Assessing the Computer Network Operations Threat of Foreign Countries

Dorothy E. Denning

As the introduction to this book so aptly stated, advances in information technologies simultaneously empower and imperil those who use them. They empower by facilitating communications and the flow of information; they emperil by introducing new vulnerabilities and targets of attack. Information strategy has to adapt to both of these effects, exploiting and leveraging the enabling technologies while protecting against threats to the very same technologies we come to rely upon.

In this chapter I address the latter — the defensive side of information strategy as it applies to computer and networking technologies. Computer networks have become the target of an ever increasing number of hackers, criminals, spies, and others who have found advantage in exploiting and damaging them. These actors penetrate computer networks in order to steal, degrade, and destroy information and information systems. They launch computer viruses and worms, conduct denial-of-service attacks, vandalize websites, and extort money from victims. The effects have been costly: businesses disrupted or closed, military systems disabled, emergency and banking services suspended, transportation delayed, military and trade secrets compromised, and identity theft and credit card fraud perpetrated around the globe. The potential consequences of cyber attacks will only get worse as our use of and reliance on information technologies increase.

Many government officials and security experts believe that foreign governments pose the largest threat to computer networks, followed by terrorists. Of especial concern is a possible "electronic Pearl Harbor" or act of cyber terrorism that would affect a critical infrastructure such as the power grid or banking network, with devastating economic, social, or national security consequences. An attack against military networks could potentially undermine the armed forces' ability to effectively fight an adversary, especially during a time of conflict, and even attacks against civilian infrastructures, such as energy and telecommunications, could severely damage military capability because of widespread dependence on civilian systems.

So far, the number of reported cyber attacks attributed to foreign governments or terrorists has been relatively small, and none have been devastating. Cyber incidents attributed to governments have mostly involved espionage, and network attacks by terrorists and their sympathizers have fallen more in the domain of crime and vandalism than terrorism — mainly web defacements, denial-of-service attacks, and credit card fraud. In 1999 and early 2000, the Chinese government was accused of attacking foreign websites associated with the outlawed group Falun Gong,[1] but government sabotage of this type against foreign computers appears to be the exception. Today it seems more likely that the Chinese government would use its national firewalls to filter out objectionable websites than launch attacks against them. However, government exploitation of computer networks for intelligence purposes seems highly likely given intelligence exploitation of other telecommunications media.

The paucity of published information about what terrorists and governments are interested in and able to do in cyberspace, coupled with the fact that nothing resembling an electronic Pearl Harbor or act of cyber terrorism has occurred, has led many to question whether these threats have been overhyped or are even real. Yet, it would be as foolish to dismiss such threats as it would be to base policy and plans on speculation and unsubstantiated fear. Instead, we need well-grounded assessments of what potential adversaries are motivated to do and capable of doing.

We also need sound assessments of vulnerabilities in critical infrastructures and how risks can be mitigated. However, these evaluations can be conducted without regard to any particular actor or motive. Computer networks need to be protected from damaging attacks regardless of whether they originate from a runaway worm, a hacker out to see what's possible, a greedy crook who sees an opportunity for extortion, a former employee seeking revenge, a nation-state, or a terrorist. Computer worms alone have brought down emergency 911 services, a train signaling system, the safety monitoring system at a nuclear power plant, and ATM networks. Insiders determined to cause harm are in a particularly powerful position. In what was perhaps the most damaging infrastructure attack, a former contractor, armed with the requisite hardware, software, and knowledge, hacked a water treatment system in Australia and caused raw sewage overflows.[2]

Arguably, it may be more important to focus on protecting the networks rather than studying particular actors. However, there are also benefits to be gained by understanding the motives and capabilities of those who might attack them. First, if networks are attacked, we would be in a

better position to narrow down likely perpetrators. Second, if we enter into military conflict with a particular adversary, we would know what that adversary could and could not do to our military networks and critical infrastructures. Third, we may learn of capabilities and methods of attack that we had not considered.

In 2003, the Naval Postgraduate School began a study to assess the computer network operations (CNO) threat of foreign countries. The objective was to develop a general methodology that could be applied to any country and to apply it to specific countries as test cases. For our study, we chose Iran and North Korea. Our country results were published in two master's theses, one on Iran[3] and one on North Korea.[4]

In our project, we sought to elaborate a comprehensive methodology and were less concerned about producing a thorough, definitive assessment of the countries we chose. Indeed, because we limited our research to unclassified information available through open sources, we almost certainly missed key information about these countries. We did not attempt to determine what the intelligence services might know that we did not.

This chapter summarizes the results of our research. The next three sections describe our methodology and the results for Iran and North Korea. In the country sections, citations are to original sources where verified or found in the process of writing this paper. Otherwise, citations are to the theses. I have also added some of my own thoughts, which are presented without citation.

In the discussion of Iran especially, I have singled out specific individuals and groups who have engaged in CNO-related activities to illustrate the capability we found. In so doing, I do not mean to imply they are the only ones working in CNO or that they pose any sort of threat — indeed, many are working toward better information security.

METHODOLOGY

The US Department of Defense defines computer network operations (CNO) as comprising three types of operations: computer network attack, computer network defense, and related computer network exploitation-enabling operations.[5] Computer network attack (CNA) refers to operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Computer network exploitation (CNE) consists of enabling operations and intelligence collection to gather data from target or adversary computers and networks in support of CNA. Computer network defense (CND) consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. In short, CND refers to operations that protect against adversary CNA/E.

Outside the US military, it is common to use the term “attack” to refer to any operation that intentionally violates security policies and laws. This includes CNE as well as exploit operations conducted for the purpose of intelligence collection, not just to enable CNA. It is also common to see the term “security” for “defense” and to include within it protection against adversary

intelligence operations as well as information operations that disrupt, deny, degrade, or destroy. Both sets of terms are used in the discussion below.

Although the CNO threat is derived from attack/exploit operations rather than defense, we included the latter in our analysis. It is not possible to build strong defenses without knowledge of how systems are attacked, so the presence of a CND capability within a country implies at least some CNA/E knowledge. Furthermore, it seems unlikely that any country would develop a CNA/E capability if it is unable to defend its own networks from a counterattack, so the apparent lack of a CND capability would suggest a corresponding lack of CNA/E capability, assuming no information to the contrary. A country with a strong CND capability would be in a much better position to build and use a CNA/E capability than one without.

To assess a foreign state's CNO threat, we looked for indicators of capability and intent to conduct CNO. These indicators were based on generic factors that could be applied to any country. The factors were grouped into four general categories:

- Information technology industry and infrastructure
- Academic and research community
- Government and foreign relations
- Hacking and cyber attacks

The categories are not entirely disjoint. For example, government-sponsored research on CNO falls into the second and third categories, and government-sponsored cyber attacks fall into the

third and fourth. In the discussion below, we have generally assigned each type of activity to a single category and treated it in that context.

Within each category, we began with an initial set of questions to guide our search for information, although we did not limit our collection to those questions. In many cases, we could not answer the questions directly but found other information that was useful for our analysis.

All of the information we used was unclassified. Most was acquired through the Internet and personal contacts in the United States and countries other than those we studied. A more complete picture could be obtained with access to classified information or to persons within the countries of study. It was especially difficult to obtain information that originated in North Korea owing to the closed nature of the country and its apparent isolation from the Internet.

Most of the material we used was in English. We arranged for translation of a few web pages in Farsi that we thought might be useful for the Iranian study, but limited time and resources precluded translating more. For the most part, we simply ignored websites and documents that were not in English. A comprehensive study that includes more foreign language sources could very well turn up evidence we did not find.

We made extensive use of Google searches to find relevant information. These searches led us to web pages that we had not found by simply browsing institutional websites. However, we did not have time to pursue all search hits or to try an extensive set of search strings, which leaves open the possibility that we missed a large amount of useful information. For future study, it would be

worthwhile to try to identify a collection of search strings that would likely uncover most of the relevant information that can found through open-source searches.

We began our study in October 2003. Two students were assigned to the project, one for Iran and one for North Korea. Their objective was to report their results in the form of separate master's theses for a September 2004 graduation.

In March 2004, we were invited by the Institute for Security Technology Studies at Dartmouth College to review a draft report of a study whose objectives were very close to our own. At that time, we were far enough along with our own work to provide feedback on theirs, and their study provided valuable input for our own. Their final report was published in November 2004,[6] after our study of North Korea was complete but while we were in the middle of our Iranian study. The Iranian study was delayed for a year because the student conducting the work had an unexpected reassignment of duties. Another student later joined the project to see it through to a September 2005 completion.

The Dartmouth group took a somewhat different approach in their analysis. In particular, they organized evidence indicative of capability or intent into two categories. Category 1 evidence consists of direct links to a foreign cyber warfare capability. It is derived from US government reports (which we did not use), foreign official statements, and foreign military and intelligence agency research. Category 2 evidence consists of circumstantial links indicating a baseline information technology infrastructure necessary to support a cyber warfare operation. The Dartmouth country reports are organized around these categories and sources of evidence,

whereas ours are organized around the four categories of activity described above. The Dartmouth report also covers six countries, including the two we studied. Besides Iran and North Korea, they studied China, India, Pakistan, and Russia.

The following subsections describe the four areas of activity we investigated, our rationale for looking at these areas, and the type of information we sought.

Information Technology Industry and Infrastructure

Our goal here was to assess a country's information technology (IT) industry and its information infrastructure. In the area of IT, we examined the country's hardware and software industry, IT service companies, access to international IT supply chains, industry partnerships with foreign companies, and IT professionals in the country; we paid particular attention to companies that provided CNO-related technologies or services. However, other areas of technology are also relevant. If a country does not have access to or experience using popular hardware and software platforms, such as Microsoft Windows and related products, it will be at a disadvantage in terms of developing a capability to attack or defend those systems. Also, many of the skills used in one area of IT, such as general knowledge and skills in computer networks, operating systems, and programming, are transferable to CNO.

In the area of infrastructure, our main interest was computer networks, especially the Internet and intranets, but we also considered the country's telecommunications and electrical infrastructures,

since both support networking. If telecommunications or electricity is inadequate or unreliable, it may be difficult to launch a sustained attack against another country.

For computer networks, we considered prevalence, connectivity, capacity, technologies and platforms used, presence of Internet service providers (ISPs), and government regulations. We reasoned that a country that is well connected through modern technologies and high-speed links is in a better position to develop a CNO capability than one that is not, as it can draw on the considerable expertise and talent acquired through use of the networks. Internet penetration is particularly valuable, because it gives the population access to global CNO resources, such as hacking tools and "how to" guides, as well as to international targets to attack. But even a country that has promoted a national intranet while stifling or prohibiting Internet use is in a better position than one that has little networking of any type.

We also considered the legal and regulatory infrastructure as it pertains to CNO, including computer crime laws and their enforcement. A lack of laws in this area could be indicative of little hacking activity within the country or against the country's computer systems, in which case one might conclude that the country has little or no CNO capability, offensive or defensive, at least outside government. However, an absence of cyber crime laws might also mean that more general laws (e.g., governing sabotage and fraud) are considered sufficient for prosecuting cyber attacks.

Academic and Research Community

For this category, we assessed the extent to which faculty and students engaged in educational and research activities that support a CNO capability. We also examined research conducted in the public domain by persons outside the academic community. Research areas we examined include system and application vulnerabilities, computer crime and network attacks, technologies and methods of defense, and CNO policy and legal issues. Within this broad research community, we looked for CNO-related publications and projects. We also looked for conferences and workshops hosted by members of the community within the country or attended by members of the community in other countries.

In the academic community, we focused on higher education. We looked for courses in areas of CNO and for faculty and students who were conducting research or publishing papers related to CNO. We tried to determine whether any faculty members who were engaged in CNO activity had been educated outside their country and whether students studied CNO abroad. Much of our information was obtained by searching online for school websites and résumés containing CNO-related entries.

We also examined general education in IT and the IT skills of students at all levels, including primary and secondary school. We were especially interested in whether college students in the country participated in the annual ACM International Collegiate Programming Contest,[7] and if so, how well they did. The ACM programming contest, which traces it roots to a competition at Texas A&M University in 1970, has evolved into a multitiered competition involving three-person student teams from around the world. In 2005, the contest drew 4,109 teams from 1,582 universities in 71 countries. We reasoned that a country needs talented programmers to develop

new or sophisticated cyber attacks, so placing well in the contest would suggest the presence of a talent base on which to draw.

Government and Foreign Relations

Here we considered efforts on the part of government agencies to develop a CNO capability. We looked for signs that the government was creating one or more CNO units or teams, conducting training in CNO, or sponsoring or conducting research on CNO. We also looked for documents or statements from official government sources that outlined government policy or doctrine on CNO.

We tried to determine whether the government was using the Internet for intelligence collection, and if so, whether its tactics went beyond open source collection to hacking into computer networks. We reasoned that a government with the ability to penetrate and exploit foreign networks for intelligence collection would have a head start on developing a CNO capability, as many of the same skills are needed.

We considered a government's relations with other countries to determine whether it might acquire CNO-related resources from another country. Such resources might include information, technology, or training in CNO. We also looked for motives and objectives that might lead the government to conduct a cyber attack against another country.

Hacking and Cyber Attacks

This category focused on actual cyber attacks originating in the study country. We considered attacks by all types of actors, from teenage hackers to criminal groups to government agencies. (Often, however, it is not possible to determine the source of an attack.) We tried to identify nongovernment hacking groups and individual hackers operating from within the country.

We wanted to know what types of attack the country's hackers conducted and what tools and methods they used. We considered all types of attack, including denial-of-service attacks, web defacements, launching of viruses and worms, use of Trojan horses and spyware, and so forth. We considered cyber operations that acquired sensitive information, including trade secrets, personal information such as Social Security or credit card information, and sensitive government information.

Although we examined attacks against international targets, we were especially interested in cyber attacks against US systems and whether such attacks were politically motivated. Patriotic Chinese hackers, for example, attacked US systems after the 1999 US bombing of the Chinese embassy in Belgrade during the Kosovo conflict and then again in the wake of the US-China spy plane incident in 2001.

We tried to determine how the government responded to hacking by its citizens. We wanted to know if specific attacks, particularly those against US systems, were tolerated, encouraged, or even supported. We wanted to know if the government hired hackers or otherwise made use of

hackers' expertise or skills. A country with an active hacking community can draw on that community to develop its CNO capability; it could recruit them into the military or an agency with CNO authority, employ their services as consultants or trainers, or participate in their activities, such as conferences and online discussion groups. However, if hackers are hired, there is a risk that they will attack the government's own systems or otherwise engage in illegal or inappropriate hacking. A country might also encourage its hackers to participate in a war against another state as "citizen cyber soldiers."

IRAN

Jason Patterson and Matthew Smith, both lieutenants in the US Navy, performed our study of Iran. They found considerable amounts of information on Iranian websites, particularly sites associated with universities, government-sponsored research centers, hacking groups, and industry. Although they concentrated their efforts on sites that were in English, they obtained translations of a few sites that were in Farsi. They completed their study in September 2005.[8] The following subsections summarize some of their key findings and provide additional information and analysis not included in their thesis.

IT Industry and Infrastructure

Iran's information infrastructure has been undergoing growth and modernization since the first of a series of five-year plans adopted by Parliament in 1990. The plan, which aimed to restore the

Iranian economy in the wake of the Iran-Iraq war, included requirements for information and communications technology.[9]

As of 2003, Iran had about 27 main telephone lines and cellular subscribers per 100 people, which represented a 670 percent increase from 1990, when there were only 4 such lines and cellular subscribers. However, the numbers are still low compared with, say, the United States, which had 117 per 100 population in 2003.[10]

Iran provides access to the global telecommunications network through fiber-optic and satellite links. A 721 km segment of the Trans-Asia-Europe Project, the world's largest overland fiber-optic system, passes through Iran, transmitting data at 622 megabytes per second. In addition, an underwater link transmitting at 140 megabits per second connects Iran to the United Arab Emirates. Satellite communications were achieved with Inmarsat land earth stations connected to commercial satellites, although Iran is now in the process of creating its own satellite network, to include two Russian-supplied Zohreh satellites, five land stations, 135 primary and secondary stations, 27 zonal stations, 31 community stations, and 1,374 rural stations.[11]

Iran's foray into the Internet began in the early 1990s when the Institute for Studies in Theoretical Physics and Mathematics joined BITNET through Iran's membership in the Trans-European Research and Education Networking Association. As BITNET was absorbed into the Internet, the Iranian node developed into a Class C Internet node. By 2000, Iran had over 30 ISPs.[12]

According to the International Telecommunications Union, the proportion of Internet users in Iran rose from 1.6 percent in 2001 to 7.2 percent in 2003.[13] By December 2005, it was up to 10.8 percent, or about 7.5 million people.[14]

While promoting the Internet, the Iranian government also censors it. This is done largely under the wide-ranging Press Law of 1986. According to a study by the OpenNet Initiative, the government blocks access to most pornographic sites and anonymizer tools, a large number of sites with gay and lesbian content, some politically sensitive sites, women's rights sites, and certain targeted web logs (blogs).[15] The study did not examine whether any hacking sites were blocked. ISPs use filtering software developed in the United States to block foreign sites. Sites based in Iran may be shut down, suspended, or filtered. Operators and authors are subject to pressure and even arrest.

Iran's hardware and software industries are wanting, hampered by state controls, restrictive trade policies, external trade embargoes, contradictory legislation, and a lack of software management expertise within the industries themselves. Iran has approximately 200 companies involved in software development and 20,000 workers in the software industry.[16]

In the area of CNO, we identified one company, Sharif Secure Ware, that bills itself as a network security and consultation company.[17] We also found a software development company, Systems Group, that formed an alliance with a German security company, Securepoint Security Solution. Under an arrangement announced in July 2005, Systems Group will be the exclusive representative of Securepoint products and services in Iran. Together the two companies seek to

become the leading Iranian security software company. With almost 600 employees and 4,500 customers, Systems Group claims to be the largest software corporation in Iran.[18] That Systems Group would team with a German security company suggests that Iran might not have a competitive domestic security company, although there could be other reasons behind the partnership.

Iran does not have any laws that define or specifically prohibit cyber crimes. There are copyright protections for domestically produced software, but the laws are seldom enforced and do not apply to imports. Software pirating and hacking both run rampant.[19]

Academic and Research Community

Iranian universities have strong IT programs, including computer science and computer engineering. They have been active in the ACM programming contest, and two universities did as well as any US schools in the world finals held in Shanghai in April 2005. Teams from Amirkabir University of Technology and Sharif University of Technology, both located in Tehran, tied for 17th place along with Penn State and the University of Illinois.[20] Some 60 teams from 41 schools participated in the Tehran regionals leading up to the Asia-Pacific regionals and then the world finals. Four of the top ten in the Tehran regionals were from Sharif University of Technology.[21] Sharif did even better in the 2006 contest, placing 13th, ahead of all US schools except the 8th-ranked Massachusetts Institute of Technology.[22] These results show that Iranian schools are producing the programming talent needed to conduct CNO, even if the skills are being employed for other purposes.

We identified several universities engaged in CNO education research. These include Sharif and Amirkabir, plus the University of Isfahan and Isfahan University of Technology.

At Sharif University of Technology, we found faculty and students with interests in computer security. One professor, Shahram Bakhtiari, has taught courses titled Cryptography and Network Security, Computers and Networks Security, and Systems and Networks Security. According to the course description for the third, "Students who take this course become familiar with methods of attack and the ways to protect systems and networks." His website includes links to class presentations, including one on "Hacking Techniques" and one on "IP Security Flaws." Professor Bakhtiari has also published numerous papers on cryptography in journals and conference proceedings. He ran three workshops on information security in Iran: a 1999 workshop held in conjunction with the Computer Society of Iran's annual international conference, a second 1999 workshop held with the Iranian Conference on Electrical Engineering, and a 2001 workshop held with the International Internet and Electronic Cities Conference.[23]

Mohammad Abdollahi Azgomi, a PhD candidate at Sharif, wrote his master's thesis on network security and published papers on firewalls and other security topics.[24] Hashem Habibi, a master's student in software engineering working with "a huge number of other people" on network security, has links to security and hacking sites on his homepage at Sharif. His website also has photos of himself and others associated with the Network Security Center and with "Seclab."[25] Sauleh S. Etemad, an alumnus of Sharif, taught courses and wrote technical reports on network and operating systems security at Iran's Advanced Information and Communication Technology

Center before going on to earn a master's degree in electrical and computer engineering from Michigan State University. At Sharif, he completed his bachelor's thesis on operating systems security.[26]

In late 2005, I received an e-mail from a graduate student at Sharif who was completing a master's thesis on the topic of stream ciphers. His research interests included coding and cryptrographic protocols, and he was interested in pursuing a PhD as a member of my group. He had already published two conference papers.

Sharif has hosted information security conferences, including the Second Iranian Society of Cryptology Conference and the Operating System and Security Conference 2003. In addition, it has hosted more general IT-related conferences and a conference on electronic warfare.[27]

Amirkabir University of Technology houses a Data Security Research Laboratory within the department of Computer Engineering and Information Technology. The role of the laboratory is to help promote "research and innovations on computer, information, and communications security" and to help train engineers and scientists in related areas.

Two students affiliated with the lab, Haamed Gheibi and Salman Niksefat, taught a workshop on hacking operating systems at a conference held in Tehran in 2004. They also posted information about a Microsoft Windows security flaw on a computer security electronic mailing list, Bugtraq, in 2003, after unsuccessful attempts to gain the attention of Microsoft. Gheibi represented Amirkabir in the 2003 ACM programming contest.[28]

Several faculty members at Amirkabir listed computer security as an area of interest. One professor, Mehran Soleiman Fallah, works extensively in the computer security field. His PhD thesis was on denial-of-service attacks, and he has published several papers on this topic. He has also taught an undergraduate course on network security and three graduate courses on information security and network security.[29]

At the University of Isfahan, we found two professors who conduct computer security research: Ahmad Baraani-Dastjerdi and Behrouz Tork Ladani. Baraani's area of research includes cryptography, database security, and security in computing.[30] Ladani's includes cryptographic protocols, information system security, and network security. In 2005, Ladani also taught undergraduate courses on cryptography and network security and on security in computer systems. He received his PhD from the University of Tarbiat Modares, Iran, where he wrote his thesis on cryptographic protocols.[31] This would suggest that faculty at Tarbiat Modares are also conducting CNO-related research, which is confirmed in the next paragraph.

Isfahan University of Technology hosted the Third Iranian Society of Cryptology Conference in September 2005. The conference covered a broad range of topics in cryptography and computer and communications security. Several faculty members at the university served on the conference committee, so we can assume that there is some CNO-related research taking place at the school. The committee also included representatives from Sharif University of Technology (nine people, including Bakhtiari), Amirkabir University of Technology (Fallah), the University of Isfahan (two, including Baraani), Tarbiat Modares, and several other schools and research

institutions.[32] We did not attempt to track down all 34 people on the committee, but the size of the committee alone indicates a substantial community of security researchers in Iran, most likely numbering at least a hundred or two. That Iran has a Society of Cryptology, which has sponsored at least three conferences, is further proof of an active and established security research community.

We found several websites in Farsi relating to network security. These included sites for the IR Computer Emergency Response Team (www.ircert.com), Iran Security (weblog.iransecurity.com), Iran Virus Database (www.irvirus.com), and Hat-Squad Security Group (www.hatsquad.com). These sites appear to discuss network vulnerabilities, with the objective of promoting better security.[33] Hat-Squad offers security risk assessment, training, consultancy, incident response, penetration testing, and advisories that describe vulnerabilities and exploits.

We did not find any research or discussion on how Iran might employ CNA against its adversaries or the need to defend critical infrastructures in Iran from adversary CNA. The focus seems to be on security in general and on technology.

Government and Foreign Relations

The Iranian government promotes research and development in IT through several institutions, among them the Iran Telecommunications Research Center, the Technology Cooperation Office, Guilan Science and Technology Park, and Pardis Technology Park.

The Iran Telecommunications Research Center (ITRC) was formed in 1970 as the research arm of the Ministry of Information and Communications Technology. Research is organized into four departments: Information Technology, Strategic Management, Networking, and Transmission. Network security and security management are part of the center's research agenda, and one of the workshops on information security run by Shahram Bakhtiari of Sharif University of Technology was held at ITRC.[34]

ITRC is also involved in standards setting. It is a member of the European Technical Standards Institute and has created study groups aligned with the International Telecommunications Union study groups. Study group 17 is on security, languages, and telecommunications software.[35]

We found three researchers at the center who had presented papers on network security at international meetings. Mehdi Rasti, Davood Sarramy, and Mahmood Khaleghi gave a paper on network security assessment at a computer applications conference in Orlando, Florida, in 2004. In 2003, Rasti gave a paper on anomaly detection at the same conference in Las Vegas, Nevada.[36]

The Technology Cooperation Office (TCO) was founded in 1984 to serve the president of Iran. Its mission is to support development and cooperation in advanced technologies, including IT. Among the forms of support it offers Iranian institutions are coordinating joint research projects and establishing relations with foreign industrial and scientific research centers.[37]

Guilan Science and Technology Park was established in 1989 as the Iranian Research Organization of Science and Technology. The research center was reorganized as a technology park in 2002. One of the focus areas for the park is IT, and several IT companies have offices in the park. We did not identify any CNO-specific activity at the park.[38]

Pardis Technology Park (PTP), located 20 km from Tehran, was established in 2001 by TCO in order to create an environment for researchers, educators, and companies suitable for developing Iran's high-tech industry.[39] PTP's objectives are to intensify high-tech industry development; promote cooperation among industry, academia, and government research centers; create synergy between private and state sectors; commercialize know-how and innovations generated by research centers; and promote research and development in the private sector. PTP is run by a board of directors whose members are designated by TCO and Sharif University of Technology. The network security company Sharif Secure Ware is among the 45 companies that have signed a contract to purchase land at the park.[40]

We found no evidence that the Iranian government was developing a CNA/E capability against its adversaries. However, given Iran's pursuit of asymmetric warfare capabilities, including nuclear weapons, ballistic missiles, and support for terrorism,[41] it is possible that it will pursue, if it is not already, a CNA/E capability as well. If so, it might collaborate with North Korea, which purportedly has been training cyber warriors for years (discussed below). According to reports, Iran has cooperated with North Korea on military technology training and transfer in the past, including development of missile systems. Iran has also sent military and intelligence officers to North Korea for training in psychological warfare and counterespionage.[42]

Hacking and Cyber Attacks

Iran has numerous hackers and hacking groups, some of which also sell network and security services. One such group is IHS Iran Hackers Sabotage. According to their website, the group was formed in 2004 "with the aim of showing the world that Iranian hackers have something to say in the world wide security [sic]." After "rooting many important servers," they decided to participate in the "vulnerability assessment and exploitation process" and to offer a "highly secured hosting service." Their website offers several original exploitation programs for download, each written for Visual C++ and based on vulnerabilities reported by others. The group consists of three active members, two of whom say they are university students.[43]

As of October 2005, IHS had defaced over 3,700 websites.[44] All of the defacements we examined contained political messages. For example, a defacement on 25 July 2005 against the US Naval Station Guantánamo's public website emphasized that Muslims were for peace, not terrorism, and that many had been harmed in Israel, Iraq, and Guantánamo.[45] On 2 October 2005, a defacement of a Novell site proclaimed that Iranians had a right to atomic energy and that "NO one can rule us not to use atomic power."[46]

Another group, the Ashiyane Digital Security Team, which sells web hosting and network and security services, has defaced over 2,800 websites. Their website includes tools and tutorials on hacking and security, a discussion forum, a link to their web defacements, and a list of over 3,500 registered users interested in security and hacking.[47]

Assuming most of the registered users are Iranian, which seems likely given that much of the website is in Farsi, we can conclude that there are thousands of people in Iran interested in network security and hacking.

A defacement of the National Aeronautics and Space Administration's website on 11 August 2005 challenged US policy in the Middle East,[48] but most of the Ashiyane defacements we examined did not contain a political statement. In one case an attacker who goes by the name ActionSpider left his e-mail address and offered to help protect the site from other hackers; in another, the attacker offered free help patching the hacked server.

Ashiyane team members boast a wide range of experience in operating systems, programming languages, and hacking, including firewall penetration, database and operating system hacking, software cracking, and social engineering (conning a victim to perform some task, such as disclosing a password). Several members taught fee-based courses on hacking and other topics at a vocational school in Tehran.[49]

Among the other Iranian hacking groups we found are Iranian Boys Black Hat, Iran Hackers Association, Iran Babol-Hackers Security Team, Crouz Security Team, and Persian Crackers. Iranian Boys Black Hat has defaced as many sites as Ashiyane (over 2,800). As far as we could tell, none carried political messages. This was also true of defacements by Iran Babol-Hackers Security Team (over 400), which some members claim are "just for fun."

Iran formed a Defcon group in February 2004. Defcon groups are local groups associated with the annual Defcon meeting, which bills itself as the "largest underground hacking event in the world," drawing thousands of information security experts, hackers, and government officials to Las Vegas every summer for talks and hacking contests. The individual groups serve as local gathering places for discussions of technology and security. Iran's Defcon group was based in Tehran, but apparently it had ceased to exist by April 2006.[50]

Besides web defacements, we found evidence of other political hacking within Iran. For example, the weblog of former vice president Mohammad Ali Abtahi was hacked several times after he posted entries about government torture of other bloggers, and the website of former presidential candidate Ali Larijani was subjected to a distributed denial-of-service attack. Larijani's campaign committee claimed that his site was hacked by the opposition. Bloggers theorized that the government was responsible for the attacks against Abtahi and Larijani, but no supporting evidence was provided.[51]

Iranians have also acquired and used software that bypasses the government's Internet filters. In an interview with Shift.com, Oxblood Ruffin, founder of Hacktivismo, reported that their software was being used in Iran. We did not find evidence of Iranians developing their own anticensorship software.[52]

Summary

Although less than 11 percent of Iranians were online at the end of 2005, Iran has a sizable community of interest and expertise in computer network attack and defense. We estimate that there are 100 or more academics working in information security, publishing research papers in journals and conference proceedings, hosting and attending conferences, and teaching courses on network security topics. Although we could not determine sponsorship for this work, it is probably fair to assume that it is at least approved, if not also funded, by the government.

We also estimate that there are thousands of additional hackers and network security specialists. Many of them have experience in breaking into websites and conducting other types of attacks. Some offer network security products, services, and training.

The Iranian government is actively promoting many areas of IT, including networks, with the goal of stimulating economic growth. Although we found government-sponsored research in network security taking place within government labs, we did not identify any government involvement in cyber attacks or any government effort to develop a CNA/E capability against adversary countries. However, should government officials decide to develop such a capability, they could draw on the Iranian IT community to put together an attack team.

All of these findings indicate that Iran is concerned about network security and taking steps to defend its networks, advance the common body of knowledge in security, and exploit the commercial market for network security products and services. It also has its share of hackers, including people who deface websites. This is all to be expected in today's interconnected world, which has been attracting an ever increasing body of cyber vandals, crooks, and spies, as well as

people devoted to improving computer defense. Any country that would ignore network security would do so at its peril. From open sources, we did not find indications that Iran's efforts in network security are motivated by a desire to conduct crippling attacks against the infrastructures of other countries.

NORTH KOREA

Our study of the Democratic People's Republic of Korea (DPRK) was conducted by Navy Lt. Christopher Brown and completed in September 2004.[53] We found very little information coming directly from inside North Korea, and most of that was posted on websites belonging to the government. Hence, we relied more on second-hand information provided by governments, news agencies, and scholars residing in other countries. The following subsections summarize some of the key findings.

IT Industry and Infrastructure

North Korea is one of the most disconnected countries in the world. In 2001, it had 1.1 million telephone lines,[54] which represents less than 5 lines per 100 population, compared with 27 for Iran and 117 for South Korea and the United States. North Korea began to develop a cellular infrastructure, but in May 2004 the government banned mobile phones in order to limit foreign influences. The country owns two satellites, an International Telecommunications Satellite (Intelsat) and a Russian satellite, both operating in the region of the Indian Ocean. The French provide technical support.[55]

The situation with the Internet appears to be even worse. Although North Korea has a top-level domain name (.kp) and two assigned Class C Internet protocol (IP) address blocks with 131,072 addresses, we found no evidence of any activity originating from these assigned IP addresses or the .kp domain.[56] A Google search of the .kp domain returned 147 hits on 24 October 2005, but none of the websites were accessible, and no content was displayed with the search results, unlike most searches, which return two lines of content for each matching website. It is possible that the sites are registered but not yet used. Alternatively, the sites may be up but inaccessible from the United States or outside North Korea.

We did find North Korean websites hosted in other countries, including China, Japan, and Australia. The small handful of official state-sponsored sites we found were located on servers in China and Japan.[57] The website for the Korean Central News Agency of DPRK, for example, is in Japan (at http://www.kcna.co.jp/).

Internet access in North Korea is extremely limited. An Internet café was opened in Pyongyang in May 2002, but the rates were reported to be about $10 per hour, more than one-fifth of the average North Korean's monthly earnings. Thus, the café is believed to serve mainly visiting businessmen, tourists, and diplomats. Some hotels in Pyongyang also provide Internet access, but again for visitors.[58] We did not find any information regarding Internet access for the general population. Considering the ban on cell phones, it seems likely that Internet access is highly restricted, if even available.

North Korea has a national intranet. The Kwang Myong (Bright Star) Network runs through fiber-optic cable with a backbone capacity of 2.5 gigabytes per second.[59] Developed in 1996 with the goal of linking various research and academic institutions, the Bright Star Network now also includes government and military agencies, as well as public access. By November 2004, several PC cafés were open in Pyongyang, providing access to e-mail, internal websites, chat, online games, and streaming movies over a 100 megabit-per-second fiber-optic link to the national intranet. The largest café, located by a subway station, has around 100 computers.[60] A 2001 report indicated that North Korea had begun testing a firewall between the Bright Star Network and the Internet in order to screen and restrict information flows in both directions.[61]

Telecommunications and networking depend on power, and North Korea's electrical infrastructure is both antiquated and unreliable, with frequent power outages and poor frequency control. Since reliable and stable power is needed for sustained computer network operations, North Korea's ability to conduct CNA/E against its adversaries is probably limited.[62]

North Korea has developed a personal data assistant (PDA), the Hana-21, based on an original Korean operating system. However, much of its IT hardware sector is technologically dated, and computers and communications equipment are imported from China and Southeast Asia.[63] Technology exports to North Korea are severely restricted under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, limiting North Korea's ability to acquire advanced information technologies from signatories of the treaty (which includes the United States and South Korea but not China).

North Korea's software industry is closely tied into its research institutions, including the Korean Computer Center, the Pyongyang Programming Center, and Kim Il Sung University. Areas of focus include voice recognition, language translation, gaming, animation, multimedia, and biometrics.[64] Except for biometrics, which can be used for network security, these technologies are not germane to CNO.

We did not find any laws specifically addressing the Internet, including computer crime laws. However, telecommunications are heavily censored, and all international telephone calls are facilitated through a state-run exchange operator, which is closely monitored. Until computers, telephones, and the Internet become more prevalent, North Korea may not see much need for computer crime laws.

Academic and Research Community

North Korean leader Kim Jong Il has said that there are three basic types of fools in the twenty-first century: people who smoke, people who do not appreciate music, and people who cannot use the computer. An avid Internet user, he has stated that IT is the future of North Korea and that those who do not educate themselves in it will be left behind. Hence, it is not surprising that computer education is mandatory and emphasized, starting in grade school. Computer science has topped the list of curriculum choices among young military officers and college students, and possessing a computer-related job is considered a sign of privilege. North Korea does not participate in the ACM programming contest, but students can submit software they have developed to a government-sponsored national programming contest.[65]

We found three major academic institutions in North Korea actively involved in IT: Pyongyang University of Computer Technology, Kim Chaek University of Technology (KUT), and Kim Il Sung University. Faculty at Kim Il Sung University have developed security-related software products, including Worluf Anti-Virus and Intelligent Locker.[66]

In 2001, KUT and Syracuse University began discussions on the possibility of research collaboration in integrated information technology. By June 2004, KUT representatives had made three visits to Syracuse, and the Syracuse team had made one trip to North Korea. The general area of collaboration is systems assurance, in particular technology to foster trusted communications. Although "trusted communications" is often linked with cryptography and network security, the group seems to be concerned more with integrity, safety, and reliability than network defense. The current focus has been on using open-source software to produce a back-end library management system for the KUT digital library. The group has produced designs for twin research labs, software specifications, joint work on proving software correctness, research presentations, and an academic paper.[67]

Government and Foreign Relations

North Korea has seven research institutions focused on IT. The most prominent are the Pyongyang Informatics Center, the Korea Computer Center, the DPRK Academy of Sciences, and Silver Star Laboratories.

The Pyongyang Informatics Center (PIC) was established in 1986 to develop computer-based management techniques and to help promote the use of computers in government and industry. Its primary focus is software development, and PIC has produced a variety of products, including the software filters used between the Bright Star Network and the Internet, which serve a role in computer network defense as well as censorship. However, most of PIC's development work seems to be in areas unrelated to CNO, including electronic publication, computer-aided design, embedded Linux, web applications, interactive programs, accounting, and virtual reality. This assessment is supported by a report that in 2001, researchers at PIC requested 250 IT books from South Korea; they were especially interested in books on graphics and virtual animation but also on common operating systems and communication methods. The list did not include any books relating to cyber security.[68]

The Korea Computer Center (KCC) was established in 1990 to promote computerization. With 800 employees at its inception, it has produced some of North Korea's cutting-edge software, including systems for voice recognition, fingerprint identification, and artificial intelligence. It has produced a Korean version of the Linux operating system, and its chess playing software has dominated Japan's annual Chinese chess competition.[69]

The KCC is directed by Kim Jong Nam, the son of Kim Jong Il. Nam, who also heads the State Security Agency (SSA), which is North Korea's intelligence service, moved SSA's overseas intelligence unit into the KCC, according to a South Korean newspaper. South Korean media have also claimed that the KCC is "nothing less than the command center for Pyongyang's cyber

warfare industry, masquerading as an innocuous, computer geek–filled software-research facility."[70]

The DPRK Academy of Sciences and Silver Star Laboratories are also involved in software development. Between them, they have produced software for language translation, optical character recognition, artificial intelligence, multimedia, remote control, and communications. We did not find any indications that either institute had developed CNO-related software.[71]

In 1984, North Korea established the Mirim Academy, which offered a two-year program in IT and electronic warfare for top military students. Two years later, the school became a five-year college, Mirim College, and opened admissions to high school students from the top percentile. The school, also known as the Automated Warfare Institute, purportedly offers curricula in command automation, computers, programming, automated reconnaissance, and electronic warfare.[72]

According to a June 2003 news report, Maj. Gen. Song Young-keun, commanding general of South Korea's Defense Security Command, said that North Korea has been producing 100 cyber soldiers annually.[73] In May 2004, at a conference in Seoul organized by the Korea Information Security Agency (KISA), Song said that "Following orders from Chairman Kim Jong Il, North Korea has been operating a crack unit specializing in computer hacking and strengthening its cyber-terror ability." He said that the hackers were handpicked from among the top graduates of Kim Il Sung Military Academy and given intensive training in computer-related skills before being assigned to the hacker's unit.[74] According to East-Asia-Intel.com, which provides news on

the Far East, Mirim College was renamed Kim Il Military Academy and later Pyongyang College. The news site also reported that Byun Jae-Jeong, a research fellow at the South Korea Agency for Defense Development, claimed that the cyber agents had a technical ability on a par with that of CIA hackers and that they were able to "infiltrate and gather information from Web servers from various countries."[75]

Developing a CNA/E capability is certainly consistent with Kim Jong Il's interest in IT and his military objectives — to "disturb the coherence of South Korean defenses in depth including its key command, control, and communications, and intelligence infrastructure."[76] Moreover, Richard Clarke, former special adviser to the president for cyberspace security, reported that North Korea was "developing information warfare units, either in their military, or in their intelligence services, or both."[77]

Hacking and Cyber Attacks

At the 2004 conference in Seoul, Maj. Gen. Song Young-keun claimed that North Korea's military hackers had been breaking into the computer networks of South Korean government agencies and research institutes to steal classified information.[78] We also found reports of other cyber attacks being attributed to North Korean hackers. However, Director Baek, of South Korea's National Intelligence Service (NIS), told us in a telephone interview in April 2004 that NIS had no knowledge of confirmed CNA/E activities originating from within North Korea, or of North Korea sponsoring CNA/E against any country. This view was echoed by officials at KISA.[79]

We found no evidence that North Korea has hackers operating outside the government. Given the severe restrictions on Internet use within the country, any hacking being conducted from North Korea would most likely be government sponsored. Within the government, hacking seems to be confined to the KCC and Mirim College (Kim Il Military Academy/Pyongyang College).

Summary

North Korea most likely has a CNO capability within its military and intelligence services. It appears to recognize the value of IT and CNO to its future and to have devoted resources to training and supporting cyber warfare units.

Whether North Korea's CNO capability has been used to attack targets in South Korea, the United States, or elsewhere is less certain. The capability may be used primarily for defensive purposes or for intelligence collection against foreign governments and businesses. However, if North Korean hackers are able to stealthily penetrate or exploit computer networks in order to acquire secrets, they could as well use their skills to damage or disrupt these networks.

North Korea faces several obstacles to developing and deploying an advanced CNO capability. Its highly restricted Internet connectivity and unreliable and antiquated electrical infrastructure could interfere with the conduct of attacks, especially sustained attacks. Trade restrictions make it difficult for the country to acquire the latest hardware and software platforms, which in turn

hampers its ability to develop and test attacks against these systems. Restrictions on Internet access would make it hard for North Korea to acquire hacking tools and information from the Internet, and to use or build on the work of tens of thousands of others in the world. Because much of the North Korea's IT research and development effort is in areas unrelated to CNO, the country's own academic and public communities would have little to offer in the way of CNO expertise. Internet restrictions would also preclude North Korean youth from getting involved in the Internet hacking scene and building up knowledge and skills that could later be channeled into government-sponsored activity. CNO agents would have to be trained from scratch.

While these hurdles do not imply that North Korea could not develop a powerful CNO capability, they suggest that a certain amount of skepticism may be appropriate when assessing claims about the effectiveness of that capability.

CONCLUSIONS

Our study concluded that both Iran and North Korea have a CNO capability. However, whereas the capability we identified for Iran lies within its academic and research communities and the general population, North Korea's lies mainly within its military.

We did not find evidence that either country had a highly sophisticated capability that would even come close to matching that in many other countries, including Australia, China, Russia, the United Kingdom, and the United States. Both countries, but especially North Korea, operate at a disadvantage because of trade restrictions prohibiting exports of advanced Western technologies to them. North Korea's disadvantage is compounded by its extreme isolation, not just from the Internet but from most of the world. Iran is plugged into the Internet and the international business, security, and hacking communities and thus can better leverage technologies and knowledge developed outside its borders. Moreover, the Iranian government can build on the knowledge and skills of its own population as participants in these international communities. North Korea is confined to whatever CNO capability it can develop in-house, behind government doors.

There are several limitations to our study. First, and perhaps most important, it is difficult and risky to draw conclusions based on a lack of evidence. It could be that both countries have highly advanced CNO capabilities, and that we just did not look hard enough or in the right places. As noted earlier, we did not have access to government officials in either country, and we did not use classified information from our own intelligence services, which no doubt limited what we could learn, especially about military capabilities. Our limited resources — we could not conduct every possible Internet and library search, follow every link, and translate every foreign website and document — also limited our data collection.

Another limitation is that our assessment is mainly qualitative. We attempted to measure a few factors, including the number of security researchers and hackers in a country, the percentage of

the population with Internet access, and the size of the security industry, but we did not formulate specific metrics that would allow one to rate a country's CNO capability on, say, a scale from 0 to 10. That said, I might rate Iran at 2 or 3 and North Korea at 1. I would rate Iran higher if we had evidence of a strong CNO capability within its military.

A third limitation is that our research and assessments were inherently subjective, biased by our own preferences and beliefs. These included beliefs that it would be difficult to develop a strong CNO capability in isolation and that a CNO capability within a country's population could be leveraged by a government to develop or strengthen its own.

These limitations present an opportunity for future research. Currently, however, we have shifted our focus to the terrorist threat. We have developed a methodology to assess the CNO threat of terrorists, in the process applying it to al-Qa'ida and the global jihadists.

NOTES

---

[1] D.E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," chapter 8 in J. Arquilla and D. Ronfeldt (eds.), *Networks and Netwars*, Santa Monica: RAND, 2001, pp. 276–277.

[2] D.E. Denning, "Information Technology and Security," chapter 4 in M.E. Brown (ed.), *Grave New World*, Washington, DC: Georgetown University Press, 2003, p. 98.

[3] J.P. Patterson and M.N. Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran," master's thesis, Naval Postgraduate School, September 2005.

[4] C. Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea," master's thesis, Naval Postgraduate School, September 2004.

[5] The definitions here are based on Field Manual (FM) 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, US Army, November 2003. They are consistent with revisions to the Joint Doctrine for Information Operations, Joint Pub (JP) 3-13, Joint Chiefs of Staff.

[6] C. Billo and W. Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*, ISTS, November 2004, http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf (accessed 26 April 2006).

[7] The website for the contest is at http://icpc.baylor.edu/icpc/ (accessed 26 April 2006).

[8] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Information technology statistics for 2004, International Telecommunications Union, http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet04.pdf (accessed 13 October 2005).

[14] Internet World Stats, http://www.internetworldstats.com/stats5.htm (accessed 13 April 2006).

[15] Internet Filtering in Iran in 2004–2005, OpenNet Initiative, http://www.opennetinitiative.net/studies/iran/ONI_Country_Study_Iran.pdf (accessed 13 October 2005).

[16] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[17] Website of Sharif Secure Ware, http://www.amnafzar.com/ (accessed 17 October 2005).

[18] "Leading Iranian Software Company System Group Made Exclusive Contract with Securepoint Security Solutions," 19 July 2005, http://www.securepoint.cc/press_partnership_iran.html (accessed 17 October 2005).

[19] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[20] ACM programming contest rankings for 2005, http://icpc.baylor.edu/past/icpc2005/finals/Standings.html (accessed 14 October 2005).

[21] Twenty-ninth ACM International Collegiate Programming Contest, 6th Asian Regional Contest in Iran, http://sharif.ir/~acmicpc/acmicpc04/index.html (accessed 14 October 2005).

[22] ACM programming contest rankings for 2006, http://icpc.baylor.edu/icpc/Finals/default.htm (accessed 26 April 2006).

[23] Website of S. Bakhtiari, http://sharif.ir/~shahram/ (accessed 14 October 2005).

[24] Website of M. Azgomi, http://mehr.sharif.edu/~azgomi/ (accessed 14 October 2005).

[25] Website of H. Habibi, http://ce.sharif.edu/~hhabibi/ (accessed 14 October 2005).

[26] Resume of S. Etemad, http://www.egr.msu.edu/~etemadys/Resume.pdf (accessed 14 October 2005).

[27] Research website of Sharif University of Technology, http://www.sharif.ir/en/research/ (accessed 2 November 2005).

[28] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[29] Website of M. Fallah, http://ce.aut.ac.ir/~fallah/ (accessed 14 October 2005).

[30] Website of A. Baraani-Dastjerdi, http://eng.ui.ac.ir/ahmadb/ (accessed 14 October 2005).

[31] Website of B. Ladani, http://eng.ui.ac.ir/ladani/ (accessed 14 October 2005).

[32] Website of Third Iranian Society of Cryptology Conference, http://iscc2005.org/iscc/index.php?sel_lang=english (accessed 14 October 2005).

[33] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Website of Pardis Technology Park, http://www.hitechpark.com/ (accessed 17 October 2005).

[40] Ibid.

[41] Bill Gertz, "Iran Militants in Power Stir Fears," *Washington Times*, 14 October 2005, http://www.washingtontimes.com/national/20051013-114716-3258r.htm (accessed 17 October 2005).

[42] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[43] Website of Iran Hackers Sabotage, www.ihsteam.com (accessed 18 October 2005).

[44] The statistics on web defacements were obtained 18 October 2005 from the Zone-H website at www.zone-h.org. The site also hosts mirrors of defacements.

[45] Zone-H mirror of web defacement, http://www.zone-h.org/en/defacements/mirror/id=2645159/ (accessed 20 October 2005).

[46] Zone-H mirror of web defacement, www.zone-h.org/en/defacements/mirror/id=2917409 (accessed 18 October 2005).

[47] Website of Ashiyane Digital Security Team, http://www.ashiyane.com/ (accessed 18 October 2005).

[48] Zone-H mirror of web defacement, http://www.zone-h.org/en/defacements/mirror/id=2757538/ (accessed 20 October 2005).

[49] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[50] Website of Defcon Groups, http://www.defcon.org/html/defcon-groups/dc-groups-index.html (accessed 15 October 2005 and 26 April 2006).

[51] Patterson and Smith, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran."

[52] Ibid.

[53] Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea."

[54] The Central Intelligence Agency, The World Factbook, North Korea, http://www.odci.gov/cia/publications/factbook/geos/kn.html (accessed 20 October 2005).

[55] Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea."

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] "'PC Café' attracts Youth in Pyongyang," December 2004, http://www.vuw.ac.nz/~caplabtb/dprk/NK_S&T.htm (accessed 21 October 2005).

[61] Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea."

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] Ibid.

[67] S.T. Song et al., "Bilateral Research Collaboration Between Kim Chaek University of Technology (DPRK) and Syracuse University (US) in the Area of Integrated Information

Technology," Prepared for the Asian Studies on the Pacific Coast (ASPAC) 2003 Annual Meeting, Honolulu, Hawaii, http://www.koreasociety.org/FYI/20030630-ASPAC-Kim-Chaek-Syracuse-rv.pdf (accessed 21 October 2005); "Project Status Report: July 2004 on The KUT/SU Research Collaboration," Nautilus Institute, DPRK Briefing Book, http://www.nautilus.org/DPRKBriefingBook/economy/30-KoreaSociety.html (accessed 21 October 2005).

[68] Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea."

[69] Ibid.

[70] J. Larkin, "North Korea Preparing for Cyberwar," *Far Eastern Economic Review*, 25 October 2001, http://archive.infopeace.de/msg00464.html (accessed 24 October 2005).

[71] Brown, "Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea."

[72] Ibid.

[73] "North Korea Suspected of Training Hackers," Associated Press, June 2003, http://smh.com.au/articles/2003/06/10/1055010959349.html (accessed 24 October 2005).

[74] "North Korean Military Hackers Unleash 'Cyber-terror' on South Korean Computers," AFP, 27 May 2004, http://www.freerepublic.com/focus/f-news/1143440/posts (accessed 24 October 2005).

[75] "North Korea's Cyber Guerrillas Called CIA-Class Threat to US Pacific Command," East-Asia-Intel.com, 7 June 2005.

[76] Brown, “Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea.”

[77] Ibid.

[78] “North Korean Military Hackers Unleash ‘Cyber-terror’ on South Korean Computers,” AFP, 27 May 2004, http://www.freerepublic.com/focus/f-news/1143440/posts (accessed 24 October 2005).

[79] Brown, “Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea.”