairs,” Foreign Policy, November 8, 2022,   
https://foreignpolicy.com/2022/11/08/albania-iran-cyberattack-mek-us-israel/.  
149   
“e-Albania Partially Restored after Cyber Attack,” Albanian Daily News, July 20, 2022, https://albanianda­  
ilynews.com/news/e-albania-partially-restored-after-cyber-attack.  
150   
“Microsoft investigates Iranian attacks against the Albanian government,” Microsoft, April 2023, https://  
www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-th  
e-albanian-government/.  
151   
A. J. Vicens, “Hackers Deploy New Ransomware Tool in Attacks on Albanian Government Websites,”   
CyberScoop, August 4, 2022, https://cyberscoop.com/iran-hack-albania-ransomware-mek/.  
152   
“Iranian State Actors Conduct Cyber Operations Against the Government of Albania,” U.S. Department   
of Justice and the Cybersecurity and Infrastructure Security Agency, September 21, 2022, https://cisa.  
gov/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-th  
e-government-of-albania.pdf.  
153   
Interview with General Director of the National Authority on Electronic Certification and Cybersecurity   
of Albania and National Coordinator for Cyber Security, October 13, 2023.  
154   
“Online Services Via e-Albania Portal Rully Restored,” Government of Albania, August 12, 2022,   
https://www.kryeministria.al/en/newsroom/sherbimet-publike-online-rikthehen-ne-normalit  
et-te-plote-ne-e-albania.  
155   
“Iranian State Actors Conduct Cyber Operations Against the Government of Albania,” CISA, September   
23, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.  
156   
“Albania cuts Iran ties over cyberattack, U.S. vows further action,” Reuters, September 7,   
2022, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-a  
ttack-pm-says-2022-09-07/.  
157   
“Lajmi i mirë është se agresioni është zmbrapsur me sukses nga një superskuadër shqiptaro-amerikane,   
se asnjë e dhënë nuk është fshirë, se shërbimet publike janë kthyer në punë! Vazhdon operacioni i   
forcimit të mureve mbrojtëse dhe hetimit për identifikimin e sigurtë të agresorit!” Edi Rama, Twitter   
post, July 24, 2022, 9:08 am, https://twitter.com/ediramaal/status/1551192528669605888.

**Page 54**

158   
Elona Elezi, “Albania blames Iran for cyberattacks,” Deutsche Welle, September 16, 2022, https://www.  
dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-exp  
elling-diplomats/a-63146285.  
159   
“Albania cuts Iran ties over cyberattack, U.S. vows further action,” Reuters, September 7,   
2022, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-a  
ttack-pm-says-2022-09-07/.  
160   
“Pro-Iranian Hacker Group Targeting Albania with No-Justice Wiper Malware,” The Hacker News, Janu­  
ary 6, 2024, https://thehackernews.com/2024/01/pro-iranian-hacker-group-targeting.html.  
161   
Llazar Semini, “A cyberattack targets Albanian Parliament’s data system, halting its work,” Asso­  
ciated Press, December 26, 2023, https://apnews.com/article/albania-cyberattack-parliament-ira  
n-cc1a03b58bd753bbe935ad74f1abc0f7; and “Albanian authorities accurse Iranian-backed hackers of   
cyberattack on Institute of Statistics,” Associated Press, February 14, 2024, https://apnews.com/article/  
albania-iran-hackers-cyberattack-statistics-e80780e2d927394589c3d8903e36d066.  
162   
Lily Hay Newman, “An Attack on Albanian Government Suggests New Iranian Aggression,” Wired, Au­  
gust 4, 2022, https://www.wired.com/story/iran-cyberattack-albania/.  
163   
“Tool of First Resort: Israel-Hamas War in Cyber,” Google, February 2024, https://services.google.com/  
fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf.  
164   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
165   
Securelist, “A hack in hand is worth two in the bush,” AO Kaspersky Lab, 16 October 2023, https://se­  
curelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/.  
166   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
167   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
168   
James Coker, “Iranian Phishing Campaign Targets Israel-Hamas War Experts,” Infosecurity Magazine,   
January 18, 2024, https://www.infosecurity-magazine.com/news/iranian-phishing-israel-hamas/.   
169   
Daryna Antoniuk, “Wiper malware found in analysis or Iran-linked attacks on Albanian institu­  
tions,” The Record, January 8, 2024, https://therecord.media/albania-parliament-telecoms-airlin  
e-cyberattacks-wiper-malware.  
170   
“Iran Surges cyber-enabled influence operations in support of Hamas,” Microsoft Threat Intelligence.  
171   
“IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater   
Systems Facilities,” CISA, December 1, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/  
aa23-335a; and Vicens, “U.S. government sanctions Iranian officials over Pennsylvania water facility   
hack.”  
172   
Dan Milmo, “Iran-backed hackers interrupt UAE TV streaming services with deepfake news,” The   
Guardian, February 8, 2024, https://www.theguardian.com/technology/2024/feb/08/iran-backed-hacker  
s-interrupt-uae-tv-streaming-services-with-deepfake-news.   
Julia Dickson and Emily Harding | 49

**Page 55**

1616 Rhode Island Avenue NW  
Washington, DC 20036  
202 887 0200 | www.csis.org  
COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK