2005-09

Developing a reliable methodology for assessing the computer network operations threat of Iran

Smith, Matthew N.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A RELIABLE METHODOLOGY FOR ASSESSING THE COMPUTER NETWORK OPERATIONS THREAT OF IRAN

by

Jason P. Patterson
Matthew N. Smith

September 2005

Thesis Advisor:	Dorothy Denning
Second Reader:	James Ehlert

Approved for release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Developing A Reliable Methodology for Assessing the Computer Network Operations Threat of Iran			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jason Patterson Matthew N. Smith			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis is part of a project at the Naval Postgraduate School to assess the Computer Network Operations (CNO) threat of foreign countries. CNO consists of Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND). Threats to the nation's critical infrastructures come from an adversary using CNA and CNE to degrade, deny or destroy access to the information systems they depend upon. Defensive capabilities are also addressed since exploitation, attack, and defense are inherently related. The result of a successful cyber-attack upon these critical infrastructures has the potential to cripple a country's communications and other vital services, economic well-being, and defensive capabilities.

The goal of this thesis is to develop a methodology for assessing the CNO threat of Iran. The methodology is based on open sources that can supplement classified information acquired by the intelligence community.

14. SUBJECT TERMS Computer Network Operations, CNO, Computer Network Attacks, CNA, Computer Network Exploitation, CNE, Computer Network Defense, CND, Iran			**15. NUMBER OF PAGES** 85 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for release; distribution is unlimited

DEVELOPING A RELIABLE METHODOLOGY FOR ASSESSING THE COMPUTER NETWORK OPERATIONS THREAT OF IRAN

Jason P. Patterson
Lieutenant, United States Navy
B.S., University of Illinois at Urbana-Champaign, 1999

Matthew N. Smith
Lieutenant, United States Navy
B.S., United States Naval Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Authors: Jason P. Patterson
Matthew N. Smith

Approved by: Dr. Dorothy Denning
Thesis Advisor

James F. Ehlert
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis is part of a project at the Naval Postgraduate School to assess the Computer Network Operations (CNO) threat of foreign countries. CNO consists of Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND). Threats to the nation's critical infrastructures come from an adversary using CNA and CNE to degrade, deny or destroy access to the information systems they depend upon. Defensive capabilities are also addressed since exploitation, attack, and defense are inherently related. The result of a successful cyber-attack upon these critical infrastructures has the potential to cripple a country's communications and other vital services, economic well-being, and defensive capabilities.

The goal of this thesis is to develop a methodology for assessing the CNO threat of Iran. The methodology is based on open sources that can supplement classified information acquired by the intelligence community.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACM	Association of Computing Machinery
AICTC	Advanced Information and Communication Technology Center
ATM	Asynchronous Transfer Mode
AUT	Amirkabir University of Technology
B.A.	Bachelor's of Arts
B.S.	Bachelor's of Science
BHST	Iran Babol-Hackers Security Team
CAINE	Conference for Computer Applications in Industry and Engineering
CMM	Capability Maturity Model for Software
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
DCI	Data Communications Company of Iran
DDoS	Distributed Denial of Service
DST	Ashiyane Digital Security Team
GEO	Geostationary Earth Orbit
GSTP	Guilan Science and Technology Park
IAEA	International Atomic Energy Agency
IASP	International Association of Science Parks
ICEE	International Conference on Electrical Engineering
ICPC	ACM International Collegiate Programming Contest
ICT	Information and Communication Technology
ICTI	Information Communication Technology Institute
IHS	Iran Hackers Sabotage
IN	Intelligent Networks
IP	Internet Protocol
IRICA	Iranian Customs Administration
ISP	Internet Service Provider

ITRC	Iranian Telecommunication Research Center
ITU	International Telecommunications Union
IUT	Isfahan University of Technology
J. UCS	Journal of Universal Computer Science
M.A.	Masters of Arts
M.S.	Masters of Science
MPO	Management and Planning Organization
NASA	National Aeronautics and Space Administration
PDN	Public Data Network
PTP	Pardis Technology Park
PTSN	Public Switched Telephone Network
QoS	Quality of Service
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SIGSAC	Special Interest Group on Security, Audit, and Control
SUT	Sharif University of Technology
TAE	Trans-Asia Europe Project
TCO	Technology Cooperation Office
TERNENA	Trans-European Research and Education Networking Association
TWA	TransWorld Airline
USG	United States Government
VPN	Virtual Private Network
WMDs	Weapons of Mass Destruction

ACKNOWLEDGMENTS

We would like to thank Dr. Dorothy Denning and Mr. James Ehlert for their expertise and insight during this study. It has been a very challenging and rewarding experience for both of us. We are very grateful for their assistance and patience.

From Jason: To my wife, Cassie and son, Cooper. Thank you for your love and support throughout this experience. Your sacrifice is recognized and greatly appreciated. I love you both.

From Matthew: Thank you to my family for their love and understanding.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

With the conclusion of the Cold War, the United States has become a supreme power that exerts political and military influence over world affairs. Rogue nations do not have the means or the capabilities to confront this hegemonic power with conventional warfare methods. Instead they look to develop asymmetric capabilities to combat an overwhelming adversary. Opposing nations could benefit greatly by developing a cyber attack capability that could potentially deal a crippling blow to critical infrastructures of the United States. Although the US is considered to be on the forefront of Computer Network Defense (CND) technology, the worldwide availability of the Internet and the constant stream of newly discovered vulnerabilities in software make it a potentially easy target for exploitation and attack.

Attacks on the critical infrastructures are becoming more prevalent as access to the Internet is expanded. It is in a foreign country's best interest to develop a capability to degrade, deny, or destroy an adversary's access to information. According to Richard Clark, a former United States Government (USG) counter terrorism and cyber security advisor, rogue countries such as Iraq and North Korea have spent hundreds of millions of dollars to develop an atomic bomb. He postulates that engaging in a cyber war would cost less and doesn't require the support of a nation state. [Vamosi 02] However, in spite of this prediction and others like it, very little is known with respect to the Computer Network Attack (CNA) and Computer Network Exploitation (CNE) capabilities and intentions of foreign states. It is unclear whether hacking activity is state sponsored or the actions of unorganized, mischievous hackers, or perhaps even a combination of both. Clearly, a better understanding of the CNA/E activities of a given nation state would assist in our development of a robust and proactive CND capability.

B. OBJECTIVES

This thesis is part of a project at the Naval Postgraduate School to assess the CNA/E threat of foreign countries. The definition of Computer Network Operations

(CNO) consists of CNA, CNE, and CND. The threat to critical infrastructures comes from CNA/E. Since CND capabilities are inherently related to exploitation and attack, the thesis also addresses defensive capabilities. The goal is to develop a methodology and apply it to selective countries. The methodology is based on open sources that can supplement classified information acquired by the intelligence community An analysis of North Korea has already been completed. [Brown 04] This thesis is intended to develop the methodology for an analysis of Iran's CNA/E capability.

The methodology used for this thesis consisted of analyzing four areas of activity relating to a country's CNA/E capabilities and intentions. Each of these is discussed in a separate chapter. The first chapter addresses the Iranian information technology infrastructure. The chapter describes its capabilities and limitations. The chapter also discusses laws and regulations associated with Internet use, including computer crime laws, and Iran's current diplomatic and ideological relationships with the United States and other countries. The second chapter is an analysis of academic activity and public community. It examines the involvement of Iranian academia with respect to education and research relating to CNA/E. The third chapter is an examination of the government activity in the development of a CNA/E capability. It shows the Iranian government's interest in expanding the IT infrastructure and its role in elevating Iran's IT reputation in the worldwide scientific community. The fourth chapter examines the CNA/E activity within Iran. It discusses the various motivations of hackers, provides some examples of hacking groups within Iran, and explains the difficulty in identifying these Iranian hackers.

This research consisted of open source unclassified intelligence collection and analysis. Much of the research was conducted using Internet sources, including websites, discussion groups, and web logs. This methodology will be presented in a manner that can then be applied in the analysis of another country of interest.

II. BACKGROUND

A. INTRODUCTION

This chapter provides the background information to help frame the scope of this research. It will examine Iran's foreign policy, information technology infrastructure, and existing legal framework. In addition, it attempts to provide insight into Iran's motive and technological capability to conduct computer network operations and attack against potential adversaries.

B. FOREIGN RELATIONS

In order to develop an understanding of Iran's motivation for developing a cyber-attack capability, a closer look at Iran's foreign policy is required. After World War II, Iranian leaders had aligned themselves with the Western World. This was due to the ideological commonalities they shared and the perceived aggression from the former Soviet Union. This relationship with the western world dramatically changed when the Shah of Iran was overthrown in 1979. After the victory of the Islamic Revolution and the hostage crisis in 1979-1980, foreign relations with the western world have been on a downward spiral. The leaders of the revolution were skeptical of the United State's heavy involvement in the region and denounced the United States as the "Great Satan." By the early 80's, most of the political elite inside Iran had accepted this point of view. [LOC 04] Since then, Iran has had a history of challenging the western world and calling for the complete removal of all western interests from the Gulf region. Recent news headlines have highlighted the impending danger of Iran's nuclear program. These reports cite intelligence sources from western countries that claim the existence of secret nuclear weapons material production and testing facilities. Iran claims that these sites do not exist and such ambitions are strictly peaceful to ensure adequate power generation requirements for their developing country. Western policy makers contend that their motives go beyond power production. The International Atomic Energy Agency (IAEA)

and the European Union have been in negotiation with Iran to prevent them from acquiring nuclear weapons. Such negotiations have not been fruitful and have contained terse rhetoric from both sides.

More specifically, the United States has labeled Iran as world's most active state sponsor of terrorism. President Bush has labeled Iran, along with countries such as Iraq and North Korea, as being a member of the "Axis of Evil." [Bush 04] This labeling by the US government brings with it implications of sanctions to include:

1. A ban on arms-related exports and sales
2. Controls over exports of dual-use items, requiring a 30-day Congressional notification for goods or services that could significantly enhance the country's military capability or ability to support terrorism
3. Prohibitions on economic assistance
4. Impositions of miscellaneous financial and other restrictions to include:
    - Requiring the US to oppose any loans by the World Bank and other world financial institutions
    - Allowing families of terrorist attacks to file lawsuits against Iranian diplomats in US Courts.
    - Denying tax credits for income earned in Iran
    - Authority to prohibit financial transactions with Iran without a Department of Treasury license.
    - Prohibition of Department of Defense (DoD) contracts over $100,000 with Iran.

The import and export of technology items are considered dual-use and are therefore prohibited under these sanctions. [USDOS 03] Iran has consistently pursued relationships with other state sponsors of terror and terrorist organizations. In February 2005, Iran and Syria announced that they would form a united front against pressure from the United States and the western world. Syria was the only Arab country that continued warm relations with Iran during the 1980-1988 Iran-Iraq War and has been a strategic ally for years. [AP 05] Iran's connections to former Iraqi leader Saddam Hussein and terrorist organizations has been documented by an Iranian defector and former director of intelligence for the Iranian Revolutionary Guard. Hamid Reza Zakiri described his personal knowledge of Iranian cooperation with other state sponsors of terror and terrorist organizations. For instance, Zakiri tells of the cooperation between North Korea and

Iran. He has personally attended military courses such as psychological warfare, counter espionage, and physical security pertaining to nuclear installations for 40 day periods in North Korea. He goes on to describe Iran's connection with Al-Qa'ida, Hezbollah, and other terrorist organizations. He provides details of Iranian Revolution Guard involvement with terrorist organizations in the 1983 bombing in Beirut and the 1985 hijacking of the TWA airplane resulting in the death of numerous US servicemen. And while Iran did not play an active role in the attacks on September 11, 2001, Zakiri states that the Revolutionary Guard received correspondence requesting assistance from Ayman Al-Zawhairi. He stated that while they were ordered not to assist, they were to maintain relations with Al-Qa'ida for future operations. Furthermore, Iran has assisted with the harboring of many Al-Qa'ida terrorists following OPERATION ENDURING FREEDOM and IRAQI FREEDOM to include the transportation of Osama bin Laden's wife and son to Yemen. Zakiri also speculated that Bin Laden himself may have escaped with the assistance of the Revolutionary Guard. He details relationships with bogus companies headed up by Qusay Hussein since the 1990's to assist with the smuggling of oil. [MEMRI 03] Smugglers of oil from Iraq generally had unrestricted access to Iranian territorial waters. Iran's territorial waters became known as a "superhighway" of smuggled oil due to a smuggler's ability to traverse and exit the entire Persian Gulf inside Iranian territorial waters. These strategic connections with other state sponsors of terror and terrorist organizations detail a foreign policy that is very hostile to the United States and the western world.

Iran has also established military development relationships with other non-western military powers throughout the world. These countries include Russia, North Korea, and China. In mid-2000, Iran announced a "25-year military development program" with Russia, for which very little of the details of the agreement are known. [Billo/Chang 03] To counter the American influence on behalf of Iraq in the Iran-Iraq War, the former Soviet Union saw an opportunity to increase its influence by selling military equipment. After the 1991 Gulf War, Russia had lost Iraq as one of its primary customers of military equipment. Russia was compelled to further strengthen financial ties with Iran to compensate for the closure of its market and to reestablish influence

within the region. The United States had repeatedly tried to convince Russia to cut off military support for Iran with very little success. While the United States has sometimes sanctioned the individual entities that deal with Iran, it has never sanctioned the Russian government. [Katzman 03] Iran and China also have a history of military dealings since the early-80's. To Iran, China is just another source of military equipment that is willing to sell technology needed to counter the perceived US aggression. China does not agree ideologically or politically with Iran, but views the relationship as an opportunity to divert the US military from the China-Taiwan stand-off. Besides obvious revenues from the sale of its military technology, China also has to ensure an adequate supply of oil in a tight market for a growing economy. [Katzman 03] As was the case with Russia, the relationship between Iran and China is mutually beneficial.

The Iranian relationship with North Korea is much more forward than that with Russia and China. Traditionally, North Korea has always aligned itself with countries such as Iran, Syria, and Libya that share its opposition to the policies of the United States. This relationship has been furthered strengthened by the United States' characterization of North Korea and Iran as "rogue states" and institution of trade sanctions against them. [Katzman 03] Although countries such as Iran, Russia, China, and North Korea may not agree ideologically or politically, mutual interests have brought these countries together to compete better in a world currently dominated by the west.

Since the fall of the Shah in 1979, Iran's foreign policy has been extremely critical of the influence of the western world. Iran has shown that it will use any means necessary, including acquiring weapons of mass destruction, to strengthen its position in the world. The western world's heavy reliance on information technology makes cyber-attack by countries such as Iran a likely possibility.

C. INFORMATION TECHNOLOGY INFRASTRUCTURE

As with most developing nations, information technology is just starting to make an impact upon the education, economy, and social values within Iran. With the cessation of hostilities in the Iran-Iraq war in August 1988, the Iranian government set out to develop a plan to restore the Iranian economy. Included within this plan were

requirements for the spread of Information and Communications Technology (ICT). Called the First Five Year Plan, it was adopted by the Parliament in early 1990 and has experienced three iterations since then. The current plan is called the Fourth Five Year Plan and contains the goals for 2005-2010. [OXR 04] The development of information technology in Iran was met with initial resistance, but was followed by a much more rapid growth of adaptation, use and privatization. [Rouhani 00]

The following sections examine different sectors of the information infrastructure.

1. Telecommunications

Iranian telecommunications are currently inadequate, but are being modernized and expanded to not only increase the volume and efficiency of urban services, but also to increase reach to rural areas throughout Iran. The number of main telephone lines has risen dramatically with only 830,000 installed main lines in 1978 [ITU 05] compared to 14.5 million installed lines in 2003. According to the International Telecommunication Union there were 27.06 subscribers per 100 inhabitants of Iran. [CIA 05] While this is still a low penetration factor compared to the developed world, the overall increase has been dramatic. As with most developing nations, demand for cellular phones within Iran has taken off. In 2003, the mobile handset market grew by almost 26% within the African and Middle East region. [AMET 04] This rapid expansion is due to the low cost required to expand cellular phone infrastructure compared to traditional telephone lines. As depicted below, Iran has one of the fastest growing telecommunications expansion rate in the Middle East.

	1990	2003	Percent Increase
Iran	4.04	27.06	669.8%
UAE	24.25	101.68	419.3%
Oman	6.13	31.67	516.63%
India	.6	7.10	1183.3%
US	56.85	116.96	205.7%
Saudi Arabia	7.78	47.65	612.5%
China	.59	42.38	7183.1%

Table 1. Number of Main Telephone Lines and Cellular Subscribers per 100 Population [UNSD 04]

In addition to the rapid increase in telephone and cellular phone access within the country, access to the world telecommunication network has also greatly increased by a combination of satellite and fiber optic connectivity. One such fiber optic line is the Trans-Asia-Europe (TAE) Project. Agreed upon in 1993, it is the world's largest overland fiber-optic system. By following the ancient silk trading route, it provides a link that stretches from China to Europe. The fiber has the capability of up to 622 MBps. Participants in the TAE Project include China, Kazakhstan, Turkmenistan, Uzbekistan, Turkey, Belarus, Poland, Hungary, Austria, Germany, Georgia, Armenia, Azerbaijan, Pakistan, and Afghanistan. The Iranian portion of the fiber-optic line is 721 km and connects Turkmenistan to Turkey. (see Figure 1. below) Another fiber optic line that links Iran to the global communication system is a submarine line that links Iran's southern coast with Fujirah in the United Arab Emirates. It is a 172 km, un-repeatered line that provides a direct connection supporting a bandwidth of up to 140 Mb/s. These fiber optic lines assist with providing Iran the much needed bandwidth of a developing nation. [ORN 99]

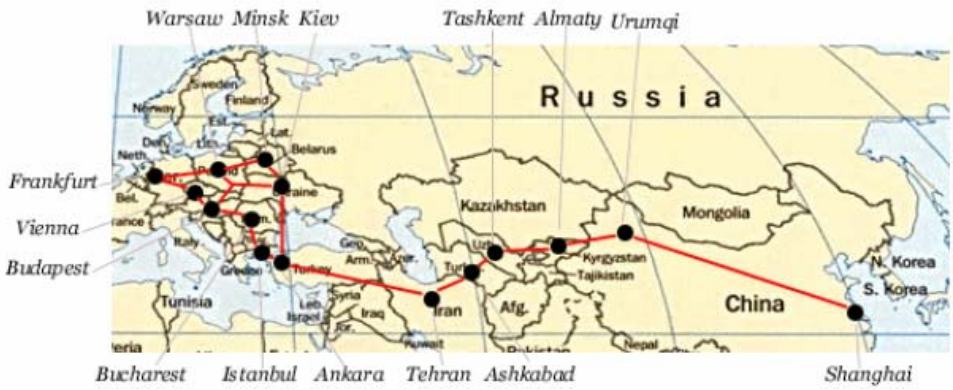

Figure 1. TAE Fiber-Optic Line [ORN 99]

The final link of Iran's telecommunication system to the world is through satellite technology. Prior to recent developments, Iran's satellite communication ability was limited to using Inmarsat land earth stations connected to commercially operated satellites over the Indian Ocean that routed calls to terrestrial phone lines. Since the 1970's, Iran has considered creating a government-owned GEO (Geostationary Earth Orbit) communications network. Through initial planning agreements in 1993, France, Italy, Russia and China, are said to be assisting with the development of the Zohreh (Venus) systems of satellites. This system of 2 satellites will expand Iran's telecommunication capability, provide military and data communications, and improve Iran's broadcasting capability. The ground infrastructure needed for this system will include five land stations, 135 primary and secondary stations, 27 zonal stations, 31 community stations, and 1,374 rural stations. [ORN 99] In January 2005, a contract was signed in Tehren for the delivery and launch of the Zohreh satellites by a Russian subcontractor called The Academician Reshetnev Applied Mechanics Research and Production Association. It is reported that it will take 30-36 months from initial building operations to final acceptance. [SAT 05] Iran's interest in space is still in the early development phase and aerospace companies throughout the world are willing to provide the expertise to expand Iran's capabilities.

2. Internet Infrastructure

Like the rest of the world, internet usage in Iran has exploded. Iran's first use of the internet was spearheaded by the Institute for Studies in Theoretical Physics and Mathematics (IPM) during the early 1990's. The IPM established a link through the BITNET network through Iran's membership in the Trans-European Research and Education Networking Association (TERENA). The link later developed into a full-fledged internet connection with acceptance of Iran as a Class C node. Initially the primary users were academic and research institutions, but domestic Internet connections have grown rapidly. At times, growth of the Internet has placed Iran among the top countries for the rate of growth for internet access. [Arabshani 97]

The first Internet Service Provider (ISP) in Iran was the Data Communication Company of Iran (DCI). As of 2000, this government-owned company was the largest ISP in Iran. There are well over 30 ISP's that provide internet service. Some of the more popular services are Neda Rayneh, IRNET, Virayeshgar Corporation, Apedana, and Pars Suppala. [Rouhani 00] According to the ITU, internet users per 10,000 inhabitants rose from 155.57 in 2001 to 723.66 in 2003. The number of internet hosts has also risen dramatically. In 2001, there were .38 hosts per 10,000 inhabitants. This rose to .76 hosts per 10,000 inhabitants in 2003. [ITU 05] Recently the French company Alcatel won a contract to provide the first DSL network in Iran. Alcatel will provide and support access to 100,000 DSL lines over the next three years. [AMET 04-1] Prior to this, access to end users throughout the country was strictly via a Public Switched Telephone Network (PSTN) or the Public Data Network (PDN). The PSTN provides 56kbps dial-up access to people willing to pay for service. Access to the PDN is mostly limited to academic, government and some private entities. Originally, this link used multiple 64kps ISDN lines (see below), but was upgraded with a combination of fiber optic backbones and T1 lines. [ORN 99] As of 1999, only 170 locations throughout Iran had access to this technology, but that number has grown dramatically since then. With the announcement in early 2004 that Alcaltel was going to provide the first DSL networking Iran, access to high-speed internet and information technology promises to improve.

Use of the internet has also spilled into the political arena of Iran. While still a very censored medium within the country, the Internet provides more freedom for people to speak out when compared to the state-controlled print, television, and radio media. Officials running for elections have begun to see the power that access to the internet can provide for a campaign. During the May 1997 presidential campaign, the two presidential candidates, President Khatami (http://www.khatami.com) and the conservative candidate Ali Akbar Nategh Nouri (http://nategh.co.ir), used the World Wide Web to disseminate their messages. In addition to this, the results of the election were posted "live" on the website of the Iranian government at www.netiran.com. [Rouhani 2000, 27] The Internet has also become the voice of many people on the political spectrum. The use of web logs has exploded in the country. These "blogs," which blur the line between reporting news and expressing political views, have become the voice of reformists unsatisfied with the current government. The government has actively attempted to censor the expression of these web journalists. The use of the Internet for Iranian politics will be examined further in the next chapter.

Figure 2. Iran's inter-city ISDN lines as of 1997. This network has since been expanded to include other cities such asYazd, Zahedan, Arak, and Rasht [ORN 99]

Internet usage in Iran has become very controversial. The debates are similar to those within most countries throughout the world about the social impact of the internet. The conservatives are concerned with the negative social impacts that the internet brings to an Islamic society. They believe that the influence of westerns ideals, drugs and sex will become the demise of the Islamic state. Furthermore, they believe that the internet will foster immorality and the "Americanization" of the Iranian youth. While many conservatives realize that the internet is necessary to continue technological development within Iran, their argument is that internet regulation is necessary to protect the Islamic society. The more liberal factions within the country believe that such restrictions will obstruct the learning development of people and that the individual or their family should

limit access to improper information. They stress the importance of the internet for its economic advantages, expeditious transactions and democratic access that it offers. [Ebrahimian 03] These issues are not unusual and are being faced by countries all over the world. However, they become much more dangerous in a theocracy such as Iran in which censorship becomes a very likely possibility.

3. Hardware Industry

When compared to Iran's successful industrial sectors such as oil and natural gas, development of Iran's technological manufacturing capability has not been as successful. Iran's automobile and military production capability has attracted some foreign investment, but Iran's attempt to create a high technology electronics industry has been unsuccessful. Imported hardware is in limited supply due to import and export trade regulations and taxation. Domestic industries in need of IT products find that there is a shortage of national producers of computer and communication hardware. On a policy level, a prevailing barrier to technological advancement is the menial effort to attract private sector involvement. This is due in part to the state's mismanagement of legal and regulatory procedures. The state controls all national business activities under a confusing regulatory framework. During the 2000 presidential elections, Tehran police closed all the cyber-cafes with broadband access due to political reformists gaining popularity from their effective use of the internet. The government cited the lack of necessary permits as the reason why the cafes were shut down even though there were not any laws requiring permits. Actions like these create an atmosphere of uncertainty for willing investors. There are increasing efforts for privatization of state run sectors of the economy. In October 2004, the Management and Planning Organization (MPO) had drawn up a 20-year strategy for economic, social, and cultural development which can only be accomplished by privatization. The Supreme Leader Ayatollah Ali Khameni has ordered this plan to take effect commencing 2005. [Ebrahimian 03] It is believed that privatization of industries will reduce both the amount of government censorship and regulation and is the only way to spur economic and commercial development.

Iran's restrictive trade policies also make foreign investment very difficult. Taxation on imports are often levied in an inconsistent and undefined manner. For instance, Iran imposes heavy import duties on computer peripheral products such as printers and displays. Businesses that can afford to purchase approved point of sale systems cannot afford to purchase the printers or displays that are needed for them. Increases in productivity that are gained from the point of sale system are lost in the inability to print a receipt. [Ebrahimian 03]

Iran's contradictory legislative actions have also deterred foreign investment. For instance, Iran agreed to a contract in early 2004 with the Turkish cell phone company Turkcell to be the first foreign nation to provide nation-wide cellular phone service. Several months later, the Iranian legislative body voted to sharply cut the company's share in the multi-billion dollar deal. The original deal consisted of an alliance of four companies; 51% of the shares were to go to Turkcell, 20% to two Iranian communications companies, and 9% to Nokia. Instead, the Parliament voted to increase the Iranian portion of the deal to 51% and the remainder to go to Turkcell and Nokia. This has caused Turkcell to reconsider and possibly withdraw from the deal. This type of contradictory behavior creates a uncertain business environment and makes future foreign investment in any industry much more difficult.

4. Software Industry

Since the late 90's and early 00's there has been a demand from Western firms to seek countries with highly trained software engineers to outsource the development of coding and thus become more competitive in the market. Developers have found that outsourcing can be much more cost efficient than very expensive domestic employees. Countries from all over the world are competing for this outsourcing and Iran is no exception. The Iranian software industry suffers many problems that hamper its development as a competitor on the world market. It is estimated that there are 20,000 working in the software industry with about 200 companies involved in software development. The required technology level of hardware in Iran is generally lacking. Application development in some cases is still based in MS-DOS. There is widespread

lack of software management expertise. Even with high technical skills, large-scale projects often fail due to poor management. There are no copyright protections of foreign-produced software in Iran, so pirating is widespread. Many software companies cannot afford or are unwilling to buy software tools for development and will in turn use pirated version of these tools. Developers are unable to receive technical support from the manufacturers for these pirated tools, so they rarely understand the full capabilities of the packages. While there is an eagerness to explore the software export market, there is a lack of expertise to develop the necessary relationships needed for foreign investment. The US trade embargo has also hampered the software export market. In addition, there is an inability to develop a desirable portfolio of services to export to overseas companies. Development of products for exports requires a thorough understanding of the needs of the world market. Iran has not been able to capitalize on the same industry that other countries such as India have due to the general consensus that "lower-level" service does not fit in the with "Iranian national character." Instead, Iranians preferred to focus on "high-level" application work. Over the years, India has gradually been able to break into developing more complex applications by creating a reputation on the world market as being proficient in software development. Another lost opportunity for Iran is the lack of collaboration between software companies and universities. Even with 70% of software companies centered around Tehran, there is very little coordination amongst them. Coordination promises to improve with the construction of Technology Park in Tehren that will attempt to bring researchers and technology businesses together. Currently, there are no Iranian companies with standard certifications such as ISO9000 or Capability Maturity Model for software (CMM). Experiences in India have shown that these standards reassure foreign companies wishing to pursue outsourcing. [Nicholson/Sahay 03]

Like the hardware industry, the software industry suffers greatly from a lack of a clear policy from the government. There have been several plans and statements describing the importance of establishing a strong software industrial base, but the general consensus from those in the industry is that these are rarely followed through. The desire to become more competitive on a global scale is there, but there are technical,

social, and political barriers to overcome. These barriers, at least in the near term, prevent Iran from establishing a strong foothold in the world software market.

D. LEGAL FRAMEWORK

There are very limited and inconsistent laws in Iran governing the protection and use of Information and Communication Technology (ICT). The first law for the legal protection of software products was enacted in the year 2000. This law, called "Support for Computer Software Developers," gave legal protection of software copyrights to domestically produced software. Software applications that are produced and properly registered with the Supreme High Council of Informatics are legally protected from pirating. Even with this law, software pirating is still widespread since it is rarely enforced. While this law establishes legal protection for domestic software, there is no protection for imported software. In 2003, a bylaw was passed defining the procedure for the execution of ICT expansion. The specifics of the bylaw include an implementation of e-government initiative and expansion of ICT in education. [Sanaray 05] While these initiatives are a good start, there are still some issues that need to be addressed. There is no definition of cyber-crime and therefore no laws to prevent it. In addition to this, copyright laws need to be enforced and protections expanded to include foreign intellectual property. The Iranian government has promised to improve legislation to provide a more secure investing environment for foreign interests. Without clear definition of cyber-crime laws, Iran's internet community runs rampant in lawlessness and ensures that hackers will go unpunished for their actions.

E. CONCLUSION

This chapter discussed the background necessary for the basis of this thesis. It examined Iran's foreign policy, information technology infrastructure, and legal framework. The political alignments, basic technological capabilities, and legal consequences provide insight into the ability and motivations for state-sponsored hackers to conduct cyber-attack against the United States.

III. ACADEMIC ACTIVITY AND PUBLIC COMMUNITY

A. INTRODUCTION

This chapter describes Iranian academic and public community involvement with respect to Computer Network Attack and Exploitation capabilities. It will discuss the Information Technology related educational opportunities available to Iranians as well as any activity in the public community that may be related to developing a cyber-attack capability.

B. IRANIAN ACADEMIC OPPORTUNITIES

In order to assess Iran's cyber attack capabilities, a thorough examination of its academic institutions must be conducted. Iran has an extensive academic research system spread throughout the country. Like other developed nations, students have the opportunity to get undergraduate and graduate educations in major fields ranging from philosophical areas such as Islamic studies to sciences such a mathematics, engineering, and physics. In particular, access to information technology related educations is widely available to those students that qualify for entry based on national exams. The analysis provided is limited to the major institutions that had public information available.

1. Sharif University of Technology

Located in Teheran, Sharif University of Technology is one of the largest engineering schools in Iran. It was established in 1966 under the name of Aryarmehr University of Technology. When it was first founded there were 54 faculty members and a total of 412 students. In 1980, the university was renamed Sharif University of Technology. SUT now has a total of 300 full-time faculty members, approximately 430 part-time faculty members and a population of about 8,000 students. Undergraduate and graduate degrees are offered in computer engineering and software engineering.

Within SUT is the Advanced Information and Communication Technology Center (AICTC). This center conducts research in various aspects of Information and Communication Technology. Its faculty educational backgrounds range from computer

science, information technology, engineering, and mathematics from both western universities and Iranian universities. Several faculty members had degrees from U.S. universities such as University of Illinois and Pennsylvania State University. Some of the research that the center conducts includes video communication in wireless networks such as scalable video coding, error concealment and post-processing techniques, rate control, wireless media streaming, transporting video over 3G wireless networks, and mechanisms to improve multimedia applications throughput over wireless links. The center is also heavily involved in the development of Farsi Linux, a government directed OS initiative to lessen the dependence of western based software makers. [SHARIF 05]

While some of the professor's biographies included interests in computer security, there were a couple of faculty members that stood out. Professor Shahram Bakhtiari shows an extensive interest in computer security topics. He received his M.S. and Ph.D from Wollongong University in Australia. He has published extensively in journals and conference proceedings such as the Journal of Universal Computer Science (J.UCS) and ACM Special Interest Group on Security, Audit, and Control (SIGSAC) Review. Some interesting topics of his publications are "Keyed Hash Functions," "Practical and Secure Message Authentication," and "On the Weaknesses of Gong's Collisionful Hash Function." Some of the courses he teaches are called Systems and Networks Security, Advanced Topics in Programming, Data Structures and Design of Algorithms, and several programming courses in different languages. A course syllabus of the Systems and Networks Security course was also posted on his site. The course description is quoted below:

> In this course we study the applications of cryptography in systems/networks security and show how systems may encounter unauthorized access by intruders. Due to the extensive use of computer networks and the Internet, there exist a range of methods that intruders might use to access the information and files stored on a particular host. Students who take this course become familiar with methods of attack and the ways to protect systems and networks.

He also posted links to the presentations that he uses for this class. One such presentation was titled "Hacking Techniques." However, the links were broken, so the presentation could not to be viewed. [Bakhtiari 01] Also found through a simple google search of

“sharif university security” was the resume for Sauleh S. Etemady. He recently completed his M.S. in Electrical and Computer Engineering from Michigan State University. His undergraduate work was performed at SUT. While a student at SUT he taught courses such as Network Security, Securing and Optimizing Linux, and TCP/IP Administration for the AICTC. His publications include “Proposal for Information Security Center,” “Mail Security Solutions,” and “Security Aspects of Operating Systems.” While he is no longer affiliated with SUT, his computer security background was established during his time at Sharif as a student. [Etemadi 05] Another interesting personal web page found from SUT was that of Hashem Habibi who is currently a student studying for his Masters degree in Software Engineering. His personal page consists of links to pages of fellow classmates, photo galleries, and links to various web logs and hacking sites. His page also mentions a Network Security Center at SUT with pictures of some of the members of the center, however, a website for the Network Security Center was not found. Another biography found was that of a PhD candidate named Mohammad Abdollahi Azgomi. He has numerous papers published and has taught several courses on computer security topics. Some of his more notable publications include “Design and Implementation of a Firewall in Computer Networks,” “Security Enhancement for Network Services,” and “Modeling and Analysis of Reactive Systems.” According to his resume, he has consulted for the government on network security matters in the Iran Expediency Council Secretariat, State Organization for Registration of Deeds and Properties of Iran, Iranian Customs Administration (IRICA). He has taught several programming and simulation courses at Sharif and other Iranian universities. [Azgomi 05]

Sharif University of Technology has been engaged in extensive computer security research and education. Several faculty members and students have focused on computer security topics. There are also courses in computer security. While the principles of computer security are being taught to students, there was no evidence that the school was using this education to promote hacking in any way.

2. University of Tehran

The main part of the University is located at the center of Tehran. Some of the faculties and research centers are also located in Karaj, Qom, Pakdasht, Sari and Kheyrood Kenar. The University has 1500 faculty members. At present, this University admits students to 111 B.A./B.S. degree programs, 177 M.A./M.S. degree programs and 156 Ph.D. degree programs. The educational capacity of this university is about 32 thousand students. According to the university's website, 340 foreign students also study at the University.

Like other universities, the information technology related faculty has wide ranging educational background in fields such as computer science, computer engineering, and mathematics. Degrees offered include software engineering and computer engineering. The university's advertised research projects include mostly electrical and computer engineering topics. One particular project listed was called "Iran National Grid Blackout, Power System Protection Point of View." There was not any additional information to ascertain if this research was pertaining to defense of Supervisory Control and Data Acquisition (SCADA) systems. The University does conduct some defense related research as a master's thesis was found that focused on improving missile accuracy. The school's website had very little information regarding the specifics of the degree programs or individual course information. [University of Teheran 05]

3. Amirkabir University of Technology

Also located in Tehran, the Amirkabir University of Technology was established in 1958. The university's website boasts close ties with the Ministry of Science, Research and Technology. There are currently 6400 students enrolled in 132 disciplines. It has 14 engineering groups, 7 research centers, and an ACM chapter. It offers undergraduate and graduate degrees in Information Technology and Computer Science. Although this school has a relatively low enrollment compared to other Iranian institutions, its research seems to be more focused on computer security topics. Within

the Computer Engineering and Information Technology department is the Data Security Research Laboratory. The website's description of the laboratory's mission is quoted below:

> The role of this laboratory is to help promoting research and innovations on computer, information and communications security, and help training engineers and scientists in related areas, while there will be special attentions on design and analysis of cryptographic algorithms, design and analysis of secure protocols with public use, developing hardware and software for secure data communications, processing and computations, and also for secure speech and image communications and processing, and design and implementation of secure computer systems, e.g. secure o.s. However, all aspects of cryptology and computer and communication security are interested research objectives of the Lab.

There is evidence that this security center actively attempts to identify vulnerabilities in software systems. A posting was found on the New Order security site (neworder.box.sk) from April 2003 from Haamed Gheibi and Salman Niksefat of the Data Security Research Laboratory housed at Amirkabir University of Technology. They claimed in the post to find a Microsoft Windows SMB flaw. [NEW 03] Unsuccessful attempts to gain the attention of Microsoft through emails and phone calls warranted them posting this information on the Bugtraq mailing list. Replies to the Bugtraq posting claimed that this exploit has been used before and that this vulnerability can be corrected by changing the LMCompatabilitylevel to a higher level as directed in the Windows 2000 Hardening Guide. [Bugtraq 03] Their attempt to contact Microsoft prior to publishing the flaw suggests that he was not maliciously subverting the software, instead attempting to get the vulnerability fixed. Gheibi also represented Amirkabir in the 2003 ACM International Computer Programming Contest held in Tehren, which is explained in greater detail in a following section. [ACMICPC 03]

As with other universities, the faculty educational and research vary within the fields of information technology and computer sciences. One particular faculty member that stood out was Professor Mehran Soleiman Fallah. His interests and educational background are exclusively in the computer security field. His PhD dissertation was an analysis of denial of service attacks and a determination of the weaknesses of the protocol

upon which the attacks were carried out. Other faculty members also listed computer security as an interest, but Fallah was the only one who exclusively researched in this field.

4. Isafahan University of Technology

Located in the city of Isafahan, this university has about 7000 undergraduate and nearly 2000 graduate students studying Agriculture, Engineering, Basic Sciences and Natural Resources. Within IUT is the Information and Communication Technology Institute (ICTI). Research areas within the ICTI include distributed system development, management information systems, and computer networks. No specific information was found regarding specific degrees, research or classes in computer or network security related fields. [IUT 05]

In September 2005, the university will host the 3rd Annual Iranian Society of Cryptology Conference. Notable conference topic areas include cryptographic algorithms, digital signatures and hashing algorithms, PKI, network security, firewall and access control, stenography, electronic security laws and legal issues, and intrusion detection systems. Committee members for the conference include numerous professors from IUT as well as from other Iranian universities. The conference offered an open invitation to anyone wishing to attend. There does not appear to be any published limitations on conference attendants. [ISCC 05]

5. University of Isfahan

Located in the city for which it is named, the University of Isfahan has a student population of 14,000. It has 450 faculty members and a wide variety of academic majors. It offers curriculums in information technology, computer science, and computer engineering. As with the other universities, faculty member have varying educational backgrounds. Research interests listed by faculty biographies cover traditional research areas expected from any major university. Three professors focused on computer security research. The biography of Professor Behrouz Tork Ladani lists formal specification and verification, cryptographic protocols, information system security

analysis and design, information security standards and applications, network security, and Virtual Private Networks (VPNs). He has several papers written in the same subject areas for various security conferences that were held both inside and outside Iran. Another faculty member, Professor Ahmad Baraani-Dastjerdi, is also heavily interested in research areas such as security in object-orientated databases, cryptography, security in computing, and computer science. He also has many papers written that support his research in those areas. A third faculty member, Professor Shahram Bakhtiari has research interests of network security, VPNs, and cryptologic protocols. He also teaches artificial intelligence, formal methods, and cryptology and distributed security system classes. He has published numerous security related articles for various journals and conferences. [Bakhtiari 01]

Graduate and undergraduate degrees offered include Computer Engineering, Software Engineering, and Information Technology Engineering. More specific information regarding research areas or class descriptions required intranet access.

There are many other universities within Iran. The institutions listed above had the most substantial information technology, computer science, or software curricula of those websites examined. However, access to information varied. Some institutions required privileged access to view information pertaining to research programs, while others had inoperable websites. In general, Iranian academic institutions exhibit ongoing research interest and education in computer security related topics. The institutions' faculty had a wide range of educational backgrounds to include western universities. The information available shows Iran's academic community does not exhibit any activity outside the norm of typical academic institutions. No evidence was found from academic institutions of open government sponsorship to develop an Iranian cyber-attack capability.

C. INFORMATION TECHNOLOGY ASSOCIATIONS AND PUBLICATIONS

Commensurate with the national goal of becoming a leader in information technology in the Middle East, there is a substantial network of information technology

associations and publications. Participants in these publications and associations come from the academic and business communities of Iran. Web sites and print publications promoting scientific exchange are abundant throughout the country.

There are a number of computer-related associations in Iran. Participation in these societies consists of professionals and researchers from all over the world. Some of these are chapters of world-wide associations while some are strictly focused on Iranian Information Technology. For instance, the Association of Computer Machinery has a professional chapter located in Tehran and student chapters at Sharif University of Technology, Amirkabir University of Technology and University of Qazvin. These chapters hold workshops, social gatherings, and discussions regarding the advancement of computing. Members from these chapters actively contribute to ACM publications.

ACM chapters within the country also compete in the yearly ACM-International Collegiate Programming Contest (ICPC). The 29th Annual World Finals were held in Shanghai, China in April 2005. International teams including some from China, Russia, and Korea competed. Also attending were top US Universities such as Duke, Massachusetts Institute of Technology, and University of Illinois. Iran sent teams from Sharif University of Technology and Amirkabir University of Technology. AUT and SUT tied for 17th place, ahead of all US university teams. [ACMICPC 05] There have also been a lot of Iranian schools represented in previous regionals. Sharif University of Technology is hosting the Asia regional contest for the next ACM-ICPC competition in November 2005.

There are also societies within Iran that focus exclusively on national information technology issues. A comprehensive list of these societies can be found at the Pars Times (www.parstimes.com). Numerous scientific associations and institutions are listed in a wide range of fields. Some of these relating to ICT include the Iran Informatics Companies Association, Information Technology Council, Iranian Organization of Scientific and Technical Research, and the Iran and Information Society. The Academic Center of Educational, Culture, and Research hosts a website that catalogs papers submitted to various academic journals from Iranian researchers.

(http://www.sid.ir/En/Index.asp) It contains 16740 documents in many fields including Information Technology.

There are also several IT-related online news magazine publications. These publications include PC World Iran (http://www.pcworldiran.com/) and the ITNA (http://itna.ir/). These publications are geared to researchers, professionals, and consumers with an interest in the field. These sites are similar to those such as CNET.com or PC Magazine found in the US. In addition to magazine publications, most major newspapers have science and technology sections that discuss news and advancement within the industry.

The information technology publishing within Iran is quite extensive. There is an obvious interest within the country to disseminate and exchange information related to IT. Iranian scientists and professionals actively participate in both Iranian and world-wide associations. Their participation is measured by active contributions in peer-reviewed academic journals, newspapers, and computer related magazines.

D. IRANIAN PUBLIC INTERNET COMMUNITY

As access to technology increases, so does participation on the Internet within Iran. The Iranian theocracy is trying desperately to balance the need for more information exchange while maintaining control of a growing opposition. Groups opposing the Iranian government are using the Internet as a medium of communication. A rapidly growing virtual community of people who are openly exchanging ideas has become a tool for the political opposition. Contrary to government attempts to shut them down, reformists continue to use web logs to voice their opinions. In addition to Iranian politics, the Internet has become the gathering place for those with an interest in network security. These include both blackhat and whitehat groups. Whitehat hackers identify security weaknesses in a computer system or network, but instead of taking advantage of it, expose the weakness in a way that will allow the system's owner to correct it. On the other hand, blackhat hackers identify weaknesses and vulnerabilities in the same manner, but instead exploit the weakness for a variety of reasons. This section will examine

political websites, web logs and white hat activity. Blackhat activity within Iran will be examined in greater detailer in subsequent chapters.

1. The Internet and Politics

Over the last 10 years, an increasingly powerful reform movement has taken root in Iran. Experts have begun to question whether the Internet has been critical for this development. As previously discussed, websites promoting political opinions have become commonplace. The government has tried to block access to these sites, but as Dr. Payman Arabashi, an expert on Iranian telecommunications stated in an interview, "web page content monitoring is not easily regulated. Although all ISPs in Iran do provide web hosting for their users, many users choose to use free web hosting services abroad…So as long as you can get on the Net, you can pretty much do whatever you want, including setting up web pages outside of Iran, or surfing to any sites that may be 'blocked' using a variety of proxy and/or annonymizing services [such as safeweb.com]." [Mazaar 02]

Numerous Iranian political websites have been published on the Internet. Some of the more significant of these are Presideent Khatami at http://www.president.ir/; the reformist parliament at www.majlis.irl; a website from the 2001 presidential election http://www.entekhab80.20m.com/; outspoken critic of the current regime and Shi'ia cleric Ayatollah Hussein Ali Montazeri at http://www.montazeri.com; and the Supreme Leader Ayatollah Khameini at http://www.wilayah.ir/. The importance of this new medium is beginning to be recognized as more candidates seek the support of the youth of Iran. Dr. Assad Homayoun, the President of Azedagan, an Iranian exile organization, argues that "Mao Tse-Tung used to say that real powers come from the barrel of a gun, but today real power comes from the Internet." His opinion is slightly exaggerated, but the Internet can be partly responsible for democratic progress within Iran. Nasser Hadian-Jazy, a political science professor from the University of Tehren agrees that, "like it or not, the satellite and the Internet are changing Iran and the conservatives have no idea how to deal with it." [Mazaar 02]

The use of web logs, commonly known as blogs, has grown considerably in Iran. A blog can take on many different implementations such as journalism, political campaigns, media programs, and even corporations. The most influential blogs inside Iran are those that are centered on politics. Blogs tend to overcome the tight control that a conservative theocracy such as Iran has over the media. The author and readers can exchange information or discuss stories that quite possibly would have never made it to the Iranian conventional media. Many have said that these blogs have become the voice of the opposition to the current regime and have advanced the cause of democracy in Iran. There are an estimated 65,000 blogs written in Farsi. Farsi is the fourth most widely used language on web logs. [WIKI 05] A comprehensive listing of blogs written by Iranians can be found at http://blogsbyiranians.com. The government has responded to the dissent among bloggers by arresting dozens of these web journalists. Some of those detained, such as Arash Sigarchi and Mojtaba Saminejad, are reportedly being held in solitary confinement and are being tortured. The government has not explicitly stated that their opposition is the reason for imprisonment, but both detainees have actively used their blogs to criticize the government. Reporters Without Borders, human rights groups, and other bloggers are attempting to gain the release of all Iranian bloggers and cyber-dissidents. [Boyd 05]

2. White Hat Network Security Groups

Along with widespread usage of the Internet for political purposes, there is a growing interest in network security. Rapid expansion of computer technology in Iran has resulted in a lack of training or attention towards network security. While Iranian academic institutions have begun to teach these fundamentals, many computer systems within Iran are targets of opportunity due to a lack of adequate protection. Widespread successful attacks on websites hosted in Iran highlight the inadequate security awareness. In response to this threat, there are numerous white-hat websites that have been published. Some examples of these are Hat Squad Security Team (http://www.hat-squad.com), Iran Security (http://weblog.iransecurity.com), IR Computer Emergency Response Team (www.ircert.com), Iran Virus Database (http://www.irvirus.com/), and Crouz Security Team (http://www.crouz.com/). These sites, written in Farsi, appear to

discuss vulnerabilities. They are similar to English-language white-hat sites that purport to expose software vulnerabilities and prompt software manufacturers to patch them. The goal of these web communities is to ensure software makers create more secure software.

In addition to white-hat websites, an Iranian group is also listed on the Defcon website as one of its membership groups. Defcon holds an annual computer security conference in Las Vegas and is considered the largest underground hacking convention in the world. Defcon groups were established to share security information among its members and to provide some cohesion within the hacker community. The Tehran based group was formed in February 2004 by a hacker named Tenebrious. Very little is known of this group's activities, but participation in the Defcon organization shows a willingness to share information among its members. [DEFCON 05]

E. CONCLUSION

The study and use of information technology has become widespread throughout Iran. Iranian learning institutions are actively teaching the fundamentals of Information Technology through undergraduate and graduate degrees. Research at these institutions is commensurate of what is to be expected from academic institutions throughout the world. The public community in Iran also actively participates through Information Technology. The Internet has become a virtual community used not only for the advancement of science, but also for political activism, conventional Iranian media, and webbloggers struggling to derive the truth from a Islamic theocracy that tightly controls the media.

IV. GOVERNMENT ACTIVITY

A. INTRODUCTION

This chapter will examine Iranian government activity pertaining to CNA/E. It will detail government entities involved in the research and development of IT, the use of IT in its military doctrine, and the likelihood of Iran conducting cyberwarrior training.

B. GOVERNMENT ENTITIES INVOLVED IN IRANIAN IT DEVELOPMENT

Throughout the last decade, Iran has expressed a strong interest in developing its information communications and technology infrastructure. It has made considerable progress in expanding access to information technology. The Second-Five Year Plan emphasized a policy in which the government would advance technology research to solve developmental problems. According to the plan, this policy was to be realized by:

- Developing a research system conducive to further enhancement, better arrangement, and coordination of research activities and their evaluation
- Setting research priorities
- Strengthening relations between the country's research centers and their international counterparts
- Reinforcing an organic relationship between research application and education.

[Shokoohi 96] Furthermore, President Khatami expressed his views on the government's role in scientific research in a speech at the 11th Khwarazmi Science Festival:

> If we are determined to make progress, our political system, government and state must earnestly engage in scientific inquiry and research so that our future course will be based on firm foundations. What is of great importance to us is turning research and investigation into a culture and everyday practice so that it can permeate all walks of life and all aspects of our society, and consequently, the notion can take root that life without inquiry and research is a life without glory and honor. The ground root and underlying foundation of our actions in the realms of science, technology, social sciences and civil service should be formed by research and investigation. To instill such a social attitude demands national determination, and the government alone will not be able to accomplish such a great task. We are all aware that the pivot of all research and

> investigation is man, that is, the thinking man. Therefore, real progress and true development is tantamount to the development of the human element. Out of the four elements which together form what we know as technology, three of them, that is, information and knowledge, skilled manpower, and management concern human beings, and only one, namely technical tools and equipment, are supposed to be non-human, although they, too, are actually the objective form and the crystallization of human thought. This goes to show that technology, which seems to be the most materialistic aspect of human society, is, in fact, the most human of all. [Khatami 05]

Given the policies set forth by the Second Five Year Plan and the opinion of the Iranian President, the government plays an active role in the development of information technology.

There are several government research institutions that conduct scientific research. Together with research from the academic institutions previously described, these institutions promote the rapid development and deployment of technology in Iran. The primary research institutions pursuing information technology topics are the Iran Telecommunications Research Center, Guilan Science and Technology Park, and the Pardis Technology Park.

1. Iran Telecommunications Research Center

Established in 1970, the Iran Telecommunications Research Center (ITRC) is the research arm of the Ministry of Information and Communications Technology. It has evolved as a key consultative body, liaising with and influencing the Ministry's decision-making concerning emerging technologies and international interactions. The center boasts about 600 active researchers from academia and industry throughout the country and has an estimated 21,000 sq. meters of modern laboratories. The ITRC is a member of the European Technical Standards Institute, participating in the development of new standards development and customization studies. According to their website, the center also embraces collaboration in the development of new technologies with peers from all over the world. Its stated goals are listed below:

- Launching research studies and disseminating results and experiences nationwide.
- Provision of consultancy services
- Directing and managing national standards and regulations of ICT

In its role as a consultant, the center advises government policy makers in the ICT "blueprint" for Iran. The center also confers with other international entities to improve the Iranian ICT infrastructure. Its research groups are divided into 4 different departments. The Information Technology department consists of multimedia, IT application, and IT strategy and infrastructure research groups. The Strategic Management department consists of ICT economic and developmental planning, ICT security management, strategic and regulatory issues, and integrated telecommunications network management groups. The Networking department studies data networks, wireless technology, and switching system groups. Finally, the transmission department focuses on antennas and radio systems, satellite communications, and optical communications groups. The Third-Five Year Plan established a framework for the ITRC to study topics such as a data telecommunication management networks with an emphasis on design of network telecommunication management network, network evaluation and quality of service (QOS), intelligent networks (IN) and related services, network security, asynchronous transfer mode (ATM) and synchronous digital hierarchy (SDH).

Within the ITRC are additional study groups that are aligned with the International Telecommunications Union (ITU-T) study groups that focus standards development and research in the form of study questions. According to the ITRC website, they are active in 12 groups and have generated numerous scientific and technical papers. Of particular interest was the ITRC participation in Study Group 17, Security, Languages, and Telecommunication Software. The ITRC website states that Study Group 17 has prepared 30 papers, conducted 5 workshops, and provided consultancy for executive departments since 2001. [ITRC 05]

In addition to conducting research, the ITRC hosts international conferences to further promote the scientific achievement of Iran. An International Symposium of

Telecommunications was being organized for September 2005. The purpose of the symposium is to highlight the most recent developments in communications and information technologies to include new concepts, theories, technological advancements, services, and network infrastructure improvements. [ITRC 05] An internet search for the ITRC yielded the resume of a Professor Shahram Bakhtiari of Sharif University of Technology. His resume includes an extensive background in network security, cryptanalysis, and object orientated design. He has run information security workshops for several conferences to include the Iranian Conference on Electrical Engineering (ICEE '99) hosted at the ITRC. [Bakhtiari 01] Another internet search result for the ITRC yielded a program for the 17th International Conference for Computer Applications in Industry and Engineering held in Orlando, Florida in 2004. One of the presentations, given by three scientists from the ITRC, was entitled "A Systematic Approach to Network Security Assessment" by Mehdi Rasti, Davood Sarramy, and Mahmood Khaleghi. [CAINE 04] A search for Mehdi Rasti yielded another publication titled "Neural Network Based Dynamic Anomaly Detection in Computer Networks: A Novel Training Paradigm Using Abnormal Behavior" from CAINE 03 held in Las Vegas, NV. [Varjani 04] Participation in International conferences demonstrates the ITRC's interest in contribution to the advancement of computer security topics.

As the principle research center for the Ministry of Information and Communication Technology, the ITRC is considered to be one of the principle elements of governmental participation of technology. There was limited information pertaining to specific research projects, but given that network security is a topic of study, there may be substantial research in that area.

2. Guilan Science and Technology Park

Formerly known as the Iranian Research Organization of Science and Technology, the Guilan Science and Technology Park (GSTP) was established in 1989 as a research center and reorganized in 2002 as a technology park. According to its website, some of the park's goals are to develop research activities in the private sector and to assist small companies to find markets for their innovations and products by promoting

cooperation with the more established high-tech industry. It is a member of the International Association of Science Parks (IASP) and works in close cooperation with the Steinbeis Foundation in Germany. The GSTP focuses on the agro-food, biotechnology, chemistry, electronics, ICT, and tourism industries in Iran. The technology companies that have established themselves in the park include the North Sabat Computer Cooperation Company, Guilan Communication and Technology Development Company, Green Pooya Net Company, Morvarid Information Technology and Software Company, and the Guilan Computer Science Cooperation Company. Within the park is an ICT Incubation center that provides additional assistance to technology companies aiming to reduce the inherent risk of technology development. [GSTP 05] While this park has been a success, its principle focus is to promote small technological business development. Its remote location relative to the thriving technology and research environment centered on Tehran presents an obstacle in becoming a premier research park in the Middle East. [Khatami 05]

3. Technology Cooperation Office

The Technology Cooperation Office (TCO) was founded in 1984 as the Office of Scientific and Industrial Studies to provide consultation to the President of Iran. It was renamed to the TCO to promote the international cooperation in the field of advanced technologies. The TCO supports Iranian organizations in the following ways:

- Technology development planning
- Organizing design offices and R&D centers
- Coordinating joint research projects
- Organizing specialized training courses, seminars and exhibitions
- Technology procurement and localization
- Establishing relations between Iranian institutions and foreign industrial and scientific research centers for technology cooperation

The TCO is active in several fields including Biotechnology, Aerospace, Information Technology, Software, New Materials, Industrial Processes, Energy, Civil Engineering, Infrastructures, Power Engineering, Studies on Technology Development and

Technology Management. Attempts to view the website directly were unsuccessful due to the website being taken offline. An archive of the TCO website is provided in Figure 3.

Figure 3. Technology Cooperation Office Archived Website [TCO 04]

4. Paradis Technology Park

While still being developed, the Pardis Technology Park (PTP) was established to foster better cooperation between large-scale public and private research. Hoping to capitalize on the success of Silicon Valley in the United States, the park has declared itself to be the future Silicon Valley of Iran. PTP is under the direct management of a Board of Directors representing the TCO and Sharif University of Technology. The involvement of the TCO shows a high level of governmental support and control. [UNIDO 05] Its close proximity to the rapidly expanding high-tech industry in Tehran and several academic institutions such as Sharif University of Technology and the University of Tehran make it a very promising venture. With a focus on ICT, the park claims the support from a myriad of local and international scientific organizations. The

government hopes that the PTP will provide a better opportunity for foreign investment of Iranian ICT. The park is considered to be the heart of Iran's strategic technology development. With an area of over 60 acres available, the park promises to provide leading edge IT infrastructure and communal facilities. Its focus areas will be advanced engineering, biotechnology, chemistry, electronics, ICT, and nano-technology. At least 45 companies have thus far agreed to purchase land in the park. A picture of the proposed headquarters building and park plans are included in Figure 4. By leveraging public, academic, and private research into a single geographic area, Iran hopes to establish this area as the premium center for technology research in the Middle East.

Figure 4. Pardis Technology Park Headquarters Complex [PTP 02]

Outside of traditional academic research being conducted by public universities, these research centers are the bulk of the Iranian effort for ICT development. The technology research centers described were established to better coordinate technology research and transfer. Given the relatively tight economic controls placed on businesses in Iran, the coordination of competing research efforts by the government is essential to further technological innovation. There was very limited information pertaining to specific research projects these institutions were undertaking, but there was substantial evidence of a proactive Iranian government approach with regards to ICT development support.

C. MILITARY DOCTRINE

Iran's military doctrine is based on its regional political aspirations, external threat perceptions, and the desire to preserve the Islamic state. Iran's strategy is to become the most dominant power in the Middle East. Recent campaigns by the United States in Iraq and Afghanistan have prompted Iran to reevaluate its strategic doctrine. The perception of being surrounded by the United States or its allies is shaping the country to pursue more asymmetric capabilities to counter a much larger and more powerful force. Iran believes that further development of WMDs and medium to long range missile systems are essential to ensure regional security. Due to increased international scrutiny, Iran does not openly admit to the development of WMDs; recent press reports on Iran's nuclear capabilities indicate otherwise. Regardless of the state of its nuclear capabilities, Iran claims to have other means to handle foreign threats. In early August 2004, Iranian Deputy Defense Minister Mohammad Shafii-Rudsari declared that Iran "has a diverse defense strategy to meet threats from foreign powers such as America and our defense capacity and power are entirely adequate for regional...threats." Iran highlighted its asymmetric military doctrine in the Ashura-5 military exercise during September 2004. In this exercise, the Iranian Revolutionary Guard Corps conducted coordinated air and ground attacks, strategic missiles, and other weapons and methods. Iran also tested its defensive tactics, psychological warfare, and logistical capabilities. [Janes 05]

There was no evidence found to indicate Iran has an ability to conduct CNA/E against its enemies, although Iran has historically supported the development of asymmetric capabilities such as WMDs to include nuclear and chemical weapons, ballistic missile technology, and the sponsorship of terrorism. [Rubin 02] Given the United States and the western world's reliance on information technology, a cyber-attack capability would give Iran an opportunity to degrade or disrupt adversary information dominance strategy.

D. TRAINING CYBER-WARRIORS

Evaluating Iran's participation in CNA/E activities has proven to be a very difficult task. Outside of the security courses being taught to university students, there was no direct evidence of state-sponsored training. Iran's cooperation with North Korea is well known by the US government to include military technology transfer and training. There have been recent reports regarding cooperation in the development of the Iranian Shahab-3 and the North Korean Nodong missile systems. [Shannon 05] In addition, according to an interview of Hamid Reza Zakiri, a senior Revolutionary Guard official who defected, Iran has sent military and intelligence officers to North Korea for training in psychological warfare and counter-espionage. Although unconfirmed by the United States government, North Korea is reportedly operating a hacking school that produces up to 100 cyber-warriors a year. [McWilliams 03] The close cooperation between North Korea and Iran makes the possibility of cross-training of personnel in CNA/E capabilities likely.

E. CONCLUSION

This chapter summarized the participation of the Iranian government in the development of information technology. Iran's efforts to be on the leading of research in the Middle East are evident in the government sponsorship and coordination of research by public, private, and academic entities. In addition, this chapter discussed Iran's military doctrine of developing asymmetric capabilities to counter larger and more capable foreign powers. Also examined were Iran's close military training ties with North Korea and possible cross-training of cyberwarfare personnel. Given Iran's steady advancement of technological capabilities, it is reasonable to assume that the government intends to leverage this capability for offensive and defensive actions.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMPUTER NETWORK ATTACK/EXPLOITATION ACTIVITY

A. INTRODUCTION

This chapter examines the CNA/E activities of Iran. There have been many suspicions and generalizations of suspected CNA/E activities being carried out by Iranian Internet users. This chapter provides insight into whether these suspicions are correct by discussing various known hacking groups, some possible motivations for hacking, and difficulties in identifying Iranian hackers.

B. COMPUTER NETWORK ATTACK

CNA is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNA relies on interpreted signals in a data stream to execute an attack. An example of CNA is sending a digital signal stream through a network to a central processing unit that instructs the controller to interrupt the power supply. CNA is often confused with electronic warfare which targets the electromagnetic spectrum rather than computer networks. [Wilson 04]

C. COMPUTER NETWORK EXPLOITATION

CNE involves the use of espionage of computer systems with tools that penetrate systems to return information enabling an adversary to gain an advantage. Prior to conducting CNA, an adversary might conduct a covert and thorough analysis using CNE to determine vulnerabilities. In addition, in order to develop an effective Computer Network Defense (CND), CNE may be conducted on adversary information systems to accurately diagnose their capabilities. Therefore, reconnaissance, probing, and scanning of networks associated with CNE can readily be used in the conduct of CNA and CND. [Wilson 04]

D. MOTIVATIONS FOR HACKING WITHIN IRAN

In order to analyze the hacking activities of Iran, an analysis of the motivations of this type of activity must be conducted first. Researchers that have interviewed individuals in the hacking community have yielded a number of common themes to explain the motivations behind these people. These motivators were a compulsion to hack, curiosity, control and attraction to power, peer recognition, and belonging to a group. [Van Beveren 01] In addition, monetary gain is increasingly becoming more influential for hackers. In Iran, some hackers have been found with political or religious motivations.

1. Traditional Hacking Motivations

There are common motivations that have motivated hackers world-wide. These include money, power, curiosity, and a sense of belonging. It is very likely that these motivations have some influence on the hacking community in Iran. Historically, hackers have defaced web pages or launched worm and virus attacks to gain notoriety among their peers. Hacking groups' discussion pages and blogs are littered with discussions of accomplishments and vulnerabilities. One such observation came from an Iranian individual named "Spiderhacker." In his blog, he talks about hacking into many websites due to a lack of security. Although he claims that he does not like to boast of his accomplishments, he believes that he is enhancing Iran's reputation in the worldwide community of hackers. [Spider 04] Another hacking motivator is the sense of belonging that is created among hacker "teammates." Various Iranian hacking teams were found. Most of their sites were actively recruiting new members with any level of kind hacking or programming proficiency. Some examples of Iranian groups found include Iran Hacker Association, Iran Hacking Sabotage Team, Iran Babol-Hackers Security Team, Ashiyane Digital Security Team and Persian Crackers. There are many more groups that have formed ad hoc hacking and computer security communities bound together by the Internet that are too numerous to list. The Iran Hacker Association claimed to have scheduled meetings with some of its members in which they promised to post the minutes from this meeting. The website also claimed "Spiderhacker" was the head of the association. [IHA 03]

Another motivator that has increasingly becoming more influential for hackers is monetary gain. According to FBI spokesman Paul Bresson, there "has been a rise in the cases where the motivation appears not just to be for the purposes of bragging in chat rooms, but to actually profit financially." He goes on to say that there is an increasing growing underground for selling credit card numbers, software vulnerabilities, or renting out "botnets." Botnets, also known as Zombie networks, are used to extort companies who are threatened with a Distributed Denial of Service (DDoS) attack. [Ever 05]

Iranian hacking teams such as the IHS Team and the Ashiyane Digital Security Team have hacked sites throughout the country in the hopes of selling security training and services. Both teams are well known for their hacking exploits on an internet database of attacks, Zone-H.org. Their activities on the Internet are directly related to services they are selling. These hacking groups exhibit some of the same motivations of hackers worldwide. The quest for recognition, a sense of belonging, power, curiosity, and monetary gain drive individuals into the hacking world. The lack of education and awareness of network security makes the Iranian portion of the Internet a target rich environment for skilled and unskilled hackers alike.

2. Politically Motivated Hacking

Iran is considered to be an oppressive theocracy that has little tolerance for dissent or disagreement from the civilian populace. Stories such as the government practice of web-content censorship and the detainment of webloggers that espouse anti-government rhetoric validate this belief. This environment coupled with widespread vulnerabilities on the Internet in Iran makes politically motivated hacking, or hacktivism, very likely. One of the most well-known hactivists is Oxblood Ruffin the publisher of www.hacktivismo.com. In an interview with Shift.com, he discusses software he has developed such as an anonymous tunneling protocol program and a program to embed messages inside of gif images to bypass censorship filters. He reports that there has been considerable activity using these programs from Iran. [Moyes 02] This technology has been used by hackers and bloggers alike to subvert government filtering. Although there was no evidence of this type of software being developed by Iranian programmers,

there have been other potential politically motivated hacks. The weblog by the reformist Iranian former Vice President Abtahi's weblog was hacked numerous times in response to his postings regarding the government torture of other webloggers. Word of this cyber attack has spread throughout the Internet on other blogger's sites. One such post on the blog of "Persian Students in the UK" attributed the following quote to Abtahi in which he hints that there is a greater conspiracy of hacking against him:

> Again for a few days I was unable to publish anything. The reason is probably obvious, after writing the post about the arrested bloggers. If I get into trouble again, I will write about it comprehensively."

Persian Students in the UK theorize that these hackers are funded by conservative elements within the country. (Parthisan 05) Other political sites have also been hacked. A more recent example of possible hacktivism is the distributed denial of service (DDoS) attack of an ex-Presidential candidate Ali Larijani. The campaign committee for Larijani claimed that the opposition had hacked his sight due to his political views. News of this activity has also made itself into several Iranian blogs such as regimechangeiran.blogspot.com and nowrooz.blogspot.com. Evidence that politically motivated hacking is occurring within Iran is fairly substantial. The attacks on the websites of Larijani and Abtahi indicate that elements within the country are attempting to silence the opposition. Many bloggers have theorized that the government has been conducting these attacks. Bloggers such as Hoder have gone as far as to label the hard line governments as "IT-ollahs." [Derakhshan 05] There was no evidence validating these claims, but this opinion is widespread throughout the blogging community.

3. Religious Motivations

As with the rest of the Islamic World, Islam has significant influence upon the lives of the Iranian people. Fatwas issued by religious scholars have significant influence upon those who follow Islam The World Wide Web is also used to disseminate information by scholars regarding Islamic law with some of them offering online fatwas for those with specific questions. These fatwas can be found on websites such as www.islamtoday.com and www.islamonline.net, and www.ask-imam.com. One particular fatwa issued by Dr. Sano Koutoub Moustapha, a Professor of Jurisprudence

and Its Principles at the International Islamic University of Malaysia, issued a fatwa giving permission to hack into computers. The question posed to him was:

> Respected scholar, I'd like to know the Islamic ruling on hacking web sites that serve the American and Israeli interests on the Internet?

Dr. Moustapha's response gives permission to hack into sites as defined below:

> Your question seems to be too general. However, Islam does stand for better cooperation and communications with nations who are not destroying and fighting us. This is clearly stated in Almighty Allah's saying: "Allah forbiddeth you not those who warred not against you on account of religion and drove you not out from your homes, that ye should show them kindness and deal justly with them. Lo ! Allah loveth the just dealers. Allah forbiddeth you only those who warred against you on account of religion and have driven you out from your homes and helped to drive you out, that ye make friends of them. Whosoever maketh friends of them (All) such are wrong doers." (Al-Mumtahanah: 8-9). This means that one should differentiate between those enemies who are killing our innocent and helpless Muslims around the world and those enemies who help or assist them in doing so.
>
> In addition to that, one has to do his best to tackle and hack those sites which are meant to murder and kill Muslims. Furthermore, Muslims should be able to discover the plans and strategies of our enemies in order for them to come up with strategies that will protect us against the attacks of the enemies.
>
> In this regard, I shall say there is no harm or prohibition to hack any site meant to destroy Muslims or occupy our lands. It is a legitimate right to defend ourselves by using all possible means and tools including hacking and destroying those evil sites. [Moustapha 04]

The fatwa above speaks with generalizations and does not say who the target of the attack should be. Given the United States military operations ongoing throughout the world, it could be assumed that he was referring to the United States and its allies. Although considered a powerful statement in Islamic law, a fatwa is only binding for the follower of the person who issues it. Many people in the Islamic world believe that there is a lack of structured leadership in Islam and there are far too many people who can issue fatwas. Nonetheless, statements like the one from Dr. Moustapha indicate that traditional Islamic jihad motivations could be used as a justification for cyber attack.

4. Hacking as an Instrument of Foreign Policy

There are several tools available to a nation state to execute its foreign policy, some examples of these include diplomacy, economic pressure, and military force. Given the overwhelming dominance of the United States and its allies in world affairs, Iran's national military strategy to counter this perceived threat is to develop asymmetric warfare capabilities. One such capability is cyber warfare. No direct evidence of Iranian sponsorship of CNA was found, but it is possible that the capability is being considered or even currently being developed.

E. IRANIAN HACKING GROUPS

There is quite a substantial hacking community within Iran. The skills of these hackers range from unskilled amateurs that can use software tools that are developed to exploit already known vulnerabilities to skilled hackers that find new vulnerabilities and exploitations. Due to government filtering, all the sites found during the research were hosted in countries outside Iran. A substantial number of websites posted vulnerabilities, exploits and downloadable software tools in Iran. Several of them stood out due to increased level of sophistication and number of attacks credited to them. These website were the Iran Hacking Sabotage Team, Aysahne Digital Security Team, and Iran Babol-Hacking Team.

1. Iran Hackers Sabotage Team

The Iran Hackers Sabotage (IHS) Team is one of the most active hacking groups in Iran. It is listed with Zone-H.org as one of the world's top attackers. According to Zone-H, IHS has conducted 3551 attacks of which 481 were single IP attacks and 3069 were mass defacements. The target of attacks that IHS have attacked include commercial, local and federal government, and academics domains within the United States. IHS has also conducted attacks on foreign domains throughout the world. [Zone 05] According to their website, they were established in early 2004 to put Iran on the map with regards to hacking ability. After being able to successfully penetrate servers throughout the world, they decided to offer vulnerability assessment services and secure

web hosting. The team consists of three hackers named NT, C0d3r, and LorD. According to the biographies on the website, NT and C0d3r are university students at an unnamed university. LorD claims that he is a security researcher and a programmer. All three express an interest in networking and exploitation coding. Several original exploitation programs were available for download. Each download was uncompiled code written for Visual C++ and contained comments providing the history of the bug/exploit. All of the exploitations available on the IHS website were based on bugs found by other people or organizations. Typically each exploitation code was generated by IHS within a few days of public release of the vulnerability on various security sites. Some examples of exploitations found include a local root exploit for IBM AIX, 3Com 3cdameon BOF exploit, Internet Download Manager remote stack overflow exploit, and PMsoftware Web Server version 1.0 remote stack server overflow exploit. The exploitation code also contained the name Kaveh Razavi as the name for C0d3r. [IHS 05] A picture of the IHS website is shown below.

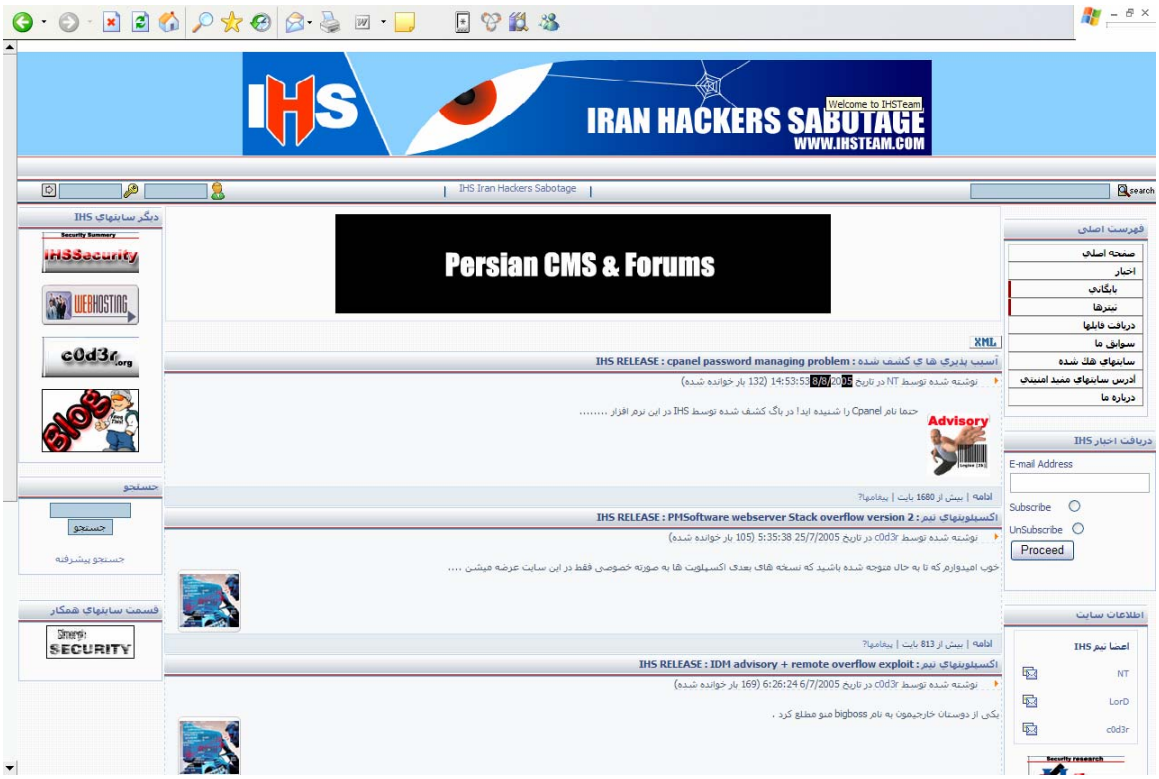

Figure 5. Iran Hacking Sabotage Team Website [IHS 05]

According to Zone-H, IHS is responsible for the July 25th, 2005 attack on the U.S. Naval Station Guantanamo's public website (http://nsgtmo.jax.spawar.navy.mil). A saved copy of the attack is depicted below. According to the text in the attack, the IHS expressed disagreement with US foreign policy. As of August 10th, 2005, the Naval Station's website was still not available. Other attacks by IHS upon U.S. government sites include the Armed Forces Institute of Pathology and various local county websites.

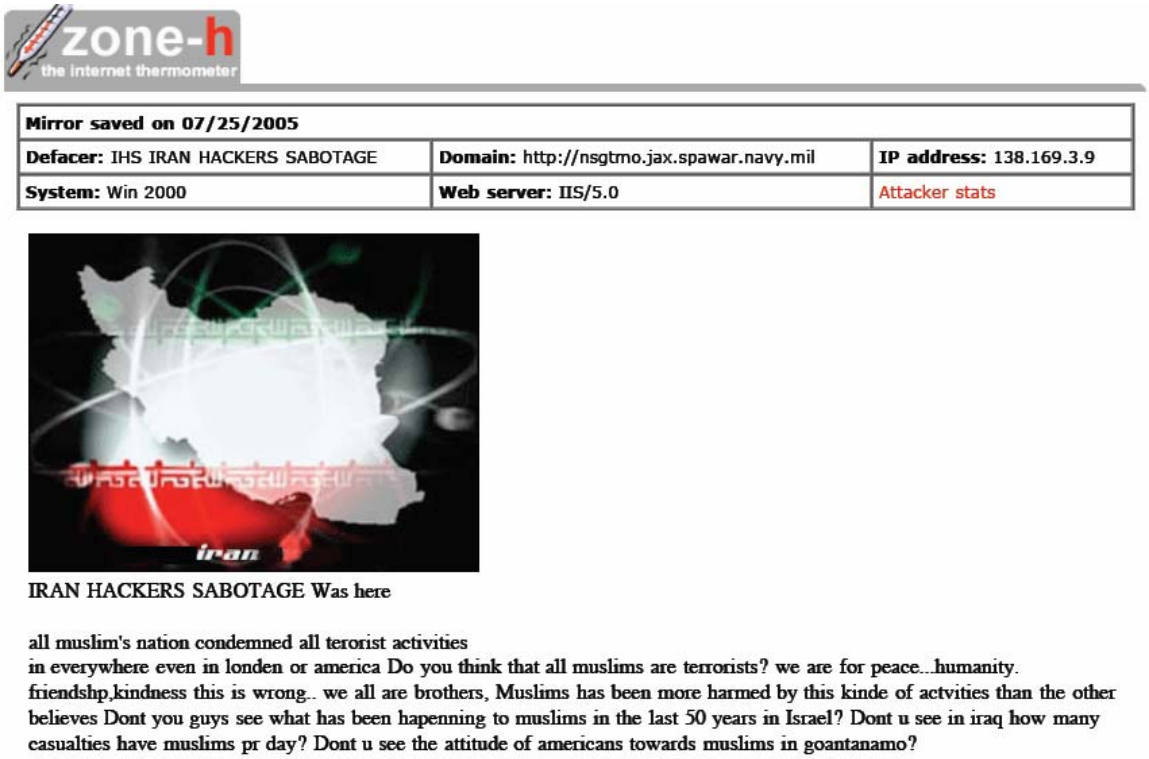

Figure 6. Naval Station Guantanamo's Defaced Webpage [Zone 05]

2. Ashiyane Digital Security Team

Another of the more well known Iranian hacking teams is the Ashiyane Digital Security Team. According to Zone-H, the Ashiyane DST is accredited with 3,007 attacks of which 396 were single IP attacks and 2611 were mass defacements. [Zone 05] Their website is included below. A simple Google search of the team name yields numerous web sites that have been hacked by the Ashiyane DST. Like the IHS, this team's principle motivation is to sell its security consultation, web hosting, and network consulting services. There was also some evidence of this team having using political

motivations to hack. A defacement of a National Aeronautics and Space Administration (NASA) website below also questioned the United States' Middle East foreign policy. Other attacks by Ashiyane were simply used to put their name with links to their website on the world-wide web. An example of one of Ashiyane DST's advertising attacks is shown in Figure 9.

Figure 7. Ashiyane Digital Security Team Website [Ashiyane 05]

Figure 8. National Aeronautics and Space Administration Website Hack by Ashiyane DST [Zone 05]

Figure 9. An "advertising" attack upon www.svidal.com by Ashiyane DST [Zone 05]

According to their website, the Ashiyane DST appears to be fairly well organized. They have several teams including management, training, defacement, and software programming teams. There were biographies listed for 15 members of the team. The team leader is Behrooz Kamalyan who goes by the nickname Behrooz_Ice. The team member's ages ranged from 16 to 28. The member of this group had a wide variety of computer related skills. Most of the team members boast experience in the major operating systems such as Windows, UNIX, Cisco IOS, and LINUX. Many of them had programming experience in languages such as C, C++, VC++, Delphi, and Perl. All of them claimed some sort of hacking capabilities to include firewall penetration, social engineering, php database hacking, operating system penetration, shareware cracking, and decoding program executables. Several of these members conducted classroom training for a fee on topics such as basic, advanced, and professional levels of hacking, hacking tools, and a list of other programming languages, operating systems, and professional certifications. These classes were taught in an audio/visual classroom at a vocational school in Tehran. The cost of hacking training varied by the level of instruction; the basic course cost approximately $200.00 for 40 hours of instruction while the professional level course cost approximately $355.00 for the same amount of instruction time. The Ashiyane DST appears to a very active and a well structured organization for hacking in Iran. Its members have a vast amount of technical knowledge and experience that could be used to develop a government sponsored CNA/E capability.

3. Iran Babol-Hackers Security Team

Very little is known of the Iran Babol-Hackers Security Team (BHST). Zone-H attributes 297 attacks with 278 as single IP attacks and 20 as mass defacements. A Google search of Iran Babol-Hackers Security Team yields many websites that have been defaced by them. Their website was very well designed but contained very little information about the team. A picture of the site is included below. While no biographies were posted, the team members appear to be Ezrael, The Undertaker, Black-Ice, FaOp, and PoPo. Most of the site was still under construction, but a statement on the site claims that it will post training videos and computer security related topics in the

future. While very little information could be determined from their website, the BHST has shown that it has the necessary skills to conduct attacks on the internet.

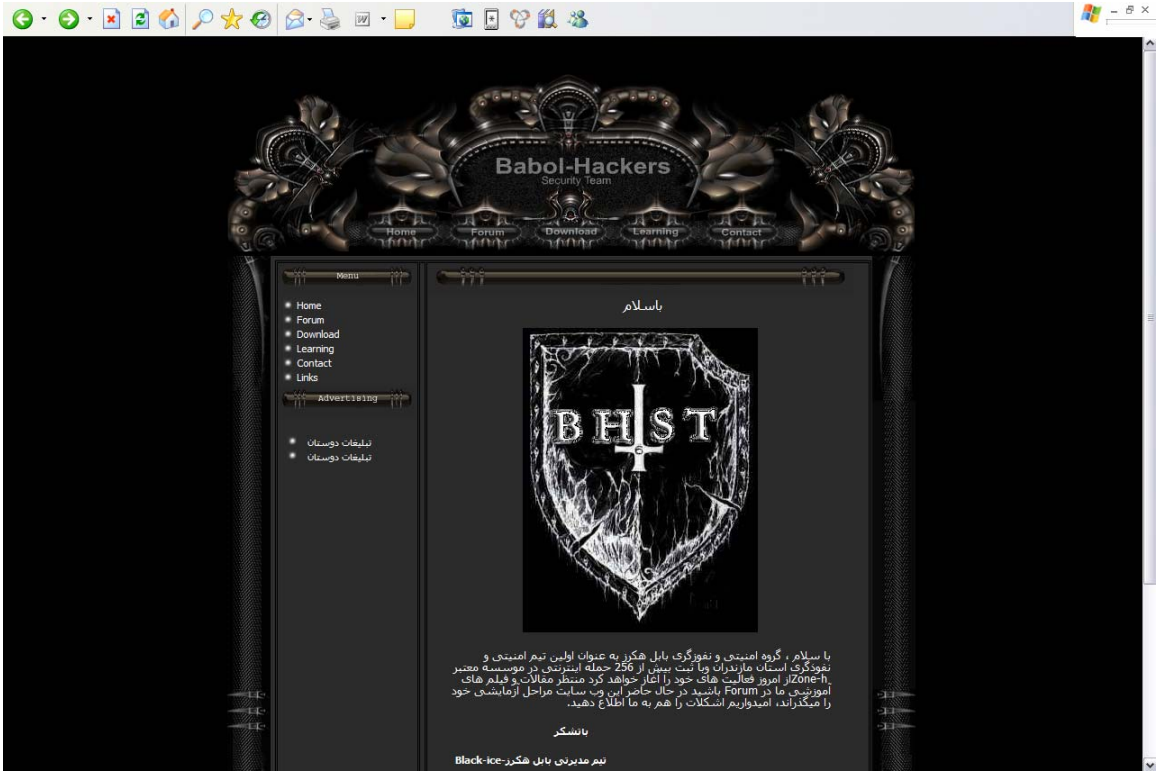

Figure 10. Iran Babol-Hackers Security Team Website [IBHST 05]

Activity by hacking groups such as the Iran Hackers Security Team, Ashiyane Digital Security Team, and the Iran Babol-Hacker Security Team indicate a substantial hacking community within Iran. There was evidence of many more hacking group's webpages or web logs. The groups listed above were the most active and well-known groups found. This malicious hacking activity indicates that an organic CNA/E capability exists. Although there was no evidence that the activity by these groups were supported by the Iranian government, a potential exists for Iran to hire the individuals involved to join a government CNA/E group.

F. DIFFICULTIES OF IDENTIFYING IRANIAN HACKERS

It can be difficult to identify hackers and the origins of attacks on the Internet. There are several reasons why this is so, including:

1. Internet Protocol (IP) Spoofing

IP Spoofing is an attempt to gain access using a different IP address. The hacker uses a variety of techniques to find an IP address from an external computer that is allowed access to the target network or computer, or to access an IP address from the addresses that the computers on a targeted network use. The illicitly obtained IP address is then used to modify the packet headers that the hacker sends, thereby tricking the target network or computer into allowing the hacker access to the target host. Sophisticated hackers undoubtedly use this technique to gain access to a protected network. Iranians could use this method to disguise their true address making it nearly impossible to trace the origin of the attack.

2. Communication Bouncing

Communication bouncing involves bouncing communications through a distributed network to disguise the true origin. Hackers can do this in a couple of different ways. The first method involves a hacker gaining access to a server or series of servers and then using them as the source of an attack. A second and far easier method is to use an online service such as the Tor network (www.tor.eff.org). It uses a set of relay servers to keep communications private and to prevent internet traffic from being analyzed. A diagram is included below to illustrate how a message is sent over the Tor network. The communications between the nodes can also be encrypted to prevent any packet sniffing. Iranian hackers could use this technology to not only bypass government filters, but also hack into computer networks.

Figure 11. Message being bounced through several nodes on the Tor network. [Dingledine/Mathewson/Syverson 04]

3. Manipulation of Event Logs

Most systems utilize system logs that record notable system events. While these logs are considered an essential security practice, hackers have found ways to bypass or change them to disguise their attacks. Some of these techniques are well-known throughout the Internet. It is likely that Iranian hackers use these techniques to avoid identification.

4. Lack of Accurate Cyber Attack Reporting

According to a speech by FBI Director Robert Mueller, most businesses do not report cyber attacks. Reports of identity theft in the media have become quite common causing damage to a company's public image. This has caused a reluctance to report attacks to the authorities. A survey by the Computer Security Institute revealed that fewer than 20% of companies have reported computer intrusions for 2004. In his speech, Director Mueller stated that the FBI "cannot investigate if we are not aware of the problem." This is a substantial problem that affects the accurate diagnosis of hacking activity. It is likely that successful attacks by Iranian hackers have gone unreported. [Sherman 05]

G. CONCLUSION

This chapter discussed the activities, motivations, and difficulties encountered through open source research of Iran's CNA/E activities. Iranian hackers have established a loosely formed virtual community of web logs and security websites

discussing network vulnerabilities and exploitations. The task of identifying hackers, their motivations, and sponsorship however, can be difficult. While Iran has a fairly substantial hacking community, it appears to lack formal structure or state sponsorship.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSION

1. Academic and Research Activity Shows an Extensive Interest in CNO Activity

Iranian academic and research institutions are on par with comparable institutions throughout the world. Many of the scientists and academic researchers that specialize in computer security have been educated in both Iranian and western academic institutions. Iranian academic and research institutions actively contribute by participating in international conferences and academic publications. There is adequate access to information resources via the internet available to scientists. The interaction with the international computer security community ensures adequate knowledge transfer.

There is substantial government interest in embracing the study of information technology. Several Iranian public academic institutions are pursuing research in computer security related topics. Faculty members from many academic institutions have had experience in or are actively pursuing topics that are relevant to CNO. Overall goals for information technology research have been promulgated by guidance in the evolving Five Year Plans. The Iranian government has maintained oversight of research efforts through the Technology Cooperation Office and the Ministry of Information and Communication Technology. The establishment of the Iranian Telecommunications Research Center, Guilan Science Technology Park, and the Paradis Technology Park are used to facilitate research. A firm foundation has been established for Iran to become one of the most technologically advanced nations in the Middle East.

2. Malicious Hacking is Widespread throughout Iran

Malicious hacking within Iran is widespread. There were dozens of websites, blogs, and discussion groups that promulgate information pertaining to vulnerabilities exploitations, and software tools. There was substantial evidence of hacking techniques such as domain hijacking, web page defacements, and software vulnerability exploitation. The activity found appeared to be mostly juvenile hacking that was unstructured and

unorganized. The motivations for this activity can be attributed to general hacking motives such as power, money, politics, recognition, etc. There have been some claims that the government has used CNA to disrupt the efforts of political candidates and dissidents, but this study found no evidence found of government support or organization of this type of activity.

3. Open Source Information Regarding Government-Sponsored CNO is Not Widely Available

Throughout the research, there was an abundance of information regarding cyber attack activity originating from Iran. Most of this information is based on generalizations and suppositions made from Iran's potential capability to conduct cyber attacks. Difficulties arise when trying to establish a direct link between the government and malicious hacking. Nation states typically try to keep their CNA/E capabilities from being released to the public as disclosure of this information would endanger the effectiveness of such operations. Information regarding the United States' CNO activities is kept at a classified level, and it is reasonable to assume that Iran's CNO capabilities are treated similarly. Open source information regarding the Iranian government's CNO activity is merely speculative and based on its potential for attack. There was an abundance of evidence to indicate that this speculation is worthwhile in determining an adequate analysis for CND of critical infrastructures. Although no direct evidence was found linking the Iranian government to a cyber attack capability, the information technology infrastructure, educational system, and government research activity indicates that such activity is possible if explored by the government. Iran's education and research system actively participates in the world-wide community with regards to computer security. Computer security specialists within Iran would be able to support or conduct cyber attacks for the government.

B. RECOMMENDATIONS FOR FUTURE WORK

1. The Assessment of a CNA/E Capability by Terrorist Groups

Terrorist groups such as Al-Qaeda and Hezbollah use the internet as a tool for public relations and recruiting. Messages from terrorist leaders are often published to the

web prior to the mainstream media receiving hardcopies. Given a terrorist's modus operandi of seeking out asymmetric capabilities against a more powerful enemy, these groups may be seeking to develop a CNA/E capability. An analysis of selected terrorist groups' CNA/E capabilities and limitations may provide insightful information to determine this possibility.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[ACMICPC 03] Association of Computing Machinery and International Collegiate Programming Contest, The 27th Annual ACM-International Collegiate Programming Contest Asia Finals 2003, http://icpc.baylor.edu/icpc/regionals/RosterPublicFull.asp?ContestID=655, 2005
Last accessed on September 5. 2005.

[ACMICPC 05] Association of Computing Machinery and International Collegiate Programming Contest, The 29th Annual ACM-International Collegiate Programming Contest World Finals 2005, http://icpc.baylor.edu/past/icpc2005/finals/Standings.html, April 2005.
Last accessed on August 26, 2005.

[AMET 04] Africa & Middle East Telecom, "Mobile Handset Market in MEA Grows by 26 Percent," September 2004.

[AMET 04-1] "Alcatel Wins Private Sector ADSL Contract in Iran," Africa & Middle East Telecom, February, 2004.

[AP 05] Associated Press, "AP News: Iran, Syria to Form United Front," http://apnews.myway.com/article/20050217/D889VGEO0.html, February 16, 2005.
Last Accessed on January 10, 2005.

[Arabshani 97] Arabshani, Payman, "The Internet in Iran: A Survey," http://www.iranian.com/WebGuide/InternetIran/InternetIran.html, June 9, 1997.
Last Accessed on August 28, 2005.

[Ashiyane 05] Ashiyane Digital Security Team, Ashiyane Digital Security Team Website, http://www.ashiyane.com/, August, 2004.
Last accessed on August 26, 2005.

[Azgomi 05] Azgomi, Mohammad Abdollahi, Mohammad Abdollahi Azgomi's Homepage, http://mehr.sharif.ir/~azgomi/, 2005.
Last Accessed on August 26, 2005.

[Bakhtiari 01] Bakhtiari, Shahram, Shahram Bakhtiari Personal Website, http://sharif.ac.ir/~shahram/, July 20 2001.
Last accessed on August 26, 2005.

[Billo/Chang 05] Billo, Charles G., Chang, Welton, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf, November 2004.
Last Accessed on August 26, 2005.

[Boyd 05] Boyd, Clark, "The Price Paid for Blogging Iran," http://news.bbc.co.uk/2/hi/technology/4283231.stm, February 21, 2005.
Last accessed on August 26, 2005.

[Brown 04] Brown, Christopher, "Developing a Reliable Methodology for Assessing the Computer Network Operations (CNO) Threat of North Korea," 2004.

[Bugtraq 03] Bugtraq Mailing List, http://www.securityfocus.com/archive/1/319424, April 22, 2003.
Last Accessed on August 26, 2005.

[Bush 02] Bush, George W., 2002 State of the Union Address, http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html, January 29, 2002.
Last Accessed on August 26th, 2005.

[CIA 05] Central Intelligence Agency, "CIA World Factbook: Iran," http://www.cia.gov/cia/publications/factbook/print/ir.html, 2005.

Last Accessed on August 28th, 2005.

[DEFCON 05] DEF CON, “Defcon Groups Index Page,” http://www.defcon.org/html/defcon-groups/dc-groups-index.html, September 7, 2005. Last Accessed on September 8, 2005.

[Derakhshan 05] Derakhshan, Hossein, "Editor: Myself,” http://www.hoder.com/weblog/, August 21 2005. Last Accessed on August 29, 2005.

[Dingledine/Mathewson/Syverson 04] Dingledine, Roger, Nick Mathewson, and Paul Syverson, “Tor: The Second-Generation Onion Router,” 2004.

[Ebrahimian 05] Ebrahimian, Laleh D. "Socio-Economic Development in Iran through Information and Communications Technology,” The Middle East Journal, Winter 2003.

[Etemadi 05] Etemadi, Sauleh, Personal Resume, http://www.egr.msu.edu/~etemadys/Resume.pdf, 2005 Last Access on August 26, 2005.

[Ever 05] Ever, Joris. "Hacking for Dollars,” News.com, Jul 6, 2005.

[GSTP 05] Guilan Science and Technology Park. Guilan Science and Technology Park Website, http://www.gstp.ir, 2005. Last Accessed on August 26, 2005.

[ISCA 04] International Society for Computers and Their Applications, "17th International Conference on Computer Applications in Industry and Engineering (CAINE-2004),” http://www.isca-hq.org/CAINE-04-FINAL-PROGRAM.pdf, 2004. Last Accessed on August 15, 2005.

[IBHST 05] Iran Babol-Hacker Security Team, Iran Babol-Hacker Security Team Website, http://www.babol-hackers.com. Last Accessed on August 15, 2005.

[IHA 03] Iran Hack Association, Iran Hack Association Website, http://hackanjoman.persianblog.com/, 2003.
Last Accessed on August 15, 2005.

[IHST 05] Iran Hacking Sabotage Team, Iran Hacking Sabotage Team Website, http://www.ihsteam.com/, August 8 2005.
Last Accessed on August 26, 2005.

[ISCC 05] "3rd Iranian Society of Cryptology Conference, http://www.iscc2005.org/, August 2005.
Last Accessed on August 26, 2005.

[ITRC 05] Iran Telecommunications Research Center, Iran Telecommunications Research Center Website, http://www.itrc.ac.ir/, 2005.
Last Accessed on August 26, 2005.

[ITU 05] International Telecommunications Union: World Telecommunication Database, "Information Technology," 2005.

[IUT 05] Isfahan University of Technology, Isfahan University of Technology Website, http://www.iut.ac.ir/, 2005.
Last Accessed on August 26, 2005.

[Janes 05] Jane's Information Group, "Jane's Sentinel Security Assessment - Gulf States: Armed Forces, Iran," http://www.janes.com, 2005.
Last Accessed on August 26, 2005.

[Katzman 03] Katzman, Kenneth, "Iran: Arms and Weapons of Mass Destruction Suppliers," Congressional Research Center, http://www.usembassy.it/pdf/other/RL30551.pdf, 2003.
Last Accessed on August 26, 2005.

[Khatami 05] Khatami, Mohammad, "Views of the President," http://www.president.ir/eng/outlooks/sicence.htm, 2005.
Last Accessed on June 16, 2005.

[LOC 04] US Library of Congress, "A Country Study: Iran," http://lcweb2.loc.gov/frd/cs/irtoc.html, Oct 1, 2004.
Last Accessed on August 28, 2005.

[Mazaar 02] Mazaar, Michael, ed. Information Technology and World Politics. New York: Palgrave Macmillan, 2002.

[McWilliams 03] McWilliams, Brian. "North Korea's School for Hackers," http://wired-vig.wired.com/news/politics/0,1283,59043-2,00.html?tw=wn_story_page_next1, June 2 2003.
Last Accessed on June10, 2005.

[MEMRI 03] The Middle East Media Research Institute, "Top Iranian Defector on Iran's Collaboration with Iraq, North Korea, Al-Qaida, and Hizbullah," http://memri.org/bin/articles.cgi?Page=countries&Area=iran&ID=SP47303, 2003.
Last Accessed on August 26, 2005.

[Moustapha 04] Moustapha, Sano Koutoub, "Live Fatwa," http://www.islamonline.net/livefatwa/english/Browse.asp?hGuestID=LayrZP, February 23, 2004.
Last Accessed on August 26th, 2005.

[Moyes 02] Moyes, Mark, "Hacking For Democracy," http://www.shift.com/print/web/396/1.html, August 22 2002.
Last Accessed on December 15th, 2004.

[NEW 03] New Order, "Exploit code for Microsoft SMB authentication flaw," http://neworder.box.sk/explread.php?newsid=7782, April 24, 2003.
Last Accessed on August 26, 2005.

[Nicholson/Sahay 03] Nicholson, Brian, Sahay, Sundeep. "Building Iran's Software Industry: An Assessment of Plans and Prospects using the Software Export Success Model," http:/idpm.man.ac.uk/wp/di/index.htm, 2003.
Last Accessed on January 25, 2005.

[ORN 99] Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey," http://science-arts.org/internet/node1, 1999.
Last Accessed on August 26, 2005.

[OXR 04] OxResearch, "IRAN: Five-Year Plan Embroiled in Politics," 2004.

[PTP 02] Paradis Technology Park. Paradis Technology Park Website, http://www.hitechpark.com/Paradis/English/English.htm, 2002.
Last Accessed on August 26, 2005.

[Parthisan 05] Parthisan, "Abtahi's blog was hacked for revealing torture details," http://www.persianstudents.org/archives/001269.html, January 2 2005.
Last Accessed on August 26, 2005.

[Rouhani 00] Rouhani, Farhang, "The Spatial Politics of Leisure: Internet Use and Access in Tehran, Iran.," http://www.georgetown.edu/research/arabtech/wp/papers/frouhani.htm, April 16, 2000.
Last Accessed on August 26, 2005.

[Rubin 02] Rubin, Michael. "The Tehran Temptation," Commentary, January 2002.

[Sanaray 05] Sanaray Corporation. "ICT Laws and Regulations.," http://www.sanaray.com/english/Site.aspx?ParTree=AH&LnkIdn=791, 2005.

Last Accessed on August 28, 2005.

[SAT 05] "Russia to Deliver A Satellite to Iran.," Satellite Today, 4.25, 2005.

[Shannon 05] Shannon, Elaine. "An Ominous Pairing," Time, February 28th, 2005.

[Sharif 05] Sharif University of Technology, Advanced Information and Communication Technology Center Website, http://www.aictc.com/index.htm, 2005. Last Accessed on August 26th, 2005.

[Sherman 05] Sherman, Mark. "FBI: Businesses (Still) Reluctant to Report Cyber Attacks," Information Week, Aug 11 2005.

[Shokoohi 96] Shokoohi, Akbar. "Public Administration Reform for Economic Transformation in Iran: The Legal Framework," Asian Review of Public Adminstration, 8.2 (1996): 33.

[**Spider 04**] Spiderhacker, Spiderhacker Website, http://spiderhacker.persianblog.com, 2004.
Last Accessed on August 26th, 2005.

[TCO 04] Iranian Technology Cooperation Office, "Technology Cooperation Office," http://web.archive.org/web/20041130031440/http://www.tco.ac.ir/, 2004.
Last Accessed on August 26th, 2005.

[UNIDO 05] United Nation Industrial Development Organization, "Technology Parks - Iran," http://www.unido.org/en/doc/34918#io, 2005.
Last Accessed on August 26th, 2005.

[UNSD 05] United Nations Statistics Division, "Millenium Indicator: Telephone Lines and Cellular Subscribers Per 100 Populuation 2004," http://unstats.un.org, March 31, 2005.
Last Accessed on August 28, 2005

[USDOS 03] United States Department of State, "Patterns of Global Terrorism 2003," http://www.state.gov/documents/organization/31912.pdf, 2003.
Last Accessed on August 28th, 2005.

[UT 05] University of Tehran, University of Tehran Website, http://www.ut.ac.ir/, 2005.
Last Accessed on August 26th, 2005.

[Vamosi 02] Vamosi, Robert, "Is the US headed for a cyberwar? Actually, yes." Cnet.com, http://reviews.cnet.com/4520-3513_7-5021272.html, September 25 2002. Last Accessed on August 26th, 2005.

[Van Beveren 01] Van Beveren, John, "A Conceptual Model of Hacker Development and Motivations," Journal of E-Business 1.2 (2001).

[Varjani 04] Varjani, Ali Yazdian. Ali Yazdian Varjani Homepage, http://www.modares.ac.ir/eng/Yazdian/publication.htm, 2004. Last Accessed on August 26th, 2005.

[Wilson 04] Wilson, Clay. Information Warfare and Cyberwar: Capabilities and Related Policy Issues, Vol. RL3`787, CRS Report for Congress, 2004.

[WIKI 05] "Iranian blogs," http://en.wikipedia.org/wiki/Iranian_Blogs, May 21, 2005. Last Accessed on August 26, 2005.

[Zone 05] Zone-H. "Digital Attacks Archive.," www.zone-h.org/defacements, 2005. Last Accessed on August 26th, 2005.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dorothy Denning
   Naval Postgraduate School
   Monterey, California

4. James Ehlert
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Dartmouth College
   Institute for Security Technology Studies
   Hanover, New Hampshire

7. Paul Powell
   National Security Agency
   Ft. George G. Meade, Maryland

8. Andrew Macpherson
   University of New Hampshire
   Durham, New Hampshire

9. Clay Wilson
   Library of Congress
   Washington, District of Colombia