Chapter 54
Punching Above Their Digital Weight:
Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations

Ralph Peter Martins
Harvard University, Cambridge, USA

ABSTRACT

This article describes how in recent years, Iran has joined the top ranks of the world powers in cyberspace and has demonstrated the ability to leverage cyberwarfare as a significant tool in its arsenal for pursuing its national security goals. While this increase in cyber power is relatively recent, some of the incidents and events that serve as the catalyst for the sudden digital surge go back decades. The reasons for these increased capabilities revolve around historic means of power projection, defense and preservation of the principles of the Iranian Revolution, response to Western aggression and Iranian nationalism. This article explores these ideological drivers and events to provide context for their trajectory and analysis of their likely implications.

INTRODUCTION

Since the turn of the 21st century, the Islamic Republic of Iran has joined many other nations in setting up formal, robust national cyberwarfare capabilities. Not only has Iran built these programs, but in more recent years, it has developed them to such a degree that Iran is now increasingly recognized as disproportionally strong in cyberspace. To put it in perspective, the United States, China and Russia are considered the top three cyber powers, and many would place the United Kingdom and Israel 4th and 5th in the world. In recent years, Iran has directed its attention and resources towards its cyber capabilities, and many now consider it to be moving up the top-10 list, which would make it decidedly more powerful in cyberspace, relative to the world, then it is in terms of conventional power. There are specific reasons for the Iranian digital surge. This paper will examine the events and drivers that prompted it to develop

DOI: 10.4018/978-1-7998-2466-4.ch054

its cyberwarfare capabilities and seek to answer the following questions: Why has Iran taken such deliberate steps to develop power in cyberspace? What ideological principles, issues, and domestic and international events have driven Iran to increasingly invest resources in its cyber programs? What are some of the alternative theories about how Iran has acquired and developed these advanced capabilities? Finally, what is the likely trajectory for Iran and what are its future plans in cyberspace?

IRAN'S GROWING CYBERWARFARE CAPABILITIES

Allegations of Russian tampering with the 2016 US Presidential elections via cyberattacks have highlighted one of the many ways that cyberspace has become a recognized domain for modern international actors to aggressively pursue their national security and foreign policy goals. Over the past decade, a number of other prominent cyberattacks have been revealed to the public, with both diplomatic and economic implications. Stuxnet was widely believed to be a deliberate and effective cyberattack on an Iranian nuclear system, reportedly setting back the Iranian nuclear program by two years (Katz, 2010). North Korea was apparently responsible for a cyberattack against Sony Pictures, allegedly in retaliation for releasing a movie that mocked Kim Jung-Un and whose plot featured an assassination attempt against him (Siboni & Siman-Tov, 2014). North Korea is believed to have penetrated Sony's computer networks, collected sensitive information and released it to the public, and destroyed other valuable corporate data as part of this operation. China is believed to have been behind the 2015 cyberattacks on the Office of Personnel Management that resulted in a data breach of highly sensitive information on approximately 4.2 million Americans (OPM: Data Breach: Hearing before the Committee on Oversight and Government Reforms, 2015). For a number of increasingly capable nation-states, cyberspace has become a place to exert influence, conduct espionage and engage in sabotage.

In 2016, the World Economic Forum declared that along with Russia, the United States, China, Israel and the United Kingdom were the top five cyber superpowers in the world (Breene, 2016). Furthermore, as the *Financial Times* noted around the same time, "Iran is rapidly emerging as the sixth member of the cyber superpower club" (Jones, 2016). As the *Times* also pointed out, Iran's power in cyberspace has been aggressively growing and has not always been so strong. The American Enterprise Institute and the Norse Corporation together released a report in 2015 describing Iran's evolution of capabilities from unsophisticated, petty attacks on websites causing minor annoyances to much more complex, clandestine efforts to collect highly sensitive information, wreak havoc and cause destruction through cyberspace:

> *Iranian hackers have progressed far beyond website defacing or distributed denial-of-service attacks, although they boast about both. This study found evidence that they are developing sophisticated software to probe US systems for vulnerabilities, inject malware, and gain control. Their attacks are designed to blend into normal traffic and use compromised third-party systems for obfuscation. Iranian hackers are becoming a serious force in the malware world. (Kagan & Stiansen 2015).*

As LTC. Eric Shafa of the Strategic Studies Institute noted, "in late-2011, Iran invested at least $1 billion dollars in cyber technology, infrastructure, and expertise. In March 2012, the Islamic Revolutionary Guards Corps (IRGC) claimed it had recruited around 120,000 personnel over the past 3 years to combat 'a soft cyberwar against Iran.' In early-2013, an IRGC general publicly claimed Iran had the 'fourth biggest cyber power among the world's cyber armies.'" (Shafa, 2014). Gabi Siboni, a cyberse-