CYBER WARFARE

AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
AT DARTMOUTH COLLEGE

November 2004
Revised December 2004

Charles Billo
Welton Chang
45 Lyme Road
Hanover, NH 03755
603-646-0700

Authors of this report:

Charles G. Billo
Senior Research Associate, ISTS

Welton Chang
Research Intern, ISTS

ACKNOWLEDGEMENTS

We are grateful for the numerous comments received from our anonymous reviewers as well as ISTS reviewers. In particular, the substantive suggestions received from Professor David Kotz, Eric Goetz, and Colleen Hurd, were especially helpful.

We would like to thank Sarah Brooks and Jocelyn Troy for their help. We would also like to thank George Bakos, Kathleen Cassedy, Amy Gannon, Robert Hillery, Dennis McGrath, and the Technical Analysis Group at ISTS.

DISCLAIMERS

All Internet links and citations contained within were active at the time of publication. We cannot guarantee that the links will remain active indefinitely, although an effort was made to ensure that each citation contained enough information for the cited source to be located in print or other forms of media.

Information available prior to November 1, 2004 was used in this report.

 This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S.Department of Homeland Security.

FOREWORD

This study, written in response to a grant provided by the Department of Homeland Security, assesses potential foreign computer threats to information technology networks in the United States. In focusing on overseas cyber threat capabilities, one of the thrusts of this study is to dispel popular myths and anecdotal understanding about the nature and degree of the cyber threat—taking into account public and private digital network vulnerabilities. Our goal is to examine the open source evidence to develop a rigorous and dispassionate assessment of both cyber "offense" by selected nation states and the likely impact of an attack through the wires on the United States.

Cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks. These individuals often operate under the auspices and possibly the support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner.

A key premise of the present report is that information processing—whether by equipment (computers) or by humans— is becoming a "center of gravity" in future warfare. Nation-states, including the United States, reconnoiter and probe to identify exploitable digital network weaknesses among potential adversaries. Our immediate goal is to both imagine and define how foreign cyber attack capabilities might threaten information networks in the United States and what potential effects they might have. The discussion focuses on relatively arcane, non-sensational concepts and terms such as packet-switched networks, grid topologies, bandwidth, reconnaissance, asymmetric doctrine, and convergence.

The *Institute for Security Technology Studies* at Dartmouth College is concerned, in part, with securing computer systems against intrusion and building secure trust relationships among networked computing devices. It is our hope that by making the findings in the present study accessible to the general reader, we will illuminate current issues, foster practical discussions, and stimulate appropriate policy solutions to the challenges identified.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this report is to provide a realistic assessment of the capabilities, means, and motivations of selected nation-states to conduct a remote, computer-to-computer attack either against the United States or against regional adversaries. We take as a given that there is no such thing as "perfect" IT security. For example, hackers seem always able to keep one step ahead of the latest software security patch, and some secure portions of the U.S. Department of Defense computer systems (pertaining to procurement and logistics) are connected to the public-switched network. The consequences of an attack "through the wires," and the degree of potential disruption, will often hinge on the pervasiveness (and therefore importance) of the network impaired by the attack: national versus regional, local, or municipal in scope.

Relying exclusively on open source information, our task is to assess the relative capabilities of certain countries identified in the literature (China, India, Iran, North Korea, Pakistan, and Russia) to wage an effective cyber attack against an adversary. The words "effective cyber attack" by no means translate into the proverbial "take down" of the Internet; on the contrary, such attacks might involve intrusions into unprotected networks for the purpose of compromising data tables, degrading communications, interrupting commerce, or impairing critical infrastructures (such as transportation or medical and emergency services) in such a way that trust is undermined at the expense of a smoothly running economy and society.

While the degree of damage that could be caused in a cyber attack bears no resemblance to an electronic "Pearl Harbor," inflicting significant economic costs on the public and private sectors and impairing performance of key infrastructures (via IT networks linked to embedded computer systems, for example) seem both plausible and realistic.

Most computers are connected to each other in some way. They usually share the same operating system software and communicate with all other computers using the standard set of TCP/IP protocols. The ease and speed of dispersion of recently devised worms and viruses such as Nimda and Sasser underscores the links among networked computers.

The country-by-country analysis in this report rests on a uniform methodology. Our first category of evidence addresses specific links to cyber warfare capability as depicted in published U.S. government reports and foreign official doctrinal statements. Our second category of evidence concerns links of a more circumstantial nature, such as the presence of a robust information technology infrastructure useful in supporting nation state cyber warfare operations. A synopsis of our individual country studies follows:

<u>China</u>

Within the framework of an integrated national plan, the People's Liberation Army (PLA) has formulated an official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises. Beijing's intelligence services continue to collect science and technology information to support the government's goals, while Chinese industry gives priority to domestically manufactured products to meet its technology

needs. The PLA maintains close ties with its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare.

India

Cyber attacks pose more than a theoretical challenge to the Indian government's day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi's nuclear weapons test and in the confrontation with Pakistan over Kashmir. The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations. An IT roadmap, enumerating a comprehensive ten year plan, was published. In the framework of the roadmap, the government has granted permission for closer government/industry cooperation to leverage the output of India's world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established. According to journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies.

Iran

U.S. national security experts have included Iran on a published list of countries said to be training elements of the population in cyber warfare. The leadership in Tehran is known to sponsor terrorist groups and for many years has chafed in the face of perceived Iranian inadequacy in the conduct of modern information warfare. Although the rhetoric of the clerical regime has been more prudent in recent years (at least until recently), the government nevertheless continues to accord economic and political priority to extending the technological threshold of its defense sector. This is illustrated in two ways: first, the armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India. Overall, we assess that Iran is leveraging its resources in the non-conventional weapons and IT sector as a "force multiplier" to gain greater influence in Central Asia.

North Korea

Although U.S. national security officials include North Korea on a published list of countries believed to be developing information warfare units either in the military or the intelligence services, the open literature contains no North Korean military doctrinal or policy statement to that effect. South Korea's defense community alleges cyber reconnaissance or network hacks sponsored by Pyongyang, but such charges may only represent "disinformation." Due to the closed, Stalinist make-up of the North Korean regime and society, concrete evidence is difficult to obtain. There are few credible first-hand sources. We believe it is *possible* North Korea is experimenting with offensive cyber attack capabilities, based on Pyongyang's track record of priority resource allocations to the military, its evident endowment of scientists and engineers, and its documented achievements in missile and related military technologies.

Pakistan

Well-documented hacker activity in Pakistan and possible ties between the hacker community and Pakistani intelligence services indicate that Pakistan appears to possess a cyber attack capability. However, the published evidence is lacking concerning the exact nature of the capability; it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program. The available evidence suggests that the main target of Pakistan's offensive capability is India—Islamabad's rival on the sub-Continent and adversary in the Kashmir dispute. Pakistan's developed IT industry, well-educated computer programmers, and supportive government that is concerned with security in Kashmir and parity with India provides circumstantial evidence suggesting a cyber warfare program.

Russia

Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. Moscow also has a track record of offensive hacking into Chechen websites. Although we assess it likely that Moscow will continue to scout U.S. military and private sector networks and websites, available evidence is inadequate to predict whether Russia's intelligence services or armed forces would attack U.S. networks, especially after taking into account present-day political and economic ties between the two nations.

Findings

The conventional wisdom holds that the Internet backbone is resilient because of back-ups and redundancies. The track record so far suggests that engineering "work-arounds" in response to router problems are achievable using alternative nodes; however, the Internet today may not be as resilient as some experts believe because of the free market progression toward central network hubs that present a potentially lucrative target for hackers. One of the corollaries of this trend is increasing *convergence* in industrial countries such as the United States of IT, telecommunications, and links to embedded computer systems employed to control physical infrastructure. The degree of convergence has accelerated markedly in the past five to ten years. IT security experts at local and national levels are often unsure of the interconnections. On top of this, our adversaries no doubt are becoming more and more proficient in harnessing and improving hacking skills intended to identify flaws and loopholes in network and software security.

IT dependence in the United States is evolving into a strategic center of gravity. This represents an inviting target to a potential adversary. While intrusions and hacks are not the exclusive province of large, hierarchical organizations, military and intelligence services possess an advantage over terrorist units for example in terms of resources, depth of personnel, and longer time-horizon reconnaissance and probes.

Moreover, as advanced industrial states such as the United States outsource their programming of software to countries such as India, Pakistan, China, Philippines, and Russia, the risk of rogue programmers using their access to commit cyber attacks rises. The possibility of abuse by hackers, organized crime agents, and cyber terrorists in countries not necessarily allied with the United States is great, and grows as more programming is sub-contracted to these countries for economic reasons.

We believe that scientific and engineering prowess in the United States and elsewhere, when properly harnessed and directed, can lead to improved security measures and better defenses (such as attack "indications and warnings") against malicious intrusions. Technology, however, is no panacea.

In conclusion, we recommend improved vigilance on the part of our homeland defense authorities against ever more sophisticated and numerous cyber attacks and probes. Given the significant economic and other interests at stake, we recommend a more systematic and sustained effort to raise awareness at the grass roots level regarding security loopholes and vulnerabilities. These efforts, led by local and national political leaders and responsible officials in the United States, will be important in changing the way the populace currently views network security. Finally, we propose greater urgency be given to the recommendation in the U.S. *National Strategy to Secure Cyberspace* calling for an effective public/private partnership to develop realistic software security and related standards that manufacturers will accept.

I. INTRODUCTION AND STUDY METHODOLOGY

We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks.

John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000.[1]

Foreign governments pose a serious and structured threat because they not only have access to the appropriate technology, but also are able to enhance the effectiveness of this technology through the use of the all source intelligence support, extensive funding, and organized professional support. In addition, government agencies may be able to conduct more extensive programs because of their willingness to invest in longer term goals and objectives.

The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications, Office of the Manager, National Communications System, December 2000, p. ES-2.

While we have not seen such attacks from a nation state, that is solely because no state or non-nation state actor has yet seen sufficient strategic advantage to be gained by doing so, and this condition will not last indefinitely.

Dr. Daniel T. Kuehl, National Defense University, before the Joint Economic Committee, U.S. Congress, February 23, 2000

1.1 THE ARGUMENT

Critical infrastructure protection became a veritable watchword in local and national security policy circles, even before the 9/11 terrorist attack and the establishment of the Department of Homeland Security. The success of the 9/11 conspiracy has been attributed in part to a "failure of imagination" on the part of the U.S. defense and intelligence community. This, in turn, has spawned reactive, "worst case" predictions, along the lines that, "the attack the experts say cannot happen or that terrorists are not interested in pursuing is simply an attack that hasn't happened yet."[2]

Seasoned observers, such as military analyst Anthony H. Cordesman writing on cyber warfare and related matters, point out the need for calm reflection and accurate calibration of the problem before allocating scarce tax dollars to critical infrastructure protection. With respect to cyber warfare, Cordesman observed in December 2000:

"There is a flood of uncertain and poorly defined data on the threat, much of which is highly anecdotal. Incidents tend to be exaggerated while the overall pattern in the threat may be understated or missed altogether. Cost and risk estimates are issued that are little more than guesstimates, often using ridiculous methods and data. There is a critical lack of technological net assessment of the trends in offense and defense…"[3]

---

[1] Congressional testimony of John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>

[2] Dan Verton, "Introduction," *Black Ice: The Invisible Threat of Cyber-Terrorism*, (McGraw-Hill/Osborne 2003), p. xxii

[3] Anthony H. Cordesman, "Homeland Defense: Information Warfare," Center for Strategic and International Studies, December 2000, pp. 185-186

Among the recommendations that Cordesman offers for consideration is the suggestion that the U.S. should identify and assess its "real vulnerabilities" and avoid extending the federal role in critical infrastructure protection at random—an effort that may only create false and inappropriate priorities.

The purpose of this report is to provide a frank and dispassionate assessment of the degree of vulnerability of information technology networks in the United States to "through the wires" attacks by selected foreign nation-states. Although our research has inherent limitations (for example we rely exclusively on published sources), we trust that publication of our findings will serve as a primer on cyber warfare matters, accessible to expert and nonprofessional alike. We address both external threats and internal U.S. vulnerabilities. Our goal is to pierce some of the myths and exaggerations related to cyber warfare. In our concluding chapter, we couple our assessment with recommendations to local and national policy makers.

Figure 1: Diagnosis of the Problem: The "Experts" Differ

Some experts maintain that cyber attacks with potential strategic national security effects, often referred to as an "electronic Pearl Harbor," are impossible. Others proclaim they are inevitable. Contemporary predictions on these matters run from the benign to the apocalyptic.

Experts toward the benign end of the spectrum often cite the robustness, resiliency, and redundancy of the Internet as inherent characteristics of a system that would prevent a cyber attack from producing catastrophic results.[4] James Lewis of the Center for Strategic and International Studies (CSIS), for example, argues that:

"Some people actually believe that this stuff here that they're playing with is equal, if not a bigger threat, than a dirty bomb… Nobody argues -- or at least no sane person argues -- that a cyber attack could lead to mass casualties. It's not in any way comparable to weapons of mass destruction. In fact, what a lot of people call them is 'weapons of mass annoyance.' If your power goes out for a couple hours, if somebody draws a mustache on Attorney General Ashcroft's face on his Web site, it's annoying. It's irritating. But it's not a weapon of mass destruction. The same is true for this." [5]

On the other hand, experts with access to classified sources point out that the growing tendency in advanced industrial economies to link internal business management tools and administrative

[4] See Scott Berinato, *CIO Magazine*, "Debunking the Threat to Water Utilities," March 15, 2002 <http://www.cio.com/archive/031502/truth_sidebar2.html>;
Chris Conrath, *Computerworld Magazine*, "Q&A: Security expert says cyberterrorism is exaggerated," October 2, 2002 <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,74791,00.html>;
Rob Rosenberger, "Computer Virus Command and Control," vmyths.com, August 15, 2002 <http://vmyths.com/rant.cfm?id=504&page=4>;
William Jackson, "Cyber Eye: A digital Pearl Harbor might not be so easy," *Government Computer News*, July 1, 2004 <http://www.gcn.com/21_29/tech-report/20047-1.html>; and
Marcus Ranum, "Myths of Cyberwar," *Information Security*, April 2004, p. 22

[5] James Lewis, Center for Strategic and International Studies, Interview for *PBS Frontline: Cyber War!*, February 18, 2003

controls to the Internet could be catastrophic for overall U.S. security. Former White House Cyber Security advisor, Richard Clarke, for example, observes:

"We, as a country, have put all of our eggs in one basket. The reason that we're successfully dominating the world economically and militarily is because of systems that we have designed, and rely upon, which are cyber-based. It's our Achilles heel. It's an overused phrase, but it's absolutely true. It could be that, in the future, people will look back on the American empire, the economic empire and the military empire, and say, "They didn't realize that they were building their whole empire on a fragile base. They had changed that base from brick and mortar to bits and bytes, and they never fortified it. Therefore, some enemy some day was able to come around and knock the whole empire over."[6]

A third set of observers maintains that the truth lies somewhere in between, and that it is best to be vigilant. They argue for a new way of approaching electronic defenses. One of the main proponents of this middle course is Bruce Berkowitz. In 1995, he wrote that cyber attacks could degrade both civilian and military networks. He emphasized the importance of mounting an information warfare "civil defense" because:

"Civilian information systems are prime candidates for attack…Just as cities are targeted in strategic bombing, in future wars we can expect civilian information systems to be hacked, tapped, penetrated, bugged, and infected with computer viruses." [7]

In 1996, a RAND research group observed that:

"Civilian data encryption and system protection are rudimentary. Talented computer hackers in distant countries may be able to gain access to large portions of the information infrastructure underlying both U.S. economic well-being and defense logistics and communications." [8]

Moreover, in 2001, a CSIS conference of Homeland Security experts concluded:

"We've known for at least a decade that the country's critical infrastructure depends on computer systems and information networks that are subject to debilitating cyberattacks. But until now, network attacks have been more burdensome than anything, and costly for only a handful."[9]

1.2 BACKGROUND

There exists the possibility that foreign nation-states—not only the U.S.—could mount and finance a well-organized cyber warfare program. This would allow them to utilize a cyber attack capability against an adversary. A multi-faceted cyber attack employing various techniques could be highly disruptive if the United States and its allies were unprepared for it. A cyber attack by nation-states targeting the transportation, communications, or banking sector computer systems in the United States would, at a minimum, entail significant economic costs that would affect

[6] Richard Clarke, former White House cyber security advisor, Interview for *PBS Frontline: Cyber War!*, March 18, 2003 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html>

[7] Bruce Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995, pp. 59-66

[8] RAND Research Brief, "Strategic War in Cyber Space," January 1996 <http://www.rand.org/purblications/RB/RB7106/RB7106.html>

[9] Kristen Batch, Joelle Laszlo, Erin Schlather, "Conference Summary: Strengthening Homeland Cyber Defense," Center for Strategic and International Studies, October 18, 2001, p. 6 <http://www.csis.org/tech/events/011018event/011018confsumm.pdf>

jobs and growth. Cyber attacks could also indirectly lead to disruptions in daily civilian life that go beyond the level of temporary nuisance to inflict sustained uncertainty, confusion, and even chaos across significant elements of the population.[10] In the most extreme of cases, these disruptions could cause human casualties.

Cyber attacks occur on a frequent basis and in a near-instantaneous manner; as the world becomes more connected, more machines and more people will be affected by an attack. In the months and years to come, cyber attack techniques will evolve even further, exposing various—and possibly critical—vulnerabilities that have not yet been identified by computer security experts. Moreover, such attacks could also be coordinated to coincide with physical assaults, in order to maximize the impact of both.

Figure 2: Snapshot of Recent Developments

During the past five years, the world has witnessed an escalation in the number of cyber attacks involving hackers attacking and counterattacking in the context of regional or local disputes.[11] When peacekeeping operations began in Kosovo, NATO and Serbian hackers attacked back and forth attempting to control each other's electronic resources.[12] The same has occurred during the Palestinian-Israeli conflict,[13] the India-Pakistan disagreement over Kashmir,[14] and between Chinese and American hackers during the accidental bombing of the Chinese Embassy in Belgrade in 1999 and the May 2001 downed spy-plane incident.[15] A cyber war between Chechen and Russian hackers has also taken place during the conflict between the Russian military and Chechen fighters.[16] These cyber wars coincided with actual physical conflicts but intrusions, in one form or another, also have taken place in isolation.

In recent years, the scope and sophistication of cyber attacks have also expanded. Whereas antecedent attacks were relatively benign, more recent intrusions have compromised vital communications and critical infrastructure systems, such as public utilities connected to the Net. The Slammer worm, for example, exploited a vulnerability in Microsoft's SQL database

[10] See CNN's account of the Slammer worm's affects on banks and airlines systems, CNN, "Computer Worm Grounds Flights, Blocks ATMs," January 25, 2003 <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/index.html>

[11] Cyber attack is defined as a computer-to-computer or computer-to-network electronic attack taken in an offensive or defensive manner with the intent of harming the target's operability. A discussion of this is undertaken later in the introductory chapter, as well as in Appendix B

[12] Anthony H. Cordesman, "Critical Infrastructure Protection and Information Warfare," Center for Strategic and International Studies, *Defending America: Redefining the Conceptual Borders of Homeland Defense* December 8, 2003

[13] Patrick D. Allen and Chris C. Demchak, "The Palestinian-Israel: Cyberwar," *Military Review*, March/April 2003

[14] Stanley Theodore, "Pro-Pakistan hackers deface Centre's venture capital site," *Statesman News Service*, August 24, 2001

[15] CNN, "Hackers Attack U.S. government Web sites in protest of Chinese embassy bombing," May 10, 1999 <http://www1.cnn.com/TECH/computing/9905/10/hack.attack/> and BBC, "Truce in US-China hacking war," May 10, 2001 <http://news.bbc.co.uk/1/hi/world/asia-pacific/1322839.stm>

[16] Lieutenant Colonel (ret.) Timothy L. Thomas, "Manipulating The Mass Consciousness: Russian And Chechen "Information War" Tactics In The 2nd Chechen-Russian Conflict," Foreign Military Studies Office, 2000 <http://fmso.leavenworth.army.mil/fmsopubs/issues/chechiw.htm>

software that led to cascading effects in our electronic infrastructure that were certainly not predicted beforehand.[17] Airline booking systems and bank Automated Teller Machines (ATMs) were among other systems impacted by Slammer infections. The Slammer worm also significantly degraded computer systems that control monitoring capabilities at the Davis-Besse nuclear power plant in Ohio.

As of this writing, the Department of Homeland Security (DHS) is dedicating significant resources to detecting, protecting against, and responding to cyber attacks.[18] Most recently, the NCSD announced the creation of a national cyber alert system aimed at "home users and technical experts in businesses and government agencies." In the view of Department of Homeland Security officials, the danger of cyber attacks requires that immediate action be taken to protect the networks critical to our function as a society.[19] However, these actions may not be enough to change a culture of lax cyber security standards, an apathetic attitude possessed by computer expert and novice alike.

1.3 ROOT OF THE PROBLEM

Most networks and therefore most computers are connected to each other in some way, be it sharing the same access provider, central server, or accessing the same set of computers. This connectivity is rapidly increasing because of the free market development of central network hubs, a point that is discussed later in the chapter. Although a completely accurate map of the overall Net has not been produced, it is logical to reason that the 95% of privately owned networks are connected to each other in some way.[20] Indeed most computers share the same operating system software and communicate with all other computers using the standard set of TCP/IP protocols.[21] The interoperability benefits of standardized protocols and the spread of recently devised worms and viruses such as Nimda and Sasser are testament to the links between these networks.

At the beginning of the transformation of society in the mid-1990s through the introduction of applications connected by networks and the Internet, profit-oriented, entrepreneurial programmers focused on creating massively used network-based utilities. These network-based

[17] See the advisory for the worm from CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, April 2003 <http://www.cert.org/advisories/CA-2003-04.html>; Wired magazine's analysis of the automated exploit can be found here: <http://www.wired.com/wired/archive/11.07/slammer_pr.html>; and Security Focus's discussion of the problem at the Davis-Besse nuclear power plant available at <http://www.securityfocus.com/news/6767>

[18] According to the Department of Homeland Security's requested 2005 budget, $79.8 million was earmarked for the new National Cyber Security Division (NCSD). See "DHS Announces FY 2005 Budget," February 2, 2004 <http://www.whitehouse.gov/news/releases/2004/02/20040202-7.html>

[19] See US Computer Emergency Response Team Press Release site for the latest releases on NCSD related news <http://www.us-cert.gov/press_room/>

[20] Because of the vast nature of the Internet, an instantaneous map that accurately represents the entire network in real-time has not been produced. See Hal Burch, Bruce Cheswick, "Internet Mapping Project," Lumeta Corporation, 1999 <http://research.lumeta.com/ches/map/> and The Opte Project, "Maps," 2004 <http://www.opte.org/maps/>

[21] TCP and IP are protocols for sending digital information (in the form of "packets") and verifying that it has been sent and received. For a discussion of TCP/IP see: H. Gilbert, "Introduction to TCP/IP," Yale University, February 2, 1995 <http://www.yale.edu/pclt/COMM/TCPIP.HTM>

utilities, such as search engines (significantly reducing information costs), automated clearing house transactions seamlessly linking consumers with financial institutions (increasing efficiency and accuracy of transactions), and near instantaneous communications capabilities (voice over internet protocol or VoIP, instant messaging, e-mail) have become the applications that many in business and daily-life take for granted. Some of these utilities run on the Internet backbone; others run on private networks with links to other networks through the Internet. The quest in the United States for economic efficiency (i.e., through reduction in the cost of information acquisition) has produced an almost unparalleled state of dependency. Our adversaries no doubt have already observed this dependency.[22]

The pervasiveness of IT networks in the United States is rapidly evolving into what military writers call a strategic center of gravity, especially because of the myriad, often unaccounted for, links to the electric power grid and other elements of the critical infrastructure.[23] As CIA analyst John Serabian testified in early 2000, "We have spent years building an information infrastructure that is interoperable, easy to access, and easy to use. Attributes like openness and ease of connectivity which promote efficiency and expeditious customer service are the same ones that now make the system vulnerable to attacks against automated information systems."[24]

As with any new technological advance, inventors and consumers in the computer and IT sectors seek to optimize the cost-reducing effects of technology. In the rush to maximize economic efficiency, safety and security concerns are often set aside and have only recently been noticed by people from software engineers to the home computer user.[25]

Figure 3: Trust is critical to the effective use of remote technologies

American institutions, government, media, military, and other organizations rely in large measure on trust in both the utilities that allow them to function as well as the integrity of the information residing in databases. Integrity in the market place formerly was centered on people-to-people handshakes. Today computer-to-computer handshakes often take precedence.

[22] As Jonathan Tucker writes: "As the most computerized country in the world, the United States relies on a vast number of networked processors and databanks for the operation of its critical infrastructure—the system of interdependent industries and institutions that provide a continual flow of goods and services essential to the nation's security and welfare." Jonathan Tucker, "Asymmetric Warfare," *Forum for Applied Research and Public Policy*, 1999

[23] Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *National Strategy for Homeland Security,* July 2002 <http://www.whitehouse.gov/homeland/book/>

[24] Congressional testimony of John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>.

[25] The world prior to the Information Age– hard copy documents, pain-staking hours-long library research without electronic databases, manual archive retrieval in every office– is now hard to imagine as ever having existed. Today we are invisibly reliant on always-on and seemingly autonomous electronic communication systems in almost all aspects of our daily life.

Information technologies pervade daily life, with much of today's medical and scientific community and financial markets relying on electronic databases and communications, without which neither could function. The electronic news media, broadcasting in its 24-hour format and worldwide scope, also could not perform in the absence of networked technology and computer-aided dissemination.

Compromising the electronic systems, even today when the technological revolution is in its infancy, would cause a significant drop in the confidence in these systems. As Stephen E. Flynn, a senior fellow at the Council of Foreign Relations points out, "the main benefit of attacks on critical infrastructure is not the immediate damage they inflict, but the collateral consequences of eroding the public's trust in services on which it depends."[26] Even after a cyber attack is halted or discontinued, the issue of data corruption, sorting out what information remains reliable and what has been irreparably harmed is an issue that insidiously undermines trust.[27]

1.3.1 Cyber warfare defined

In our research, we found that experts employ diverse definitions of cyber warfare, depending on the weight or emphasis accorded to various actions, actors, and intent. We attempted to minimize the all-encompassing and academically confusing expression "information warfare" to describe electronic attacks. In this document, we also eschew other terms, such as information operations, electronic warfare, "hacktivism", information disruption, or cyber terrorism. In each of these terms there exists a common link to cyber activities, yet each term is different enough to not entirely capture or mostly miss the definition of cyber warfare.[28]

As stated at the outset, cyber warfare, involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. In the future, if not already common practice, individual cyber warfare units will likely execute through the wires attacks against targets in a cooperative and simultaneous manner. The overall intent is to seek advantage over an adversary by compromising the integrity, confidentiality, or availability of a computing device.[29]

1.4 CRITICAL NETWORKS ARE TARGETS

The most likely targets of cyber warfare are critical networks.[30] Critical networks are those that if interrupted for significant portions of time (several days or several weeks or indefinitely) or perform erratically or intermittently (i.e., accessible only Tuesdays and Thursdays) would disrupt

[26] Stephen E. Flynn, "The Neglected Home Front," *Foreign Affairs*, September/October 2004

[27] On the issue of trusted recovery see Peng Liu, Shushii Jajodia, *Trusted Recovery and Defensive Information Warfare*, (Boston, Kluwer Academic, 2002)

[28] For a discussion on the evolution of cyber warfare terminology see Lieutenant Colonel (ret.) Timothy L. Thomas, "Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory," *Journal of Information Warfare*, February/March 2003 pp. 109-116

[29] For a more extensive treatment of cyber terminology questions, see Appendix B to this volume

[30] For a sector-by-sector discussion of vulnerabilities see earlier Dartmouth ISTS publications, including: Eric Goetz, *Survey and Analysis of Security Issues in the U.S. Banking and Finance Sector,* September 2003 and Eric Goetz, *On the Road to Transportation Security*, February 2003 <http://www.ists.dartmouth.edu/>

daily life. Networks can be large or small, and are often integrated with other architectures in a redundant chain. But there are those systems that do not have built-in redundancy and whose disruption would halt all activities associated with the network. For example, the news media disseminate information on the Internet. CNN's website is a popular news source, as is the *New York Times* electronic edition. However, if access to the Internet were suddenly disrupted for several weeks, consumers of these news sources would turn to alternatives such as print media and television. CNN's website could itself have a backup server, which would prevent a cyber attack from significantly limiting its customers' access to electronic news. Other networks, such as the 911 emergency system, medical information systems controlling sensitive data such as dosage requirements and patient records, and the automated-clearinghouse functions of major banks, the Federal Reserve, credit card companies and other financial institutions, would suffer from disruption or denial as well as disinformation. In July of 2000, Japanese cell phone users with Internet capability had their telephones hijacked by lines of code contained in e-mails directing their telephones to dial 110, the country's 911 network, tying up emergency lines.[31] According to FBI reports, a witness in a criminal case was nearly murdered when the criminal he was about to testify against broke into a hospital network and increased the dosage of his medication until it amounted to a lethal amount if administered.[32]

The information presented thus far underscores the dynamic growth, rapidly changing technologies, and simultaneous complexity and vulnerability assocated with the cyber warfare domain. In general, compromises at the national level that undermined popular confidence and day-to-day trust or resulted in damage to key national or multinational economic sectors would likely be more disruptive than local events. But the scope, direction, duration, and intent of observed attacks are hard to pinpoint. It is often difficult to disentangle the various threads of cause and effect. An adversary may employ digital laundering techniques to mask the source of the action, complicating traceability.

1.5 MOTIVATION: FOILING THE TARGET PROVIDES THE INCENTIVE

To recapitulate, the U.S. economy is becoming networked in a spiraling, complex fashion. This means that an adversary can obtain advantage by remotely accessing such networks through electronic means, compromising data integrity and undermining trust. In addition, according to security experts, trends in both dependency and connectivity overlap; convergence has made U.S. national information networks more vulnerable and therefore more attractive as targets of cyber attack. As retired Colonel Marvin Leibstone of the Computer Security and Technological Studies Project aptly puts it, "the more content there is on the Internet, and thus more valuable the contents, the more incentive there is to crack it to dominate it. And, thus, the need grows for additional protective layers and for organizations to work alongside one another."[33] And the U.S. National Intelligence Officer for Science and Technology observed in 2001:

[31] Michelle Delio, "Hello 911, I've Got a Virus," *Wired Magazine*, June 15, 2001 <http://www.wired.com/news/wireless/0,1382,44545,00.html>

[32] Valery A. Vasenin and Aleksei V. Galatenko, "Cyberterrorism," *High Impact Terrorism*, National Academy Press 2002, p.186

[33] FBIS Translation, Ud Gundar, "O-P-E-N," *Globes*, March 26, 1998. FTS 19980417001567

- The growing connectivity among secure and insecure networks creates new opportunities for unauthorized intrusions into sensitive proprietary computer systems within critical U.S. infrastructures such as the nation's telephone system.

- The complexity of computer networks is growing faster than the ability to understand and protect them by identifying critical nodes, verifying security, and monitoring activity.

- Firms are dedicating growing, but still insufficient, resources to the defense of U.S. infrastructures against foreign cyber attack—perceived as a low likelihood threat compared to routine disruptions such as accidental damage to telecommunications lines.[34]

Adversaries that cannot match U.S. conventional military strength have an incentive to employ asymmetric strategies to exploit our vulnerabilities. Different adversaries will have different goals in scouting our communications nodes and compromising our IT systems. Among these are: intelligence gathering, software theft, compromising systems or data integrity, and perception management.[35]

As CIA analyst John Serabian stated in Feburary 2000:

"There are any number of incentives to use cyber attacks, including economic, industrial, and military rationales. By way of example:

- Trillions of dollars in financial transactions and commerce move over a medium with minimal protection and only sporadic law enforcement—a structure the most complex the world has ever known.

- Increasing quantities of intellectual property reside on networked systems; and

- Opportunities abound to disrupt military effectiveness and public safety while maintaining the elements of surprise and anonymity."[36]

Years from now when historians look back upon the bridging years between the end of the 20th and beginning of 21st centuries, they will likely note the defining constructs of this time to be the socioeconomic phenomenon known as globalization and the evolution of the beginnings of the Information Age. One expert predicts that in the near future, in "as little as 3-5 years, the I&T sector [information and telecommunications] will host the complete convergence of telephone, data and video networks into a single, packet-based architecture – a unified next generation network (NGN)."[37] In the midst of the all-pervasive revolution in information processing, sharing, and communication, cyber warfare—the employment of computer-to-computer attack strategies constituting offensive and defensive operations—is no longer a leap of imagination or the work of science fiction authors.

---

[34] Lawrence A. Gershwin, Statement for the Record to the Joint Economic Committee, U.S. Congress, June 21, 2001 <http://www.fas.org/irp/congress/2001_hr/062101_gershwin.html>

[35] SANS Institute, "Security Essentials with CISSP and CBK," Volume I, 2003 p. 522

[36] John A. Serabian, Statement for the Record before the Joint Economic Committee, U.S. Congress, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>

[37] Eric Goetz, *Information and Telecommunications Sector Vulnerabilities and Threats*, Institute for Security Technology Studies, Dartmouth College, September 2002, p. 9

1.6 STUDY METHODOLOGY

As stated at the outset, this study is concerned with a realistic assessment of cyber attack capabilities of various nation-states, such as Russia, China, North Korea, and Iran. It rests on an interdisciplinary approach blending strategic, technological, and political analysis.

In compiling this primer on cyber attack capabilities and threats, our overall approach is to disaggregate complicated technical matters to assess the true nature of the challenge. Our goal is to avoid erecting policy prescriptions on a false or misleading foundation. We first define the issues involved in offensive cyber warfare. In the next section, the country studies, we evaluate the research and investments in the field of cyber warfare by selected nation-states. In the conclusion, we identify and characterize information network vulnerabilities in the United States. We derive findings and recommendations by comparing and balancing potential threat capabilities against broadly understood vulnerabilities.

1.6.1 Using open source literature

Building on previous research, and relying exclusively on open source data, we collected information on and analyzed the cyber attack capabilities, means, and motivations of several foreign countries. Our current assessment of the available open source evidence leads us to believe that several nation- states are developing such capabilities as part of an offensive cyber warfare program.

This is neither a deterministic piece nor a predictive piece on the course of action of cyber attack-capable nation-states. It also does not detail the possible events to follow a coordinated, deliberate cyber attack. Our approach is to define more systematically: 1) external nation-state capability and intent to engage the U.S. asymmetrically through these means; and 2) key factors that make the U.S. an especially inviting target. Our conclusions are also compared to known cyber events that have already taken place in the hope of leading the analysis to a more balanced result.

While some might question the validity of findings such as ours derived exclusively from open sources, we believe that our use of published materials bolsters our assessments. Assuming it is unlikely that classified information leaks into the open source arena, if such restricted information identifying and characterizing foreign cyber capabilities is generally on the mark, it would suggest a systematic bias in this report toward *understating* the threat.

1.6.2 Research and works consulted

During the formative stage of this investigation, a review was undertaken to identify relevant studies and reports. In addition to general works on cyber warfare issues by noted authorities,

our review identified several articles focusing on cyber developments in single countries. For example, retired Lieutenant Colonel (U.S. Army ret.) Timothy L. Thomas has written on cyber warfare developments China and Russia.[38] Other experts, such as Grey E. Burkhart, have researched Iran and India.[39] In the course of our investigation, we did not encounter any comprehensive reports analyzing the cyber warfare capabilities of several nation-states using an analytical framework similar to ours.

To assess the general nature of cyber warfare, we consulted several standard reference works such as Greg Rattray, *Strategic Warfare in Cyberspace* (2001); Dorothy E. Denning, *Information Warfare and Security* (1999); John Arquilla and David Ronfeldt, *Cyber war is Coming!* (1993); and Dan Verton, *Black Ice: The Invisible Threat of Cyber Terrorism* (2003). We also consulted several U.S. government publications (civilian and military), and specialized defense publications such as *Jane's Intelligence Review.*[40]

To develop a preliminary list of countries relevant to our proposed inquiry, we examined published Congressional testimony by government officials and academic experts; academic journals focusing on strategic warfare, non-conventional weapons, and national security issues; and publications of the U.S. Department of Defense.

To collect military and civilian IT-related information pertaining to the individual countries examined in this report, we reviewed foreign language resources, including selected government publications and websites, academic journals, and on-line news sites. We also relied heavily on standard media publications and "grey" source websites. The statistical data presented in this study is synthesized from a variety of sources including the CIA's *World Fact Book*.

1.6.3 Country selection

The research team accorded priority to nation-states previously identified in the review and other open sources as seeking to develop a cyber attack capability. The countries in this category are Russia, China, North Korea, and Iran. We then selected for study additional countries that did not appear consistently in all the assessments provided but for which we had identified some

[38] See, for example, Lieutenant Colonel (ret.) Timothy L. Thomas, "The Russian View of Information Warfare," Foreign Military Studies Office, Fort Leavenworth, Kansas, and "New Developments in Chinese Strategic Psychological Warfare," published in *Special Warfare,* April 2003

[39] See, for example, Grey E. Burkhart, "National Security and the Internet in the Persian Gulf Region," March 1998 <http://www.georgetown.edu/research/arabtech> and "The Internet in India: Better Times Ahead?," 1998 <http://portal.acm.org>

[40] Other works we referenced during our research included:
Stefan Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics," *Switch*, 1998;
John Arquilla and David Ronfeldt, "The Advent of Netwars (revisited)," *Networks and Netwars: the future of terror, crime, and militancy*, National Defense Research Institute, RAND, 2001;
Bruce Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995;
Jonathan Tucker, "Asymmetric Warfare," *Forum for Applied Research and Public Policy*, 1999;
Winn Schwartau, *Information Warfare*, (Thunders Mouth Press, New York), 1996;
Jerrold M. Post, Eric D. Shaw and Keven G. Ruby, "From Car Bombs to Logic Bombs: The Growing Threat from Information Systems Terrorism," *Terrorism and Political Science*, Vol. 12 No. 2, Summer 2000

interest in expert publications and professional social science journals. Two of the countries in this category are India and Pakistan, selected because of their intrinsic interest and reported propensity to use cyber attacks in regional disputes. Resource and time constraints did not permit addressing several additional nation-states of potential interest, such as Israel, Syria, and the former Yugoslavia.[41]

Table 1: Topic Areas for Cyber Warfare Capability

Government	Private Sector
Active cyber warfare units	Academia - developed educational system for computer science / engineering
Available cyber warfare doctrine	Accessibility of network to general public
Computer Emergency Response Teams	Computer security programs
Cyber crime prevention / investigation teams	Expatriate students studying in technologically advanced countries
Government-run academic institutions with cyber programs	Fiber optic cable/copper wiring
Government sponsored information technologies (IT) projects	Hackers - state-sponsored / condoned - political aims
Intelligence Service capabilities	Hardware production capabilities
Military Command and Control, Communications, Computers, and Intelligence (C4I) information warfare capability	High speed access
Military intelligence units	IT cooperation
Military units capabilities	IT infrastructure
Overall use of IT	IT security firms
State-to-state information technology initiatives	Number of ISPs and main nodes
	Number of satellite links
	Number of telephone lines
	Overall state and integration of information technologies
	Process control systems including SCADA systems
	Software development capabilities
	Transnational corporations active in the IT sector / using IT

1.6.4 Collection plan

In reviewing each country, the research team used the topic headings in Table 1 to structure the overall information collection. To acquire the necessary background, between October 2002 and September 2003 the team surveyed the extensive body of reports on the dependence of U.S. critical infrastructure on computer controls and the related vulnerability of the U.S. to cyber attack. Between September 2003 and September 2004, periodic updates and revisions to the country studies were performed as more incidents and data appeared in the open source realm. Building on this survey of expert reports, academic research, and engineering panel findings we then began research on the specific countries listed above. We collected data within the various topic areas in the above table.

[41] Other countries that we studied, for example, were: Cuba, Jordan, Syria, Libya, and Egypt. Iraq was also originally examined at the beginning of our research project. It has been suggested that if open source evidence is released as to the final condition of cyber warfare resources in Iraq, this evidence would be able to validate or invalidate our methodology. To date, no post-Gulf War II data on Iraq's cyber warfare capabilities has been made available to the public.

1.6.5 Analysis

Beyond the collection framework, our overall analytical approach towards development of cyber attack capability measurement was shaped by the work of Professor Dorothy E. Denning, among others. Professor Denning argues that cyber threats are a function of three factors: Intent; Capability; and Opportunity.[42] To simplify our work, we equated the well-publicized vulnerabilities in the U.S. electronic infrastructure with "opportunity." With regard to the intent, we assumed that any credible official documents or published statements by a foreign government or its military leaders concerning adoption of an offensive cyber warfare program (or doctrine) were sufficient to imply motivation to at least develop a cyber attack capability.

The ubiquity of computer and other information technologies plus the portability of knowledge enables sub-national elements, such as terrorist cells, to launch cyber attacks.[43] With respect to technical and institutional capabilities, nation-states—because of resource and other endowments—often possess the means to enhance the effectiveness of malicious intrusions. Cyber attacks, if applied on a massive scale by a nation-state intelligence service, for example, could yield important strategic effects. The broad spectrum of both possible attack sources and degrees of disruptiveness is addressed in the concluding chapter of this report. [44]

Many of the countries proved difficult to evaluate through open sources. Closed societies, such as the state of North Korea, present difficult problems for researchers. First, the amount of official information available is very limited. Second, sources from rival states such as South Korea that may give clues into North Korea's cyber capabilities are often unreliable due to bias among other factors. For example, the South Korean Central Intelligence Agency (KCIA) often publishes reports that contain factual errors to represent North Korea in a negative light. Lastly, translating foreign languages often results in subtle interpretational differences that may lead to differing analytical conclusions.

To recapitulate, the present report focuses on topic areas that may reveal a nation-state's means and motivations to launch cyber attacks. The following categorization of evidence specifies the topic areas and some detail on their indicators and related measurement criteria.

[42] Dorothy E. Denning, *Information Warfare and Security*, (Addison-Wesley, 1999) p. 12

[43] For a discussion of the range of potential actions in the cyber attack domain by sub-national entities see ISTS publication *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* Institute for Security Technology Studies, Dartmouth College, September 22, 2001.

[44] See Statement of Dr. Daniel T. Kuehl, Statement before the Joint Economic Committee, February 23, 2000 p.4 available at <http://www.cdt.org/security/dos/000223senate/kuehl.html>

Category One Evidence
Direct links to a foreign cyber warfare capability

1) U.S. Government Reports and Foreign Official Statements

- This evidence is the aggregate of U.S. Department of Defense assessments on a state's cyber warfare capability and that state's own official guidelines (doctrine) for waging cyber conflict.

2) Foreign Military and Intelligence Agency Research

- This area embraces multiple domains including military IT projects, equipment acquisition, active cyber warfare units, computer security, and specialized training.

Category Two Evidence
Circumstantial links indicating a baseline information technology infrastructure necessary to support a cyber warfare operation

3) Information Technology Investment

- This area embraces domains such as industrial electronics, information technology research and development efforts, network infrastructure investment, advanced university engineering curricula, software development, and state-to-state information technology initiatives, including technical assistance and training programs.

To summarize, the purpose of this report is to provide a rigorous analysis of the cyber warfare capabilities and intentions of foreign countries that is accessible to professional and non-professional readers. Cyber warfare is attractive to our adversaries because unprotected computer networks—frequently cited as America's Achilles heel—create a simultaneous dependency and vulnerbility.[45] Although we have benefited from the insights of previous research, public discourse, in many cases resting on anecdotal evidence, often inhibits understanding. We hope to raise awareness and add value to the debate through a more systematic treatment of the issues.

[45] See "The Cyber Threat to America," Jewish Institute for National Security Affairs (JINSA) Online, March 3, 2000 <http://www.jinsa.org/articles/print.html/documentid/883>

II. CHINA

WELTON CHANG

In summary, our warfare methods must adapt to the needs of information warfare. We must use all types, forms, and methods of force, and especially make more use of nonlinear warfare and many types of information warfare methods which combine native and Western elements to use our strengths in order to attack the enemy's weaknesses, avoid being reactive, and strive for being active. In this way, it will be entirely possible for China to achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology.

Major General Wang Pufeng
China Military Science, Spring 1995

"I asked why the Chinese talk in terms of "three represents," "four looks," and other such phraseology. All of you understand this, but I had to find out. Then I asked myself how those historic stratagems and sayings imbedded in Chinese culture, and the Chinese understanding of military science, affect Chinese thinking in the information age. And I was surprised to find that few had given this area as much thought as I assumed they would have. Analysts appeared more consumed with what China was doing today than how China would use its past or its tradition of military science to shape the present. Undoubtedly, a few historic Chinese phrases are thrown around when attempting to "get close" to the Chinese mentality in official speeches and even during an analysis of strategy and tactics, but I found precious few analysts had applied those strategies and concepts to electrons. Maybe that is because it is more difficult to measure the intent of an electron than it is to measure the intent of a tank."

Lieutenant Colonel (ret.) Timothy Thomas, U.S. Army
Testimony before the US-China Commission, August 3, 2001

By the early 1990s, China's military recognized that a revolution in military affairs was developing that came about as a result of the new possibilities opened up by information technologies. China's military began exploring cyber attacks as an asymmetric means of countering a technologically superior adversary on, as well as off, the battlefield. With the support of an integrated national plan, the People's Liberation Army (PLA) has developed cyber warfare doctrine, implemented basic cyber warfare training for its officers, and conducted cyber warfare exercises. China claims to be developing a unique model for employing cyber attacks, though upon closer scrutiny much of what is claimed to be unique parallels similar research done by American experts working on cyber warfare. A number of events provide some evidence the government of China condones and may even sponsor computer hacking. Beijing's foreign and internal intelligence services continue their systematic collection of science and technology information to support national goals, showing both an interest in the material collected and the high-tech collection methods. China also seeks commercial information technology products manufactured internally to meet its technology needs. While military cooperation with Russia, a country that may have developed a substantial cyber warfare program, continues, China may be developing its own models for military information collection and for the use of cyber attack technologies.

2.1 BACKGROUND

China is working diligently to sustain its rise in the world's geopolitical order. Events such as China's first manned space flight and a successful bid to host the 2008 Summer Olympic Games highlight some recent national achievements.[46] China plans to build the world's largest dam, longest bridge, fastest train, and highest-capacity railroad.[47] Beijing has crafted and implemented a multifaceted strategy by integrating its foreign, domestic, military, and economic policies in order to achieve its national objectives.[48] Edward Sobiesk writes that a cyber warfare strategy would be a logical answer to the Chinese government's current objectives of increasing "national power." A cyber warfare strategy would help to realign the international system and balance of power to one that would be more conducive to the increase of this theoretical "national power."[49]

In the short term, China's primary foreign relations issue is the question of an independent Taiwan. However, some experts believe it is unlikely that China would launch a full-scale war over the island. China considers the island a renegade province and is hostile to any moves Taiwan makes towards independence. Recent news reports as well as the official military publication titled *China's National Defense in 2002* outline force projection capabilities (primarily focusing on China's medium and long-range missile assets) and reaffirm Beijing's hard-line stance regarding Taiwan's independence. According to this publication, "China's armed forces will unswervingly defend the country's sovereignty and unity, and have the resolve as well as the capability to check any separatist act." Another issue of national importance is security relations with India as border and other disputes continue to strain relations between the two countries.[50]

China maintains secrecy concerning its military and intelligence activities as well as for all other matters of national security. Significantly, both the 2000 *Report to Congress on Implementation of the Taiwan Relations Act* and the 2003 *Annual Report on the Military Power of the People's Republic of China* note U.S. intelligence community knowledge-gaps in significant aspects of Chinese military power. American military analysts suggest that public documents, such as *China's National Defense in 2002*, may be calculated attempts to appear to be providing open information while actually keeping significant developments secret or hiding important military deficiencies.[51] At the operational level, there is little concrete evidence in open source materials describing the implementation of the new directives released in 1999 by the People's Liberation Army (PLA) Academy of Military Science.[52] What Chinese military experts state as fact

[46] Beyond its current space-faring capabilities, China has plans to build its own space station. See: CNN, "China Reveals Space Station Plan," October 16, 2003 <http://www.cnn.com/2003/TECH/space/10/16/china.space/index.html>; and the official Chinese Olympic web site <http://en.beijing-2008.org>

[47] Joseph Kahn, "China Gambles on Big Projects for Its Stability," *New York Times*, January 13, 2003 <http://www.nytimes.com/2003/01/13/international/asia/13CHIN.html?pagewanted=1>

[48] Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, July 28, 2003

[49] Edward Sobiesk, "Redefining the Role of Information Warfare in Chinese Strategy," SANS Infosec Reading Room, April 5, 2003 <http://www.sans.org/rr/papers/index.php?id=896>

[50] Op. cit. Department of Defense 2003 p.12

[51] Op. cit. Department of Defense 2003 p. 26 and China's National Defense in 2002, December 2002 <http://www.china.org.cn/e-white/20021209/>

[52] See Global Security, "China: Doctrinal Overview," 2002 <http://www.globalsecurity.org/military/world/china/doctrine-overview.htm>

concerning supposed cyber warfare developments may not actually reflect real actions taken by the PLA.

2.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

United States government officials have been reporting on China's development of cyber attack capabilities since the late 1990s. China allegedly sees cyber attacks as a component of an integrated strategy to defeat a technologically and numerically superior enemy military force. The rapidly growing Chinese economy supports the ability of the PLA to test and adopt new information technologies as a component of its modernization plans. In his 1998 testimony before the Senate Committee on Government Affairs, former CIA Director George Tenet said, "We know with specificity of several nations that are working on developing an information warfare capability."[53] Commenting on a Department of Defense assessment, Tenet said that the Chinese are attempting to "leapfrog" American military technology advances by using asymmetric means of implementing "Information Warfare" capabilities.[54] Michael Pillsbury, a research fellow at National Defense University, observed in 1997 that Beijing had the world's largest program of its type. "Judging by their military writings, they are saying that information warfare is the core of what they want to do," he said. "This way they can leap over the obsolescence of their tanks, ships, and aircraft and focus on the vulnerability of high-tech forces" like those of the United States and Taiwan.[55] The PLA has recognized the U.S. military dependence on technology in not only command and control, but intelligence gathering and precision strikes as well.

CIA Information Operations Issue Manager, John Serabian, testified before the Joint Economic Committee in February 2000 concerning China's cyber capabilities.[56] Mr. Serabian commented that cyber warfare is becoming a possible strategic alternative for countries "that realize that, in conventional military confrontation with the United States, they will not prevail." The CIA official quoted the remarks of an unidentified Chinese general: "We can make the enemy's command centers not work by changing their data system. We can cause the enemy's headquarters to make incorrect judgment(s) by sending disinformation. We can dominate the enemy's banking system and even its entire social order." Cyber attacks represent a viable strategy for countries that are "out-gunned" in conventional warfare, Serabian testified. "These countries perceive that cyberattacks, launched from within or outside the U.S., represent the kind

[53] George J. Tenet, Director of the Central Intelligence Agency, Testimony Before the Senate Committee on Government Affairs, June 24, 1998 <http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html>

[54] The assessment CIA Director Tenet refers to is as follows: Michael Pillsbury, "Dangerous Chinese Misperceptions: The Implications for DoD," 1997, unpublished paper prepared for the U.S. Department of Defense Office of Net Assessment. Pillsbury is also the author of "Chinese Views of Future Warfare," <http://www.fas.org/nuke/guide/china/doctrine/chinview/chinacont.html>. Pillsbury also wrote the Office of Net Assessment study "Dangerous Chinese Misperceptions."

[55] Reuters, "Prelude to Infowar?," June 24, 1998 <http://www.wired.com/news/politics/0,1283,13232,00.html>

[56] John A. Serabian Jr., Information Operations Issue Manager Central Intelligence Agency, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>

of asymmetric option they will need to level the playing field during an armed crisis against the U.S."[57]

The PLA has made significant strides in using information technologies to support its military objectives. The U.S. Defense Intelligence Agency Director, Vice Admiral Lowell E. Jacoby, noted in 2003 "our greatest concern is China's military buildup. Last year marked new high points for unit training and weapons integration—all sharply focused on the Taiwan mission and on increasing the costs for any who might intervene in a regional Chinese operation. We anticipate no slowdown in the coming year." Command, Control, Communications, Computers, and Intelligence (C4I) modernization and automation efforts are ongoing. China maintains separate civilian and military communication networks. Programs to support C4I are greatly enhanced by commercial information technologies now readily available in China. In examining the dual use of technologies, China is reported to have placed considerable emphasis on protecting its own C4I networks from computer attacks including viruses.[58]

The U.S. Department of Defense (DoD) reports that a Chinese strategic and tactical military revolution is underway. In the 2003 DoD *Annual Report on the Military Power of the People's Republic of China*, the authors write, "the relative technological inferiority of the PLA has led to the exploration of asymmetric methods of enabling 'the inferior to defeat the superior'."[59] Despite the statements in the DoD report, Charles Bacon believes that "China lags behind the U.S. in the development of Information Warfare capability and will probably remain behind for some time."[60]

2.2.1 Evolution of Chinese Views on Cyber Warfare

In July of 2004, Jiang Zemin, who has remained the Central Military Commission Chairman, "called on Chinese military forces to be equipped with information technology for the strategic goal of winning information warfare."[61] The development of Chinese strategy in the domain of cyber warfare can be traced to the early 1990s. Following the conclusion of the first Gulf War in 1991, the Chinese government and PLA doctrinal thinkers began to analyze the U.S. military

[57] This study uses the term asymmetric warfare or operations to describe "the actions of leveraging inferior tactical or operational strength against enemy vulnerabilities to achieve disproportionate effect in order to achieve the asymmetric actor's strategic objectives," U.S. Air Force, "Air and Space Power Course," September 1, 2004 <http://www.apc.maxwell.af.mil/text/aa/def.htm>; Another, more nuanced definition: "asymmetric approaches are attempts to circumvent or undermine US strengths while exploiting US weaknesses using methods that differ significantly from the United States' expected method of operations. [Asymmetric approaches] generally seek a major psychological impact, such as shock or confusion that affects an opponent's initiative, freedom of action, or will. Asymmetric methods require an appreciation of an opponent's vulnerabilities. Asymmetric approaches often employ innovative, nontraditional tactics, weapons, or technologies, and can be applied at all levels of warfare—strategic, operational, and tactical—and across the spectrum of military operations." Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, Strategic Studies Institute, January 2001, available at: <http://www.au.af.mil/au/awc/awcgate/ssi/asymetry.pdf>

[58] Op. cit. Department of Defense 2003 p. 36

[59] Op. cit. Department of Defense 2003 p. 21

[60] Charles Bacon, "The China Syndrome," SANS Institute, July 22, 2001 <http://www.sans.org/rr/papers/index.php?id=788>

[61] Xinhua.net, "Jiang Zemin stresses information technology in army construction," July 26, 2004 <http://news.xinhuanet.com/english/2004-07/26/content_1651552.htm>

victory. American and Coalition military forces used joint operations coordinated by electronic means in order to defeat the Iraqi military.[62] In the initial salvo of U.S. missiles, most of Iraq's command and control capabilities, as well as its information gathering radar sites were destroyed. Beijing, and many other world powers, viewed the overwhelming victory combining information technologies and conventional power as a Revolution in Military Affairs (RMA).[63]

Throughout the reports and statements China has released and published on cyber warfare, two main lines of thought stand out. First, cyber warfare strategy (as does conventional warfare strategy) in Chinese literature makes references to Sun Tzu in nearly every written document. While the actual effect of Sun Tzu's strategic principles of warfare on the modern Chinese variety is hard to discern, it is clear that Sun Tzu is a great influence, at the minimum, on Chinese doctrinal writing. Second, cyber warfare strategy is in keeping with national goals because it is a cost-effective way of conducting asymmetric operations against an adversary.

2.2.2 The Beginnings of Doctrinal Research

In one of the first papers written on Chinese cyber warfare doctrine, Shen Weiguang wrote

"Those who take part in information war are not all soldiers. Anybody who understands computers may become a 'fighter' in the network. Think tanks composed of non-governmental experts may take part in decision-making; rapid mobilization will not just be directed to young people; information-related industries and domains will be the first to be mobilized and enter the war..."[64]

Shen, now a purported expert in cyber warfare, described the "concept of 'take-home' battle" in which the Chinese would conduct a different and personal type of People's War with computers.

The evolution from the People's War strategy to the adoption of information technologies to defeat superior enemies may be seen as an integral component of a Chinese plan to become a world leader without having to spend an inordinate percentage of its GDP in a military build-up. The development of a cyber warfare arsenal is referred to by U.S. expert Lieutenant Colonel (ret.) Thomas as "adding wings to a tiger," i.e., giving increased capabilities to a foreign military largely considered to be the only power in the world that can, in the future, rival the American military. The Chinese military is attempting to produce its own specific type of "Chinese" cyber warfare strategy, much like the attempt to form socialism and communism into ideas that can be applied specifically to the Chinese people.

Several researchers at the Chinese Academy of Military Science, China's National Defense University, and the Wuhan Communications Command Academy have published books concerning the usage of cyber warfare.[65] Further data for analysis can be gleaned through an examination of the development of unique Chinese cyber warfare strategies. The U.S. tends to

[62] Referred to as the "Air-Land" Battle Doctrine

[63] Senior Colonels Wang Baocun and Li Fei, "Information Warfare," *People's Liberation Army Daily,* June 20, 1995 <http://www.fas.org/irp/world/china/docs/iw_wang.htm>

[64] Lieutenant Colonel (ret.) Timothy L. Thomas, "Behind the Great Firewall of China: A Look at RMA/cyber warfare Theory From 1996-1998," November, 1998 <http://fmso.leavenworth.army.mil/fmsopubs/issues/chinarma.htm>

[65] Op. cit. Department of Defense 2003 p. 36

focus on the computer network attack aspects of cyber warfare but China's cyber warfare focuses more on psychological operations and denial and deception of military data.[66] In times of war, Chinese cyber warfare doctrine focuses on defeating the enemy before stepping into battle; meaning that Chinese forces should have a signficant information advantage in future battles so that the outcome of engagement should be largely predetermined.

PLA senior Colonel Wang Baocun, a Chinese cyber warfare strategy expert, states that cyber warfare strategy reinforces the notion of Sun Tzu's "subduing the enemy without battle."[67] He states that the purpose of cyber warfare is to "force the enemy side to regard their goal as our goal," to "force the opponent to give up the will to resist and end the confrontation and stop fighting by attacking an enemy's perception and belief via information energy."[68] Apparently unique Chinese elements can be found in other writings as well. Senior Colonel Wang, in his article *The Current Revolution in Military Affairs and its Impact on Asia-Pacific Security*, defines cyber warfare as "a form of combat actions which attacks the information and information systems of the enemy while protecting the information and information systems on one's own side." Furthermore, Colonel Wang states that "the key elements of cyber warfare are military security, military deception, physical attack, electronic warfare, and net warfare, and its basic purpose is to seize and maintain information dominance."[69]

In 1999, two other PLA senior Colonels, Wang Xiangsui and Qiao Liang published, *Unrestricted Warfare* [Chao Xian Zhan][70], a widely referenced work on the advantages of asymmetry in the contemporary Information Age. The work drew its conclusions from analyzing both the weaknesses and strengths of the U.S. conventional military prowess. *Unrestricted Warfare's* main thrust was an argument that those who saw that the root of global hegemony was an overpowering force on the battlefield would be surpassed by those who saw that the lines between economic, political, and military warfare were disappearing. Qiao and Liang argued that in the future, raw military power will neither be the only or main way for a nation to spread its influence nor the most cost-effective way to cause harm to an adversary. A key point of *Unrestricted Warfare* stems from the idea of "build[ing] the weapons that fit the fight" instead of "fighting the fight that fit one's weapons."[71] Wang and Qiao's ideas seem to have affected the PLA's thinking on how to better use its resources and military investment, leading to a reduction of the active military forces and an increase in military information technology.

---

[66] Edward Sobieski writes that this could come as a result of the fundamental differences in strategic planning exhibited by Western and Eastern military planners, analogizing the differences in strategy with the differences between the games of Go and Chess. Op. cit. Sobieski 2001

[67] Senior Colonels Wang Baocun and Li Fei, "Information Warfare," *People's Liberation Army Daily,* June 20, 1995 <http://www.fas.org/irp/world/china/docs/iw_wang.htm>

[68] Willy Wo-Lap Lam, "China army looks to technology," March 10, 2003 <http://www.cnn.com/2003/WORLD/asiapcf/east/03/09/china.generals/index.html>.

[69] Ibid Wang and Li 1995

[70] The literal translation of the title is "war that crosses boundaries" which fits with the argument of the blurring of the distinction between civilian and military conflict because of globalization and the widespread usage of information technology. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999). A translation of this document can be found at: <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>

[71] Ibid Qiao and Wang 1999 19

Because the PLA lacks the conventional strength to defeat superior adversaries, Chinese strategists believe that innovative cyber warfare strategies can play a key role in an asymmetric victory. Major General Dai Qingmin's article on cyber warfare titled *Innovating and Developing Views on Information Operations* reasons that China's technological deficiencies can be overcome by developing good cyber warfare strategies.[72] Among these strategies are "jamming or sabotaging an enemy's information or information system, giving an enemy a false impression and launching a surprise information attack on him at the same time, causing an enemy to make a wrong judgment or take wrong action, etc." The primary conclusion of the author (Dai Qingmin) is that Chinese warfare strategies have undergone a transformation. Concentrations of forces (mass armies that characterized the Chinese military) will be replaced by new and more efficient strategies using information technology, effectively blurring the front and rear lines of combat.[73]

2.3 FOREIGN MILITARY AND INTELLIGENCE AGENCY RESEARCH

China continues to maintain the largest conventional military forces in the world.[74] Despite this fact, the PLA recognizes its limited effectiveness due to its inability to project force as well as to fight an all-out conventional war with the United States. The DoD estimated in March 2002 that publicly reported Chinese military spending totals $20 billion. However, much of the PLA's spending, such as foreign weapon purchases and research and development, is not reported. Although estimates vary, the PLA budget could total as much as $65 billion.[75] Further, most force modernization costs are outside the publicly available spending figures. Relevant to this study, the recently released PLA budget shows a change in the priorities of the PLA: a 9.6% budget boost targeted improvements in "rapid-response and IT warfare" and preparation for emergencies. PLA General Guo Boxiong emphasized that the Chinese military must improve its ability to win high tech warfare.[76]

The Chinese military is clearly pursuing cyber warfare to counter the widely acknowledged dominance of the American conventional military. The Chinese have termed this research approach "acupuncture warfare." Acupuncture warfare has been defined as "paralyzing the enemy by attacking the weak link of his command, control, communications and information as if hitting his acupuncture point in kung fu combat."[77] A component of this strategy, discussed further in the Information Technology Investment section of this report, is the use of civilian hackers. According to senior Colonel Wang, the civilian apparatus can be made to cooperate with the military cyber warfare forces to strengthen cyber attack operations. Senior Colonel Wang emphasizes that anyone with a computer can join in the fight against an opposing force acting as a force multiplier. To this end, there is some evidence that officially condoned hacking

[72] Major General Dai Qingmin, "Innovating and Developing Views on Information Operations," *Beijing Zhongguo Junshi Kexue* [China's Military Science Journal, Beijing] August 2000
[73] Ibid Major General Dai Qingmin 2000
[74] Op. cit. Department of Defense 2003 p. 41
[75] Op. cit. Department of Defense 2003 p. 41
[76] Willy, Wo-Lap Lam, "China army looks to technology," March 10, 2003 <http://www.cnn.com/2003/WORLD/asiapcf/east/03/09/china.generals/index.html>
[77] Gurmeet Kanwal, "Chinese Military II," *The Statesman*, January 16, 2002

occurred following the mid-air collision between an American surveillance plane and a Chinese fighter aircraft on April 1, 2001.[78]

In a *Jane's Intelligence Review* article published in 2002, U.S. Army Lieutenant Colonel (ret.) Thomas finds that the PLA divides Chinese cyber warfare strategy into three parts: surveillance, attack, and protection. Network and electromagnetic surveillance allows the PLA to collect information on potential targets and develop an attack plan against critical infrastructure. Computer information attack refers to "operations to disrupt, sabotage and destroy information in enemy computer network systems using specialized equipment, software or firepower." Protection refers to prevention of enemy surveillance and attack options against friendly computer systems.[79] Strategic targets of Chinese cyber warfare may include computer networking systems linking "political, economic and military installations of a country as well as society in general." According to Lieutenant Colonel (ret.) Thomas, many Chinese theorists have proposed organizing "network special warfare detachments and computer experts to form a shock brigade of 'network warriors' to accomplish these tasks."[80]

Training for future cyber attack operations is of primary importance to the PLA. Among the PLA's cyber warfare training centers are the Communications Command Academy in Wuhan, the Information Engineering University in Zhengzhou, the Science and Engineering University, and the National Defense Science and Technology University in Changsha. All of these centers maintain professors and experts on cyber warfare to train PLA soldiers. PLA officer course curriculum includes: basic theory, including computer basics and applications; communications network technology; the information highway; units connected by IT; electronic countermeasures; radar technology; cyber warfare rules and regulations; cyber warfare strategy and tactics; theater and strategic cyber warfare; information systems, including gathering, handling, disseminating and using information and combat command, monitoring, decision-making, and control systems.[81] Other formal training for PLA officers includes the usage of information weapons, simulated cyber warfare, protection of information systems, computer virus attacks and counterattacks, and jamming and counter-jamming of communications networks.[82]

Military exercises conducted by the PLA also involve cyber wafare. For example, the first "special" (meaning cyber warfare) PLA battle took place in October 1997. In the Shenyang Military Region, a Group Army (GA) underwent a computer attack that paralyzed its systems. The GA countered with virus-killing software, and the exercise was termed an "invasion and anti-invasion" event. This exercise involved the deployment of ground, logistics, medical, and air force units. The second occurred in October 1998, when the Chinese military staged an integrated high-technology exercise that united several military regions around the country. The center of gravity of the exercise was the Beijing Military Region, where a joint defense warfare drill used a "military information superhighway" for the first time. Another exercise took place

[78] BBC News, "White House website attacked," May 5, 2001 <http://news.bbc.co.uk/1/hi/world/americas/1313753.stm>
[79] Jane's Intelligence Review, "Confrontation central to Chinese cyber warfare aims," June 1, 2002
[80] Lieutenant Colonel (ret.) Timothy L. Thomas, "Like Adding Wings to the Tiger: Chinese Information War Theory and Practice," 2000 <http://fmso.leavenworth.army.mil/fmsopubs/issues/chinaiw.htm>
[81] Ibid Thomas 2000
[82] Ibid Thomas 2000

in October 1999 when the PLA conducted another cyber warfare simulation. Two army groups of the Beijing Military Region gamed a "confrontation" campaign against computer networks. Reconnaissance and counter reconnaissance, interference and counter-interference, blocking and counter-blocking, and air strikes and counter air strikes were among some of the high-tech tactics practiced during the exercise. Finally, in July of 2000, the Chengdu Military Region conducted a confrontational campaign exercise on the Internet.[83]

The Chinese military is growing not only in its understanding of and competence in cyber warfare, but also in its development of cyber warfare-related technologies. Moreover, the PLA is increasing the number and training of organizations involved with cyber warfare.[84] Chinese Major General Dai writes that not only has the Chinese military made leaps and bounds in strategy, they have also put the theories to test with their cyber warfare divisions acting as operational forces against each other. Ten strategies that were employed in these exercises include "planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information, organizing information defense, and establishing network spy stations."[85]

China is developing a strategy for integrating the country's civilian computer experts in military reserve units within the PLA. The PLA has developed recruiting programs for technical experts possibly in order to develop their cyber warfare assets.[86] Military reserve units specializing in cyber warfare are in development in several cities. As Wang Xiaodong, an officer in the PLA stated, "the Chinese population numbers in the billions. If one or two per cent of any population has an IQ over 139, as studies predict, then China must have tens of millions of people in this category. The problem is how to find more information space and equipment for all of these people." This serves the dual purpose of fulfilling the Maoist concept of a People's War and creates a large electronic army.

James Mulvenon, in writing for RAND, imagines the possible usage of such a People's War against an adversary:

"When one imagines scenarios in which the PLA would be concerned with preemptively striking U.S. forces during the deployment phase for early strategic victory, it is difficult to avoid the obvious conclusion that the author is discussing a Taiwan conflict. For the PLA, using IW against U.S. information systems to degrade or even delay a deployment of forces to Taiwan offers an attractive asymmetric strategy. American forces are highly information-dependent, and rely heavily on precisely coordinated logistics networks . . . If PLA information operators using PCs were able to hack or crash these systems, thereby delaying the arrival of a U.S. carrier battle group to the theater, while simultaneously carrying out a coordinated campaign of short-range ballistic missile attacks, "fifth column," and IW attacks against Taiwanese critical infrastructure, then Taipei might be quickly brought to its knees and forced to capitulate to Beijing."[87]

---

[83] Ibid Thomas 2000

[84] Willy Wo-Lap Lam, "China army looks to technology," March 10, 2003 <http://www.cnn.com/2003/WORLD/asiapcf/east/03/09/china.generals/index.html>

[85] Major General Dai Qingmin, "Innovating and Developing Views on Information Operations," *Beijing Zhongguo Junshi Kexue*, [China's Military Science Journal] August 2000

[86] Op. cit. Department of Defense 2003 p. 36

[87] James Mulvenon, *The PLA and Information Warfare*, RAND, 1999 <http://www.rand.org/publications/CF/CF145/CF145.chap9.pdf>

The PLA continues to develop its cyber attack capabilities. Ongoing budget increases, improvements in basic C4I, training, exercises, and new programs to recruit civilian experts are indications of China's plans. In addition to active forces, the PLA maintains reserve units whose sole mission is to perform cyber warfare functions. These units have participated in cyber warfare exercises and simulations. As of 2003, the Department of Defense reports that "China has the capability to penetrate poorly protected U.S. computer systems and potentially could use computer network attacks to strike specific U.S. civilian and military infrastructures. This anti-access strategy is centered on targeting operational centers of gravity, including C4I centers, airbases, and aircraft carrier battle groups located around the periphery of China."[88]

Despite China's apparent strides in developing cyber warfare, some skeptics see a pattern among Chinese military thinkers as they continually turn to cyber warfare as an apparent cure-all for an increasingly outdated and obsolete military. They argue the threat from cyber warfare operations is exaggerated because the PLA continues to lack sufficiently modern weapons and equipment to pose a threat to the U.S. military, even if it was able to successfully wage cyber warfare in a military setting. These critics also believe that although the Chinese military has a fully realized doctrinal understanding of cyber warfare, they lack the knowledge and technology to implement it. However, through examination of open source materials, it is evident that China already is, in practice, a rising force, and a potentially knowledgeable wielder of cyber warfare and cyber war capabilities.[89]

China maintains significant foreign and internal intelligence capabilities. Chinese intelligence services have a special interest in espionage pertaining to the information technologies. According to the 2003 Department of Defense *Annual Report:*

"As of 1991 there were roughly 4,000 individual intelligence organizations operating in China. Many of these organizations are associated with state-owned enterprises, research institutes, and academies affiliated with China's defense industrial base. The collection of technical information probably continues to be orchestrated by the CDSTIC, which now is subordinate to the PLA's General Equipment Department (GED). The GED reportedly oversees a complex web of factories, institutes, and academies that are subordinate to China's nuclear, aeronautics, electronics, ordnance, shipbuilding, and astronautics industries. Each of these institutions has an import/export corporation to facilitate the import of technology and knowledge."

Rob Koepp, a researcher at the Milken Institute in Santa Monica, argues that China is more than merely interested in catching up to the West in terms of technological development. Mr. Koepp believes that China wants to "bring about fundamentally innovative technology over time" that will set standards for the whole world.[90] According to the Federation of American Scientists, the Ministry of State Services (MSS), a Chinese intelligence organization, may "aggressively target the U.S., placing particular emphasis on the high tech sector heavily concentrated in Southern California, and in the Silicon Valley. Cover for Beijing's espionage in the United States may includes [sic]the 1,500 Chinese diplomats operating out of 70 offices, 15,000 Chinese students

[88] Op. cit. Department of Defense 2003 p. 36
[89] Toshi Yoshihara, "Chinese information warfare: A phantom menace or emerging threat?," Army War College Strategic Studies, November 2001 <http://www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf>
[90] James Flanigan, "China's Technological Ambitions Take Flight," *Los Angeles Times*, October 19, 2003

who arrive in the U.S. each year, and 10,000 Chinese who travel in some 2,700 visiting delegations each year."[91]

In addition to intelligence activities, open sources almost certainly help Chinese information collection efforts. For example, in 1991 the China Defense Science and Technology Information Center (CDSTIC) published a science and technology collection manual titled *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*.[92] This document "suggested that 80 percent of China's defense S&T needs are met through open and gray source (purchase/subscription) materials."[93] Further, the guidebook provided detailed information on foreign open sources concerning defense technology.

With American information infrastructure vulnerabilities often published in open sources, China's intelligence services may be better positioned to focus their activities on high value targets. Active intelligence programs by China, both internally and externally, are in all likelihood delivering information on new technologies and how they may be used to exploit adversaries' weaknesses. In addition, the proliferation of overseas Chinese diplomats, businessmen, and students may serve as an ongoing network for collecting open source data from a structured set of requirements produced by the Chinese government.

2.4 INFORMATION TECHNOLOGY INVESTMENT

China's efforts to acquire and develop information technologies for commercial and military uses are extensive. The CCP fully supports the adoption of efficiency-enhancing information technology. However, the use of the Internet and other technologies for political activities not authorized by Beijing is strictly controlled. According to Lu Chengzhao, deputy director-general of the Office of China National Network and Information Security Coordinating Group, "China's public Internet emergency response system is being constructed and perfected and China is expected to complete the construction of National Network and Information Security System in five years."[94] China's top leaders, many with advanced degrees in the mechanical sciences, have been supportive of technological infrastructure improvements as a component of overall economic development.

China uses various methods—seed funding, tax breaks for information technology research and development, utilization of technology development zones—to attract overseas investment, technical knowledge of advanced technology, and management experience. The Chinese government continues to stress the need to "import technology rather than finished goods, and to renovate factories through selective purchase of key technology rather than through purchase of whole plants."[95] China is actively seeking foreign direct investment, especially for those seeking to develop high-technology products. Recent reports comment that the Chinese government

[91] Federation of American Scientists Intelligence Resource Program, "Ministry of State Services," January 1998 <http://www.fas.org/irp/world/china/mss/ops.htm>
[92] Op. cit. Department of Defense 2003 p. 40
[93] Op. cit. Department of Defense 2003 p. 40
[94] People's Daily, "China to complete national network and information security system in five years," February 13, 2004 <http://english.people.com.cn/200402/13/eng20040213_134785.shtml>
[95] American University, "Information Technology Landscape of China," March 2003 <http://www.american.edu/initeb/fl9577a/china.htm>

"gives funding to academic institutions and new small companies to commercialize products of academic research."[96]

According to the 2003 DoD *Annual Report,* "thousands of PRC business entities have been established in the United States. The bulk of the business conducted by these entities is probably legitimate, but an undetermined number may target dual-use commodities and controlled technologies restricted from sale to the PRC."[97] The report's authors also note that "authoritative PRC journals have recommended an increase in the use of overseas ethnic-Chinese scientists to transfer foreign technology."[98]

In addition, with increased "out-sourcing" to China in recent years, there is the risk that software companies could deliberately embed back-doors in the programming code which would render the software vulnerable to intrusion. The presence of a software "time bomb" might not be detected until it is too late.

China may be using technically capable individuals to engage in hacking activities. As outlined in the Official Doctrine section of this paper, authors have written about the mass mobilization of the Chinese population for cyber attack operations. It is difficult to ascertain through exclusively open sources the extent of Chinese hackers' involvement with the central government. However, it is clear that hackers have launched cyber attacks following physical incidents. iDefense analysts state that the hackers in China are not actually "state-sponsored"; they place them under a category labeled "state-controlled."[99]

For example, after the May 2000 bombing of the Chinese Embassy in Belgrade, hackers attacked United States political, military, and civilian web sites. The following year, Department of Defense officials warned that reprisal was likely on the anniversary of the 2000 accidental bombing. The Chinese Liberation Army Daily reportedly advocated the recruitment of civilians to aid in the cyber attacks.[100] After major attacks did not happen, Air Force Maj. General John Bradley commented "We expected another series of attacks from Chinese hackers, but actually the government of China asked them not to do that."[101]

Following the collision of an American reconnaissance aircraft and a Chinese fighter plane on April 1, 2001, Chinese hacker groups, such as the Honker Union of China and the Chinese Red Guest Network Security Technology Alliance, organized sustained cyber attacks against American targets.[102] The FBI's National Infrastructure Protection Center (NIPC) issued an advisory warning of "the potential for increased hacker activity directed at U.S. systems during

[96] Ibid American University 2003
[97] Op. cit. Department of Defense 2003 p. 40
[98] Op. cit. Department of Defense 2003 p. 40
[99] iDefense, "Inside the China Eagle Union hacker group," *iDefense Intelligence Operations*, April 29, 2002 [White paper available upon request sent to iDefense at di@idefense.com]
[100] Hans Lombardo, "Chinese Military seeks to train Cyber Warriors," Asia.Internet.com, August 3, 1999 <http://asia.Internet.com/news/article.php/650911>
[101] Pamela Hess, "China prevented repeat cyber attack on US," *United Press International*, October 29, 2002 <http://www.intellnet.org/news/2002/10/29/13249-1.html>
[102] Op. cit. iDefense 2002

the period of April 30, 2001 and May 7, 2001."[103] In the 2001 report *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* ISTS reported that "it remains unclear whether the Chinese government sanctioned these attacks, but, in light of the fact that these activities were highly visible and no arrests were made by Chinese officials, it can be assumed that they were at least tolerated, if not directly supported by Chinese authorities."[104]

Hacker organizations may also have received help from the Chinese government in developing software, viruses, and methods to attack various computer networks. A number of recent Internet worms including Lion, Adore, and Code Red are suspected of having originated in China. Keith Rhodes, the Chief Technologist at the U.S. General Accounting Office (GAO), commented that the Code Red worm could be traced to a university in Guangdong, China.[105] This assertion must be viewed critically since other computer security experts, including the NIPC, have commented that they are unable to ascertain the worm's origin.[106] There have been other incidents in which the Chinese government has been accused of helping hackers execute cyber attacks on foreign targets. Two Canadian ISPs, BestNet and Nebula Internet service, accused the Chinese government of sponsoring hackers with a political agenda. The crackers launched a denial of service attack at the Internet Service Providers' servers because the two ISPs had been hosting websites for the Falun Gong, a religious group that is outlawed in China. The attacks were traced back to the Beijing Application Institute for Information Technology and the Information Center of Xin An Beijing. The method of attack began with penetration of the ISPs' servers and then turned to flooding the servers with incomplete information requests that caused the hosted site to crash. Although the methods were unable to bring down BestNet's services, Nebula Internet went offline due to the flood of data. The U.S. Department of Transportation also contacted Nebula because an IP address involved in a "probe" on the Federal Aviation Administration server was traced back to Nebula's servers.[107]

Hypothetically, Chinese government use of hacker organizations appears to fall within the doctrinal themes set out in the cyber warfare iteration of the People's War philosophy. Further supporting this position are the recruitment programs set up by the PLA to attract technical experts. Long-term priorities to collect science and technology information would seem to suggest the Chinese government pragmatically uses the resources at it disposal to achieve its goals. Lastly, as demonstrated by the monitoring of political activities in cyber space, the Chinese government controls access to Internet connections and is almost certainly aware of cyber attacks that originate from within its territory. Sponsorship of hacker groups may be cost-efficient for the Chinese government. In comparison to maintaining large numbers of military

[103] National Infrastructure Protection Center Advisory 01-009, "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May," April 26, 2000

[104] Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* September 22, 2001 <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>

[105] Keith A. Rhodes, General Accounting Office Chief Technologist Statement Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives, August 29, 2001 <http://www.gao.gov/new.items/d011073t.pdf>

[106] Newsfactor.com, "Feds Hunt For Code Red Creator as Reactivation Nears," August 31, 2001, <http://www.newsfactor.com/perl/story/13255.html>

[107] Oscar S. Cisneros, "ISPs accuse China of Infowar," July 30, 1999 <http://www.wired.com/news/politics/0,1283,21030,00.html>

cyber warfare specialists, lower-budget hacker groups can support and obfuscate military cyber attack operations, with little outlay of additional government resources.[108]

China continues to procure military and dual-use technologies from Russia and other countries. Russia has a well-documented offensive cyber attack program.[109] In addition, China participates in military exchanges with other nations such as Pakistan and North Korea. According to *China's National Defense in 2002* the "PLA's foreign military academic exchanges and technical cooperation have also constantly developed" including "ex-change visits of more than 100 delegations or groups of military experts with several dozen countries."[110] For example, the Chinese President of the University of National Defense Science and Technology, the PLA institution that developed the first Chinese supercomputer, visited Russia on a military exchange in 2002.[111]

Instead of following the traditional methods of purchasing technical assistance, China may be building a network for collecting information that will be utilized in commercial and military development programs.[112]

Media reports indicate that China acquires information technologies illegally. In November of 2003, Gao Zhan, formerly a researcher at American University, pleaded guilty to charges of illegally exporting computer technology to China, some of which may have wound up in the hands of the Chinese military.[113] A report noted that "among the items sent to China were microprocessors that can be used in digital flight control and weapons systems, including identifying targets. Although these microprocessors also have commercial uses, they cannot be exported without permission of the U.S. government." In December of 2003, Sun Microsystems was fined $291,000 for allegedly exporting advanced computers to China that were eventually used for military purposes.[114] According to the report, Sun sent a powerful E5000 series server to China back in 1997, more specifically to a company called Automated Systems Ltd. based in

[108] Other recent examples of Chinese hacker attacks are: Cynthia Wan, "Chinese hackers sabotage websites in Japan, Taiwan," August 6, 2004, *Kyodo*, <http://home.kyodo.co.jp/all/display.jsp?an=20040806143>; *The Chosun Ilbo*, "Global Hackers Test Their Skills on Korean Computer Systems," July 25, 2004 <http://english.chosun.com/w21data/html/news/200407/200407250029.html>; Channelnewasia, "Chinese Hackers Attack Taiwan News Agency Ahead of Drill," July 20, 2004 <http://www.channelnewsasia.com/stories/afp_asiapacific/view/96583/1/.html>, *The Chosun Ilbo*, "Hacking Attempts from China, Taiwan, Hong Kong Increasing Rapidly," July 16, 2004 <http://english.chosun.com/w21data/html/news/200407/200407160030.html>; Wang Chun Ming, *Taiwan News*, "PRC Surfers Hack into DPP Website," June 23, 2004 <http://www.etaiwannews.com/Taiwan/2004/06/23/1087958173.htm>; and *Taipei Times*, "Hackers Prey on Internet Banking," June 10, 2004 <http://www.taipeitimes.com/News/taiwan/archives/2004/06/10/2003174478>

[109] For a discussion of Moscow's cyber attack capabilities see Chapter VII of this report

[110] Op. cit. China's National Defense in 2002

[111] Op. cit. China's National Defense in 2002 and ZDNet UK, "China launches first supercomputer" September 2, 2002 <http://news.zdnet.co.uk/software/developer/0,39020387,2121608,00.htm>

[112] Op. cit. Department of Defense 2003

[113] CBS News, "Human Rights Hero Spied for China," November 26, 2003 <http://www.cbsnews.com/stories/2003/11/26/national/main585780.shtml>

[114] *LA Times*, "Sun Microsystems Fined $291,000 in Crackdown," December 16, 2003 <www.latimes.com/technology/la-fi-rup16.1dec16,1,7353734.story?coll=la-headlines-technology>

Hong Kong. Eventually U.S. federal agents found the machine at the Changsha Institute of Science and Technology, which is in mainland China.

2.5 CONCLUSION

The Chinese government has formulated and is implementing an integrated strategy of diplomatic, informational, military, and economic policies to achieve its national objectives. Although open literature strongly suggests that Beijing is pursuing cyber warfare programs, secrecy hampers detailed assessments. The CIA and Department of Defense report that China sees cyber warfare as a viable asymmetric strategy when facing technologically superior adversaries.

Chinese military institutions have published works on cyber warfare. These studies stemmed from evaluations of the revolution in military affairs that was triggered by the United States' overwhelming victory over an adversary with similar conventional military capabilities to that of China in the 1991 Gulf War. Analysis of Chinese studies on cyber warfare indicates that Beijing is developing a distinct model drawing on United States doctrine and ancient Chinese warfare tenets. Overall, the Chinese see cyber attacks as a way to combat and neutralize a superior enemy.

Although China maintains the largest conventional forces in the world, digital Command, Control, Communications, Computers, and Intelligence (C4I) capabilities are lacking. The Chinese military has spent considerable resources upgrading its C4I networks. These efforts have resulted in what appears to be an appreciation of the potential vulnerability of systems built with commercially available technology, an appreciation that has led to investments in computer network defense especially against viruses. The Chinese military routinely trains its officers concerning information technology developments. A number of exercises that tightly integrate cyber attacks into conventional scenarios have increased Chinese understanding of the dynamic involved in information operations. The PLA has implemented programs to recruit technical experts to support its cyber attack capabilities.

It is almost certain that Beijing's intelligence services are systematically collecting science and technology information from outside China's borders to support national goals. China has published collection handbooks outlining how open source materials can substantively contribute to China's research and development efforts. In addition to highly publicized international spy cases involving technology and intellectual property theft, China has significant internal security and intelligence services monitoring Internet activity.

Implementing many economic reforms, the Chinese government grants a number of incentives to foreign companies and domestic academic research to further national goals. China has targeted dual use technologies for import by Chinese owned businesses around the world. China may be harnessing the technological skill of its hacker population to support cyber attacks. Media reports support this position, but no conclusive evidence was uncovered during the research for this study. Chinese military purchases of weapons and technology from Moscow coupled with official exchanges with Russia, a country that in all likelihood maintains an offensive cyber attack capability, continue. In addition, Beijing appears to be developing a broad network of

academic and business relationships internationally to supplement external military assistance and intelligence collection.

III. INDIA

CHARLES BILLO

The traditional concept of national security has undergone fundamental changes over the years. It is no longer synonymous with sufficient military strength to defend the nation and its interests. In today's world, military might alone does not guarantee either sovereignty or security. The more realistic and comprehensive approach to national security also includes economic strength, internal cohesion, and technological prowess. The rapid technological developments underway at the same time not only facilitate these events by reducing our reaction time but add entirely new dimensions of threat and challenges, such as the Revolution in Military Affairs (RMA) and offensive/defensive information warfare.

Government of India "Challenges to the Management of National Security"
Report of the Group of Ministers on National Security, February 2001

The defense forces on their part have adopted information warfare doctrines, which include infosec as a vital element. There is a growing partnership between defense and private industry to evolve IT security solutions for the defense information infrastructure….As defense reliance on commercial off the shelf technology (COTS) grows, the dilemma of selecting an appropriate vendor has been to a large extent addressed by the CII [Confederation of Indian Industry] online defense directory—a web-based listing of Indian software vendors working on defense-related systems and applications.

Lt. Commander Prashant Bakshi, "Security Implications of a Wired India: Challenges Ahead"
Strategic Analysis, April 2001

The Indian Government's Task Force on Cyber Crime is joining hands with corporate bodies to fight Pakistani net infiltrators. The move came after hackers claiming to belong to a Pakistani organization called G-Force, defaced the home page of the Ministry of External Affairs website. A total of 162 Indian websites have been hacked into and defaced so far this year, a phenomenal increase from 72 last year.

Strategic Affairs Newsbrief, May 2001

3.1 BACKGROUND

India has experienced, and continues to undergo, cyber attacks in a variety of forms. On June 7, 1998, for example, an anti-nuclear group "Milw0rm" reportedly hacked into the Bhaba Atomic Research Center (BARC) network to protest India's nuclear tests. In the same time period, Pakistani hacker groups, such as Death to India, Kill India, Dr. Nuker, and G-force Pakistan, openly circulated instructions for attacking Indian computers.[115] According to a 2003 account in *The Hindu*, for more than two years the hacker war between India and Pakistan has been intensifying, leading to the defacement of hundreds of websites on either side. "Earlier this year, newspaper reports had indicated that an unnamed virus launched by a secretive Indian hacker group had rendered 200 Pakistani websites inaccessible for several days and erased the hard disks of scores of computer [sic] in the Pakistani Government as well as the private sector in that country."[116]

[115] According to an article in the *Hindustan Times*, websites run by Nicholas Culshaw of Karachi and by Arshad Qureshi of Long Beach, California contain malicious anti-Indian propaganda along with instructions for hacking into thousands of Indian websites. Ravi Prasad, "Hack the Hackers," in the *Hinsdustan Times*, December 19, 2000.

[116] G. Anand, "Indo-Pak Hacker War Comes Here Too," *The Hindu*, June 9, 2003

Cyber attacks consequently pose more than a theoretical challenge to the Indian government's day-to-day national security agenda. In response to these attacks, the leaders of India's armed forces have embraced the need for change and have begun to build partnerships with industry intended to transform the military into a technology-focused force.

In the late 1990's, New Delhi undertook a review of defense posture in the framework of what strategists call the "Revolution in Military Affairs" (RMA) posed by the application of digital technologies to precision guided weapons, battlefield awareness, and instantaneous communications.[117] In a 2001 report, *Challenges to the Management of National Security*, political leaders focused on addressing military and related threats below the nuclear threshold and highlighted cyber offense and defense:

> The emergence of non-state terrorist actors and the rise of their international influence is accelerating. Much of their activity is clandestine and outside the accepted international norms… India is at the receiving end of these violent elements and is likely to remain a target of international terrorism in the future. Strategies need to be evolved to counter the threat of Weapons of Mass Destruction Terrorism (WMD) as well as cyber terrorism; the latter especially against infrastructural and economic assets such as banking, power, water, and transportation sectors. [118]

Figure 1: Strategic and Geopolitical View

Due to its history, geographic location, and heterogeneous population, India faces a broad and complex range of security threats. On the one hand, there is the *domestic* threat to national unity. The insurgency in Kashmir, actively assisted by Pakistan, is a notable example. Less publicized internal challenges include left wing extremist (e.g., Maoist) violence, illegal migration (from Bangladesh), and "caste, communal and sectarian" unrest often deriving from fundamentalist rivalries and the constraints of traditional religious obligations. As a recent official study puts it: "There is no Indian community which is not a minority in some other parts of the country."[119]

On the other hand, *external* pressures from China, Bangladesh, and particularly Pakistan pose persistent challenges. A few years ago, tensions between India and Pakistan, each armed with nuclear missiles, were higher than at any time in the past decade. India holds enormous conventional military superiority over Pakistan and its defensive posture "is heavily tailored to the problem of potential conflict" with Islamabad.[120]

[117] Andrew Marshall, head of the Pentagon's Office of Net Assessment, provoked a series of debates in the late 1980s about the possibility that advances in surveillance, precision weapons, and technologies would fundamentally change advanced military operations. U.S. battlefield dominance in Gulf War I validated Marshall's vision. See Zalmay Khalilzad, John White, and Andrew Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND, 1999

[118] Government of India, *Report of the Group of Ministers on National Security*, Chapter II, "Challenges to the Management of National Security," February 2001, p. 9

[119] Ibid Government of India, p.13

[120] Thomas G. Mahnken and Timothy D. Hoyt, "Indian Views of the Emerging Revolution in Military Affairs," NSSQ, Summer 2000, p. 15

Intended transformation in India's strategic doctrine and military operational art complemented the sweeping changes in the information technology economy that began in the early 1990's. Toward the end of that decade, India's IT sector internationalized for example through the U.S. IT industry's joint investment ventures with offshore companies to develop software. Manufacturers in India were logical partners for U.S. companies because the sub-continent offered a supply of well-trained, low-cost labor.[121]

3.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

Military analysts in the U.S. and elsewhere today emphasize a generalized shift in doctrine away from traditional methods of combat toward tactics and weapons designed to produce dominance in the information "battle space." Such dominance could embrace either offensive information operations or steps to protect domestic assets and critical infrastructures against "cyber threats—or both."[122] India represents a relevant case study.[123]

India's defense establishment in the late 1990s grasped the importance of the digital revolution and its relevance to the military operational art.[124] The Report of the Group of Ministers on National Security noted in early 2001:

> The future battlefield in [the Indian] context is likely to be more digitized and transparent and would experience an exponential increase in the deployment of electronic devices, signaling the growing primacy of the electromagnetic spectrum…Thus while India needs to ensure credible nuclear deterrence…it has to simultaneously maintain adequate and duly modernized conventional forces which are properly managed, led and equipped to take advantage of the RMA and which can take care of any possible conventional conflicts."[125]

The Indian Army formally announced a shift in doctrine in 1998 to embrace electronic warfare and information operations capabilities. This new doctrine, or IT-Roadmap, enumerates ambitious plans up to 2008. These plans encompass hardware, software, and human resource

---

[121] Radha Roy Biswas, "Hyderabad-Technopolis in the Making?," Master of Arts Thesis, Department of Regional Economic and Social Development, University of Massachusetts, Lowell, 2001 p. 18. A further study on the Indian software industry attributes a significant role to Indian hi-tech professionals working in the U.S. The study argues that this group helped drive outsourcing and offshore location decisions among U.S. firms in India. Study by Arora et. al., titled *India Software Services Industry*, cited by Radha Roy Biswas, op. cit., 2001, p. 18

[122] "The Indian government is doing a lot of research on [Information Warfare]. Simply, the warfare is the use of information to achieve national objectives…Military dominance depends on speed and range. In the networked world you have both. Images can be manipulated and data is vulnerable." B.V. Naidu, Director, Software Technology Parks India, *Curz Tech News Network*, from India Express Bureau, January 21, 2003

[123] According to a declassified threat assessment in the U.S. Navy's Strategic Planning Guidance published in 2000, "Russia, China, India, and Cuba have acknowledged policies of preparing for information warfare," while "North Korea, Libya, Iran, Iraq, and Syria have some capability." John M. Donnelly, "Navy Names Nations Posing Cyber Threats," King Communications Group, Navy News Week, September 11, 2000, p. 1 A parliamentary democracy, India's military plans and priorities are relatively transparent.

[124] For example, see the discussion in "Deterring Information Warfare: A New Strategic Challenge," by Timothy Thomas, Winter 1996-1997. For a brief, general account of doctrinal discussions in India, see "Army: Now Hyper War," *India Today*, May 10, 1999

[125] Government of India, "Challenges to the Management of National Security," in *Report of the Group of Ministers on National Security*, 2001

development, with a goal of "enhancing the IT quotient" per soldier.[126] According to one of the architects of the new doctrine, Army Chief of Staff General V.P. Malik, the Roadmap is intended "To establish a strong information technology infrastructure to act as a force multiplier by incorporating fully automated and networked operational and management information system [sic], complemented by fully information technology literate manpower."[127] Assumptions behind this initiative are:

- Software rather than hardware is increasingly critical to adding value in related industries
- Industry standards are becoming more open and uniform worldwide, allowing easier market entry and innovation
- Global competitiveness and ease of transnational communications translates into faster improvements in products, architecture, and infrastructure.

General Malik has remarked that "computing is about openness, so why build and write code that can be bought off the shelf?" In addition, partnership and networking with industry can produce synergies. "The Army would prefer to enter into a long-term understanding with the information technology industry so that we can work in tandem towards a common goal."[128]

3.3 FOREIGN MILITARY AND INTELLIGENCE AGENCY RESEARCH

Contemporaneous with the military's plan to adopt an IT-roadmap, the defense industries production sector in India has instituted parallel reforms.

Prior to 2000, military production and procurement were confined to government-owned companies for ideological and security reasons. In recent years, however, the armed forces have become more open to public/private sector collaboration in the defense sector. The military has learned that technologies developed by private industry (such as encryption) may strengthen security. As an Indian military officer recently commented, "We are heavily into cyber security now and are in the process of creating a security envelope since the most advanced armies in the world face 3,000 to 4,000 attempts to hack their networks."[129]

In response to a multi-year campaign waged by the Confederation of Indian Industry (CII) requesting a share of the contracts previously reserved for public sector firms, the Minister of Defense and the CII's National Committee on Defense decided in 2000 to "establish a strong partnership between defense and industry to enlarge the role and scope of Indian industry in defense."[130] Accordingly, the Ministry of Defense and the CII formed six Task Forces: Long-term partnership; commercial process; Defense Research and Development Organization

[126] Rajat Pandit, "Army Logs on to E-Highway to Beat Enemy in IT Race," *The Times of India*, September 30, 2002
[127] General V.P. Malik, "The Thinking Soldier," from *Rediff*, September 21, 1998
[128] Ibid Malik 1998. Reportedly, General Malik's mantra is, "Cyber warfare is to the 21st Century what blitzkrieg was to the 20th."
[129] Op. cit. Rajat Pandit 2002
[130] CII National Committee on Defense, "About the CII National Committee on Defense," 2002 <http://www.ciidefence.com/general/about.htm>

(DRDO)-Industry partnership; Defense Public Sector Undertakings-Private Sector complementary; IT for Defense; and Strategy for Defense Exports. In a May 2002 briefing titled "Indian Defense Market: Opportunities for Private Investment", the CII Chairman listed three "modernization thrusts: Information technology and information warfare; electronic warfare and C4I2 [command, control, communications, computer, information, and interoperability] infrastructure; and mobility."[131] The briefing explains that the government has invited private sector participation because private producers offer modern technologies, efficiency and after-sales service, and lower costs through market competition. In a related statement, the CII Chairman said he expects "a large number of reputed companies to look towards defense not just as a supplier of defense products but as a partner in building a stronger and self-reliant armed force."[132] Reportedly, he went on to suggest that the government, jointly with the industry, should formulate product and supplier development strategies.

3.3.1 TRAINING

The Army's IT roadmap, promulgated in 1998, asserts that all its officers and junior leaders will become computer literate by 2002. In 1999, the Army Institute of Information Technology introduced its first course at its temporary campus in Hyderabad to teach war fighters the rudiments of IT warfare.[133] Simultaneously, three army technology institutes, two in Secunderabad (in Andhra Pradesh) and one in Pune (in Maharashtra state) began to introduce IT as part of their syllabus.[134] The Ministry of Defense in New Delhi is now considering a report, submitted in early 2002, calling for a thorough overhaul of defense management and research, education, and training in India's military services. Reportedly, the linchpin of the recommendations under consideration is the creation of a National Defense University (NDU) in New Delhi.

One of the focal points of the NDU will be information warfare and the digital revolution. According to a journalistic account, "The University will try to change the way our soldiers think and learn. All joint service organizations like the National Defense Academy…the Defense Services Staff College…and the Center for Defense Management…and the National Defense College…will be brought under its purview."[135] Media reports regarding the recommendations indicate the NDU will house a National Institute of Strategic Studies. Reportedly, the latter Institute will be a "research organization with a futuristic view." It will host a war gaming and simulation department. In addition to the armed services, civilian organizations, including the intelligence services, will be allowed to join the Institute. [136]

---

[131] "Indian Defence Market: Opportunities for Private Investment," PowerPoint briefing by Atul Kirloskar, Chairman, CII National Committee on Defense, May 8, 2002

[132] Rediff.com, "Top Indian Firms Must Enter Defense Arena: CII," June 12, 2002 <http://www.rediff.com/money/2002/jun/12cii.htm>

[133] "Army: Now Hyper War," *India Today*, May 10, 1999

[134] This improvement in training was foreshadowed in the comments of General Malik in 1998: "We have been imparting training to our officers and men at various training institutions. Select officers have been doing advanced training in computer sciences at the IIT's [Indian Institutes of Technology]. But this is not enough. We have therefore decided that to accelerate the process we need to work out training packages with some commercial firms like NIIT and Aptech and open our own institution of information technology in Secunderabad for advanced learning as wells [sic] application in our systems."

[135] "War Game Dept Three Years Away," *The Statesman* (India), June 3, 2002

[136] Ibid *The Statesman* 2002

According to media reports, the National Defense Academy (NDA) in Pune in June 2002 graduated its first group of students earning the degree of Bachelor of Science in computer science. Media sources say the three-year course is consistent with the latest trends in electronic warfare and growing computerization in the armed forces. A top graduate, Cadet Vishal Jain, told a reporter, "From decoding intercept signals of the enemy to the use of sonars/radars, IT has an important role to play in modern-day warfare." Jain explained that the "three year course included training in computer architecture, language principles of programming, network, system analysis and database management system.[137]

Other NDA cadets, who opt for the regular B.A. degree, reportedly are required to enroll in a three-semester computer course conducted at the Center for Development of Advanced Computing (C-DAC) in Pune.[138] C-DAC's mission, as described on its Website, is to emerge as the premier R&D institution for the "design, development, and deployment of world class IT solutions…" In addition to high performance computing and communications, the Center's areas of interest embrace multilingual technologies, multimedia, education and training, and eGovernance.[139]

The Indian military is investing significant resources to develop information technologies and to train technologically capable forces. Private companies have developed programs to integrate their technologies more directly into the defense sector's needs. Further, the Defense Research and Development Organization has initiated several programs for the development of critical technologies and systems under government auspices, including chip development. The National Defense University will centralize information warfare training and simulations for the Armed Forces and the intelligence services.

The Central Bureau of Investigation (CBI) is responsible for criminal and counter intelligence matters. The National Cyber Cop Committee, established by the software industry association in early 2001, includes representative police officials from all states in India, the CBI, and the Ministry of Home Affairs. It conducts workshops for judicial and police officers to explain various Internet-related crimes. The committee also researches methods and solutions to prevent intrusions into government websites. According to a 2002 report, the Ministry of Technology and the Central Bureau for Investigation have developed a diverse national strategy to protect India's infrastructures. This strategy recommends "involving assistance from software industries" where necessary.

In addition, the U.S. and India have set up a Cyber Security Forum to provide a conduit for an exchange of information on cyber threats. The forum fosters bilateral discussions on civilian and military infrastructure protection, legal cooperation and law enforcement, security standards, and research and development.[140] According to a September 2003 report, the CBI and the U.S.

[137] "NDA Cadets Now Computer Savvy," *The Times of India*, June 6, 2002
[138] National Defense Academy curricula are described under "Interservices Institutions," at <http://armedforces.nic.in/interservice/isindia1.htm>
[139] Center for Development of Advanced Computing, <http://www.cdacindia.com>
[140] "Hackers Take Kashmir Dispute to Cyberspace," *Jane's Intelligence Review*, October 1, 2002

Federal Bureau of Investigation completed a joint training course in New Delhi embracing "instruction on advanced cyber techniques used by some terrorist groups…"[141]

3.3.2 OPERATIONS

Pakistani intelligence services are paying Western hackers $500-$10,000 to deface Indian websites, according to Ankit Fadia, an Indian computer security consultant. Pakistani hacktivist groups, he says, are defacing at least 60 Indian sites monthly. "Targets include government and business sites, including VSNL, India's oldest and largest Internet Service Provider, and even those of non-government organizations. Those that have been attacked include Infosys and Satyam, Indian headquartered IT companies, an Indian oil company, and the Ministry of Information Technology."[142]

Although computer hacking is considered illegal under Indian jurisprudence, India's computer professionals have nonetheless established hacker groups to defend and retaliate by attacking Pakistani websites. According to a report in the Indian press, Indianspy, a hacker claiming to represent the Indian Hackers Club, defaced 8 Pakistani websites in mid-2003 and posted messages ridiculing pro-Pakistani hackers who have been targeting Indian websites. Indianspy targeted the website of Comsats, an ISP provider in Pakistan.[143]

The National Cyber Cop Committee reportedly receives advice from a group of teen hackers. According to the president of the association, the teens will "tell us where our soft spots are—where government and industry websites are most vulnerable, thus helping strengthen our e-security."[144]

Recently, India's military intelligence gathering institutions underwent a significant restructuring in response to perceived intelligence failures in connection with the 1999 Kargil intrusions by Pakistan. In early 2002, on the recommendation of a Ministerial-level group under Home Minister Advani, a Defense Intelligence Agency (DIA) was established to coordinate the directorates of Army, Naval, and Air Force intelligence. According to a journalistic account, the DIA will be responsible for executing cross-border operations and collecting tactical intelligence in neighboring states through human sources. DIA is also being given responsibility for the Signals Intelligence Directorate and the Defense Image Processing and Analysis Center (reconnaissance through satellite imaging).

Unconfirmed reports indicate that the armed forces plan to establish an information warfare agency under the tri-service integrated defense staff within the DIA. The new agency, called the Defense Information Warfare Agency (DIWA), will manage all aspects of IW, such as psychological operations, cyber war, and electromagnetic and sound waves. According to a

---

[141] "Indian Authorities Join the FBI on Training to Fight Terrorism," *Aviation Week's Homeland Security and Defense,* September 25, 2003

[142] S. Dreyfus, "Hacktivism Through the Eyes of an Infiltrator," *The Age* (Melbourne), August 5, 2003

[143] "Indo-Pak. Cyber War Continues," *The Hindu*, July 13, 2003, <http://thehindu.com/2003/07/13/stories/2003071303800900.htm>

[144] BBC News, "Teen Hackers Turn Cyber Cops," January 3, 2001 <http://news.bbc.co.uk/1/hi/world/south_asia/1099181.stm>

February 2003 account, "DIWA will be the nodal agency that will make policies for all the three services as well as formulate countermeasures to enemy propaganda."[145]

The Research and Analysis Wing (RAW) is India's civilian foreign intelligence gathering agency. RAW, whose structure and operations are not disclosed to parliament, reportedly reports to the Prime Minister's office and has played a key role in espionage and disinformation campaigns against Pakistan and other neighboring countries.[146]

In early 2003, India's intelligence agencies announced the establishment of a National Technical Intelligence Communications Center (NTICC). The purpose of this body, which is a sub-unit of India's intelligence Research and Analysis Wing, is to provide technical and electronic intelligence to the Intelligence Bureau and the Defense Intelligence Agency. According to Jane's Intelligence Review, the NTICC will focus on intercepting communications among Kashmiri terrorists now employing mobile Thurya handsets. In the future, the communications center plans to develop an interception capability modeled on the Echelon system attributed to the U.S. Department of Defense.[147]

A separate report states that this specialized intelligence gathering agency will act as a "super feeder agency for providing technical intelligence to other agencies on internal and external security…The organization will do hi-tech surveillance jobs, including satellite monitoring, terrestrial monitoring, Internet monitoring, considered vital for the national security apparatus."[148]

3.4 INFORMATION TECHNOLOGY INVESTMENT

Overall, as described above, the Indian government has elaborated a comprehensive strategy that integrates information technologies into its military. The armed services have developed IT roadmaps that lay out long-term requirements for new technologies as well as the human resources necessary to employ them. The government has forged new models for public / private sector collaboration. Changes in military thinking and loosening of formal and informal restrictions on joint manufacturing ventures will probably pay off in technological advances in the coming years.[149]

---

[145] "Info Warfare for Armed Forces," *Indian Express*, February 28, 2003 and "India Moves to Counter Pakistani Propaganda," Pakistan *Daily Times*, <http://www.dailytimes.com.pk/default.asp?page=story_1-3-2003_pg4>

[146] Federation of American Scientists, "Research and Analysis Wing [RAW]," July 26, 2002 <http://www.fas.org/irp/world/india/raw/>

[147] "India Revamps Intelligence Agencies," *Jane's Intelligence Review*, May 1, 2003

[148] "New Intelligence Agency Set Up," *The Pioneer* (New Delhi) April 7, 2003

[149] According to informed observers, there was a traditional reluctance in the defense establishment to work closely with private industry on "sensitive" military projects. An article published in June 2002 quoted Army Lt. General Singh as follows: "IT professionals in India are some of the most competent people in the entire IT world. Yet, our armed forces shy off from using this talent. This could well be because they do not appreciate the full force of IT or they erroneously believe that it would compromise security." <http://www.expresscomputeronline.com/cgi-bin/ecprint/MasterPFP.cgi>

Until recently, India's political establishment appeared mired in a sclerotic business culture resting on government guidance and inefficient defense/public sector undertakings. According to reliable reports, significant change is under way in this sector.[150]

Several reports comment on the defense sector's potential to leverage the IT software industry in India. For example, Bharat Electronics Ltd. (BEL), reportedly India's "premier" electronics organization dedicated to the development and manufacture of state-of-the-art electronic equipment for use by the armed forces and paramilitary organizations, inaugurated a military software development center in 2002, initially employing 60 professionals.[151] By 2003, the number of employees making "embedded software" rose to 100.[152] BEL's website indicates that the firm strives to retain technological leadership through in-house research as well as through collaboration with Defense Labs, foreign companies, universities and research institutes. BEL also plans to increase overseas sales of its products.

With respect to private enterprise and India's domestic IT infrastructure, the sub-continent is emerging as one of the principal global players in the Info-Tech sector. Software development is India's fastest-growing foreign exchange earner. Technical research and education institutions such as Indian Institutes of Technology and the Tata Institute of Fundamental Research are second to none. Leading institutes linked to defense, space, financial, and development projects continue to provide exemplary research.[153]

Historically, India was slower than many countries to embrace the digital era. In 1984, the central government in New Delhi initiated measures to loosen bureaucratic controls and promote private initiative, especially in selected "target" industries such as telecommunications and computers. These actions were taken because official government licensing requirements deterred start-up enterprises. In the early 1990's, regional policy makers at the state level, such as in Andhra Pradesh, boldly embraced the software development sector, yet the central government continued to vacillate. Internet access was extended outside academia through the central government's official telephone monopoly VSNL project and a few public-sector industries adopted information technologies. However, the central authorities resisted the global trend toward privatizing the telecommunications backbone. While expansion of the IT sector is hampered by such legacies as limited bandwidth, low PC penetration, and relatively low telephone density, considerable improvements have been made recently. [154]

[150] GoIndiaGo.com, "Defence," <http://www.goindiago.com/general/defence1.htm>
[151] Bharat Electronics "BEL Website- Home," <http://www.bel-india.com>
[152] "Software for Warfare," *India Business Insight*, September 20, 2002
[153] Op. cit. Radha Roy Biswas p. 13
[154] According to the CIA's *The World Factbook* (2004), India reported more than 86,000 Internet hosts in 2003 (computers connected directly to the Internet) and over 18 million Internet users. Mobile cellular telephony was introduced in 1994, arranged nation-wide into 4 metropolitan cities and 19 telecommunications circles each with about 3 service providers. In 2003, there were more than 26 million mobile cellular users. Additional trunk capacity has been added in the form of fiber optic cable, while India possesses the world's largest domestic satellite system.

3.4.1 INDIA'S IT INFRASTRUCTURE

India's overall performance in the IT sector is mixed, despite success in software development.[155] This stems primarily from obsolete technical infrastructure and inadequate investment in the communications sector.

According to a recent academic analysis, Internet expansion depends upon availability of several factors including the telecommunications infrastructure, networking engineers and end users, networking and end user hardware, and government leadership.[156] The following paragraphs characterize India's IT infrastructure along these four dimensions.

Infrastructure: India's telephone network backbone historically has been limited in size and reliability. Although changes are ongoing, the sub-continent continues to lack a fiber optic backbone for high-speed data communications. Moreover, VSNL, the state monopoly in international telephony and domestic Internet service, has inflated the cost of IT services. A report released in 2001 indicates that 500 hours annually of dial-up service can cost $200 for a slow speed connection.[157]

Engineers: The Indian government has a long tradition of support for technical education. The sub-continent is a significant exporter of engineers and scientists. According to one source, Silicon Valley boasts numerous Indian millionaires and American immigration rules have helped Indians disproportionately. Small groups of skilled engineers, working indigenously, are reportedly largely responsible for India's internationally competitive computer software industry.[158]

Networking and end user hardware: Traditionally, IT manufacturing has been a protected industry in India. With respect to computer hardware and peripherals, manufacturing growth in the 1990's was reported to have been limited due partly to minimal growth in the domestic market and partly to the inability of the volume-limited manufacturers to be competitive. When foreign investors attempted to enter the Indian market, New Delhi's lack of intellectual property protection posed problems.

Government leadership: Until the early 1990s, New Delhi's slow moving government bureaucracy and other factors impeded progress in the IT field compared to neighboring countries such as China. Building on India's formidable human resources in the computer and engineering fields, the government in the early 1990s invested in Software Technology Parks and other programs to spur development of the intellectual property. These efforts, supported by reform-minded state governments, introduced a policy environment conducive to growth.

---

[155] See the Outsourcing and IT enabled services section of this chapter

[156] Larry Press, et. al., "The Internet in India and China," 1999 <http://www.isoc.org/isoc/conferences/inet/99/proceedings>

[157] Estimated GDP per capita in 2002 was $2540. Source: CIA *World Fact Book,* 2003

[158] Robert R. Miller, "Leapfrogging? India's Information Technology Industry and the Internet," IFC Discussion Paper Number 42, The World Bank, Washington DC, 2001 p.2

3.4.2 INFORMATION TECHNOLOGY ACTION PLAN…

Recognizing that the country risked falling behind in the global IT race, the Indian Prime Minister convened a National Task Force on Information Technology and Software Development. The Task Force report published in 1999 proposed a three-part program to liberalize the telecommunications industry and transform India into a "global IT superpower."[159] The three categories for transformation were:

1. Accelerating the creation of an IT infrastructure
2. Establishing policy and regulatory environment to boost software exports to $50 billion by 2008
3. Extending the use of IT to all segments of society.[160]

3.4.3 …PROMISES INFRASTRUCTURE IMPROVEMENTS

The Common Action Plan to Promote IT in India, adopted in mid-2000, calls for a national high-speed network backbone, expansion of the Internet, rise in PC-penetration, and "localization" of Indian languages.[161] The government reportedly will allow entry of foreign investors interested in expanding available bandwidth, permit private companies to lay underwater cables for the Internet, and permit ISPs to establish international gateways and lease bandwidth on foreign satellites. [162]

Private industry is also engaged in expanding terrestrial Internet infrastructure. According to a recent study, Reliance Group is laying optical fiber cable in 16 Indian states, linking 115 cities over a length of 60,000 kilometers. BSNL, the large public sector telephone service provider, reportedly has awarded licenses to 14 entities allowing them to provide optical fiber cables, right-of-way towers and infrastructure for end-to-end connectivity throughout the sub-continent.

---

[159] The National Task Force on IT and Software Development was appointed May 22, 1998. Its mandate was to formulate the draft of a National Informatics Policy. For the details of the Task Force Report, see <http://www.IT-taskforce.nic.in>

[160] Among the specific recommendations are: proposals to accelerate depreciation on all IT products, advance the date for achieving zero import duty on IT products, create at least four venture capital funds, and implement measures conferring priority consideration by banks in loan and export financing approval. The Task Force also proposed: abolishing VSNL's [government-owned datacenter and Internet service provider] monopoly over international communications; authorizing access to the Internet through cable TV to any service provider without additional licensing; and permitting railways, defense, power grids, and various state electricity boards to host fiber optic backbones. "India Task Force Draws IT Roadmap," *Newsbytes,* July 14, 1998

[161] See Lieutenant Commander Prashant Bakshi, "Security Implications for a Wired India: Challenges Ahead" in *Strategic Analysis*, Vol. XXV, No. 1, April 2001, p 2. Hindi is the national language, spoken by only 30 percent of the population. There are 14 other "official" languages. Because the local language market is fragmented, English is the most important for national, political, and commercial communication. Larry Press, et. al., op. cit., p. 9

[162] Robert R. Miller, "Leapfrogging? India's Information Technology Industry and the Internet," IFC Discussion Paper Number 42, The World Bank, Washington DC, 2001. With respect to international connectivity, India has access to: eight Intelsat and one Inmarsat satellite earth stations; nine gateway exchanges (Bombay, New Delhi, Calcutta, Madras, etc.); and four submarine cables, with links to Penang and to the UAE, for example. Source: CIA *World Factbook*, 2002

This embraces public sector companies, such as railways and utilities, enjoying right-of-way for existing infrastructure.[163]

1. Internet

Due to low per-capita income, weak telecoms infrastructure, lack of a high-speed backbone, non-competitive telephone tariff charges and other factors, Internet development is at an early stage in terms of the number of connections and overall use. [164] Nevertheless, in the interval 1999-2000, the number of ISPs reportedly rose from 15 to 90 (a six-fold increase).[165]

Experts predict that most practical communications benefits for the foreseeable future are likely to derive from business—not consumer—use. In particular:

"Global connections will be much enhanced by India's liberalized access to international Internet gateways and to privately-provided undersea cable access. This access alone could offer India's companies opportunities that otherwise would flow to other better connected Asian competitors."[166]

2. Software Development Industry

India's annual software sales revenues rose dramatically from approximately $1.7 billion in 1996-97 to an estimated $5.7 billion in 1999-2000. The latter figure constitutes about 65 percent of total IT revenues. By contrast, hardware and peripherals account only for about 23 percent. The share of the total attributable to international sales has risen commensurately. According to the software industry association, in 1999-2000 nearly 70 percent of India's software revenues derived from exports. The U.S. accounts for approximately 60 percent of the software export market.[167]

The spectacular growth of India's software industry stems from a variety of sources, such as IT-hubs, qualified leadership, and the availability of well-educated labor willing to work for a fraction of the cost similar workers earn in the client's home country. (For a discussion of Software Technology Parks, see Figure 2).

A study published in the monthly journal of the Institute for Defense Studies and Analyses (IDSA) states that India's software industry has been growing from "strength to strength." Y2K reportedly was a turning point. The run-up to 2000 saw Western nations seeking Indian software professionals to solve anticipated problems. The Indian software industry earned an estimated $2.5 billion from Y2K business (between 1996 and 1999). Key economic indicators are as follows:

[163] Bakshi, op.cit, p. 3
[164] According to a report disseminated in 2001, in a population of 1 billion, there were fewer than two million Internet subscribers. Source: Miller, op. cit. p. 3
[165] Bakshi, op. cit., p. 3
[166] Miller, op. cit., p. vii
[167] Ibid p. 19

- Over the five year period 1996-2000, India's IT industry had a compound annual growth rate averaging 40.5 percent, almost double the growth rate of the industry in many developing countries;

- Software exports in 1999-2000 amounted to $4 billion, accounting for over 10 percent of India's total exports;

- Sales of PC desktop units attained 1 million units in 1999-2000, and the domestic hardware share grew by 58 percent;
- Among the Fortune 500 companies, 185 outsourced their software requirements to India in 1999-2000;

- Among the 23 software companies in the world with Carnegie Mellon Software Engineering Institute certification, 16 are based in India;

- Key software firms, such as Infosys, Wipro, and Satyam Computers, are listed on the NASDAQ.[168]

Figure 2: Software Technology Parks[169]

The southern software centers, Bangalore in Karnataka state, Chennai (formerly Madras) in Tamil Nadu, and Hyderabad in Andhra Pradesh, constitute the so-called "Silicon Triangle of India." Other important hubs include Mumbai (formerly Bombay) and New Delhi.
In the 1990's, the central government established the Software Technology Parks of India, a visionary project to provide infrastructure and administrative support, including reliable high speed access, for software development companies.

Hyderabad Software Industry

Software Technology Parks of India, Hyderabad was established in 1991-1992. Registration of firms in the Park rose from "a handful" in 1991 to over 1000 in 2000, and to approximately 1400 in 2002. In the early 1990's the Park's business grew at an annual rate of 100 percent. In 2000-2001 and 2001-2002, the annual growth rate tapered off to 81 percent and 42 percent, respectively. [170]

Exports: Export revenues grew from less than $1 million in 1992 to nearly $250 million in 1999-2000.[171] In 2002-2003, export revenues attained 3,668 crores (equivalent to approximately $700 million), an increase of 26 percent over the previous year. A recent press note indicates that 820 out of more than 1,400 entities in the Park are contributing to exports. Info-Tech Enabled

[168] Source: Bakshi, op. cit., p. 2
[169] Much of the information in this figure derives from Radha Roy Biswas, op. cit.
[170] Entities at STPI Hyderabad develop a wide range of software. The last two years have witnessed the launching of several embedded systems and VLSI design companies.
[171] Reportedly, software exports exploded after the installation of a Satellite Earth Station at Hyderabad in 1991 with the assistance of STPI (Software Technology Parks of India) and the government of Andhra Pradesh. STPI Hyderabad Press Note, May 5, 2003, p. 1

Services (ITES) exports, such as business process outsourcing and call centers, are increasing and now account for about 40 percent of total revenues. The number of professionals engaged in export firms in the Park rose to about 64,300 in early 2003.

The distribution among types of exports in 2003 is as follows: Approximately 79 percent through datacom facilities, 20 percent through consultancy projects, and the remainder through physical media. According to STPI, the value of software exports through datacom facilities is expected to rise in response to increased bandwidth, access to new markets, and increased outsourcing to India. Although most of the exports in 2002 were directed to the U.S. and Canada, Europe, Japan, Australia, Asia, and the Middle East also are destinations.

Outsourcing: Hyderabad is emerging as a fast growing hub for outsourcing. In 2002-2003, companies such as Nipuna, Dell, 24/7, Cognizant, Activecard, Click2learn, Swift Reponse, and Redpine Signals, Inc., established a presence in the Technology Park.

3. Outsourcing and IT enabled services

Outsourcing, according to a 2003 article in CIO Magazine, is "one of the best ways for CIOs to cut application development and maintenance costs…" Reportedly, between 50 and 67 percent of all Fortune 500 companies currently outsource to the Indian sub-continent, although many at this stage are only undertaking pilot projects. IT-enabled services (ITES) embrace call centers, medical transcription, data digitization, and web content development and animation, and are expected to grow substantially.[172]

According to a World Bank study, in 2000 India employed between 50,000 and 100,000 workers in IT-enabled services, producing about $500 million in export earnings. The amount of software services work performed in India for U.S. companies was expected to double in 2003.

Summarizing, one study notes that "The Indian IT industry is largely software service and export oriented, and often, the term "Indian IT industry" is used synonymously with the Indian software industry."[173]

According to a study by the Stanford Computer Industry Project, India's formidable human resource base historically drives national software strategy. Its world class technical training bodies, such as the Indian Institutes of Technology and the Tata Institute of Fundamental Research, also played a pivotal role.

Figure 3: Cyber Security Efforts

The Ministry of Information Technology decided in 2003 to establish a $20 million Internet security center in New Delhi. The center—supported by CERT at CMU—addresses computer security incidents, publishes alerts, and promotes information and training. Software

[172] Stephanie Overby, "Inside Outsourcing in India," *CIO Magazine*, June 1, 2003 <http://www.cio.com/archive/060103/outsourcing.html> and *Middle East News On-line*: Iran News, July 28, 2002

[173] Radha Roy Biswas, op. cit., p. 12

Technology Parks India (STPI)—an autonomous body of the government—has a stake in the proposed center. [174]

The Center for Development of Advanced Computing (C-DAC) and the DRDO have been at the forefront of information security technologies. The Networking and Internet Software Group of the C-DAC, for example, is working on the development of "core network security technologies," which include C-DAC's Virtual Private network, crypto package, and prototype of e-commerce applications.[175]

FIRST-India (Forum for Incident Response and Security Teams) is a non-profit organization for facilitating "trusted interaction amongst teams from India conducting incident response and cyber security tasks. Membership is open to private and public sector organizations in India, including the Defense Public Sector Undertakings.[176]

India's efforts to enhance and restructure technical intelligence collection, give greater prominence to information warfare operations, and permit private sector participation in defense and military contracts constitute an expanding web of connections in the evolving national security picture. However, leadership and expanding market share in the global software industry represents a double-edged sword with respect to India's national security. On the one hand, an emerging national software export strategy centered on military hi-tech spin-offs (i.e., patterned after current practice in Israel) promises to extend the benefits of state-of-the art technology while creating economic growth. On the other hand, the more ubiquitous indigenous computer software becomes and the more India's national security depends on it, the greater is the potential vulnerability to malicious intrusion or tampering.

India's prominence in the IT field (as both software developer and exporter) together with the government's announced plans to modernize the Indian armed forces have spawned significant military, business, and academic ties with entities in a host of countries, including the United States. India's Prime Minister, in a June 2003 visit to Shanghai, proposed that "Indian and Chinese firms work together" in the IT software sector.[177] Scientific and technical trade and cooperation links with Russia and Israel are of particular interest with respect to developing or enhancing New Delhi's electronic warfare and information operations.

Russia, an acknowledged leader in cyber warfare matters, has enjoyed close cooperation with India in computer research going back to the Soviet era. New Delhi's Department of Science and Technology and Russia's Academy of Sciences have sponsored and facilitated several

[174] AFP, "Region: India to Establish $20 million Internet Security Center," *Daily Times* (Pakistan), January 21, 2003 <http://www.dailytimes.com.pk/default.asp?page=story_21-1-2003_pg4_12>

[175] Nanda Kasabe, "C-DAC Foraying into Network, Internet Security," Cyber News Service, September 22, 2000, as cited in "Security Implications for Wired India: Role of Technology" by Prashant Bakshi. As the editor of defenceindia.com, Rajesh Dixit observes, "Although there is a chance of hackers doing some damage, they cannot affect equipment because they have standalone computerized systems…However, anything on a network or dependent on satellite –based functioning can be affected."

[176] See FIRST, "Forum for Incident Response and Security Teams," <http://www.firstindia.com>

[177] Muzi News, "Indian PM Proposes Info-Tech Alliance with China," Reuters, June 26, 2003 <http://dailynews.muzi.com/ll/english/1267646.shtml>

bilateral research efforts for more than a decade. India's Center for Development of Advanced Computing (C-DAC) and Russia's Institute for Computer Aided Design formed the RICCR (Russia-India Center for Advanced Computing Research) in late 2000. According to information posted on the RICCR website, the Center promotes and facilitates collaborative research in the following areas: software development for high-speed computers with parallel architecture; program codes; ecology, geology, and seismic data processing; weather forecasting and climate modeling; economics; and computer satellite systems, among others. India C-DAC has committed its PARAM super computer to this cooperative research.[178]

More recently, Moscow and New Delhi have taken active measures to strengthen traditional ties in the military defense and armaments field. In approving opportunities for cooperation in information and communications technologies, biotechnology, electronics, banking and financial services, the two sides have decided to address potential complementarities in the emerging global economic system.

3.5 CONCLUSION

The main thrust of the data presented is that India's armed forces have initiated a shift in military doctrine to embrace more directly offensive and defensive cyber warfare, leveraging India's strengths in IT research and software development. India has a robust hacking network. In addition, the government has announced several operational steps, such as founding a National Defense University with a key focus on computer software, and establishing a new intelligence communication and electronic surveillance agency. In parallel with these steps, India's traditional pre-occupation with protecting military secrets has given way to closer government/industry collaboration to keep pace with competitive challenges within the region and at the global level.

New Delhi actively seeks military-technical and scientific cooperation and exchange with strategic partners such as Israel and Russia that reputedly possess exceptional cyber capabilities. In addition, there is significant open discussion relating to adoption of the Israeli model of military/industry strategic cooperation, i.e., a national software export strategy centered on product-supplier relationships and military hi-tech spin-offs.

As noted earlier in this chapter, much of the computer software industry in India is clustered in "Technology Parks" in a few of the principal cities, such as Bangalore, Chennai, and Hyderabad. Security protection is relatively robust because of the importance of the industry to the overall Indian economy.

[178] See "Russian-Indian Centre for Advanced Computing Research," 2004 <http://www.cdacindia.com/html/misc/riccr/riccr.asp > and "Russian-Indian Centre for Advanced Computing Research," 2004 <http://www.riccr.com/main-e.htm>

Public and private sector interests in India accord priority to cyber security issues and concerns and during the last several years have implemented significant policy measures to address them.[179]

With more software used to run infrastructure and commerce in the advanced economies being "outsourced" to India and other developing countries, the risk of unauthorized intrusions or programming compromises rises. A malicious intrusion scenario, for example, might entail rogue employees in India's software development industry tampering with code to insert a back-door or "time bomb."

[179] In 1999, for example, the DRDO and the Central Vigilance Committee (CVC) issued an alert, warning Indian organizations about buying foreign network security software. Thereafter, it became mandatory for banks and financial institutions in India to procure indigenous software products.

IV. IRAN

CHARLES BILLO

The United States jams our radar systems; this is part of their Satanic behavior with their huge array of technological capabilities. We would not be surprised if they do it again. We have to find ways to get electronic counter-countermeasures (ECCM). We have taken certain measures to produce ECCM equipment.

1989 Interview with "Head of the Electronics Industry" in Iran in
Military Industries in the Islamic Republic of Iran: Assessment of the Defense Industries Organization
John M. Shields May 1996

Taking into consideration that the government…has been planning for development of information technology and communications in Iran, this issue has attracted the attention of the defense sector in the past and at the moment…Due to the interest of the defense sector in these fields, a university complex will be established to gather the necessary manpower. Along with that, all capabilities in information technology and communications manufacturing in software education and infrastructure and research are concentrated in the defense sector…

Iranian Defense Minister Ali Shamkhani
Malek Ashtar University of Technology Speech February 2003

The Farsi language broadcasts by the VOA as well as Los Angeles-based ParsTV and Appadana TV are uplinked in the United States via Telstar-5…It is then turned around at Washington International Telport in Alexandria, Va., and uplinked again to Telstar12 over the eastern Atlantic Ocean…It is Telstar-12 that is being jammed, say investigators for companies working with the broadcasters, cutting off broadcasts not only in Iran but in Europe and the rest of the Middle East as well…A representative of one of the Iranian-American broadcasters said he suspected the jamming came from Cuba, which has excellent relations with Iran, but offered no proof.

Robert Windrem, NBC News, July 2003

Iran's civilian Information and Communications Technology (ICT) culture is highly complex. The government, cognizant of the importance of the knowledge sector and the efficiencies associated with the Internet, is determined that Iran will not be excluded from the global Information Technology economy. The educated and generally literate populace, aware of external cultural developments and trends through contacts with the Iranian diaspora and through foreign travel, clamors for access to information and entertainment. Internet service entrepreneurs chafe at the antiquated and obsolescent telephone infrastructure. Conservative elements of the clerical regime nevertheless fear that unfettered access to information will lead to unrest and potential resistance.[180]

Telecommunications and Internet services in Iran generally are considered rudimentary compared to leading countries in the Persian Gulf region. One expert attributes Tehran's failure to realize its full potential to "internal religious and political contradictions."[181]

[180] For a general discussion of the complexities of the IT regulatory system "culture" in Iran, see "Internet, Mobile, and Satellite in Iran," Noruouz, September 27, 2001

[181] Grey E. Burkhart, "National Security and the Internet in the Persian Gulf Region," March 1998 <http://www.georgetown.edu/research/arabtech/pgi98-1.htm>

According to the CIA, Iran has over 5,000 Internet hosts in 2004, compared to 15,931 in Saudi Arabia and 56,283 in the United Arab Emirates.[182] As regards personal computers, the International Telecommunications Union (ITU) states that Iran's penetration rate was 7.50 per 100 persons in 2003, compared to 13.67 in Saudi Arabia and 11.99 in U.A.E.[183]

Despite Iran's mediocre standings in Internet and PC penetration, in recent years, the government has allocated significant resources to "catching-up" in the Information and Communications Technology (ICT) sector. The defense sector, in particular, enjoys priority access to financial and human resources dedicated to research and development in electronic warfare and related fields.

4.1 BACKGROUND

An oil-rich, semi-authoritarian, Islamist power, Iran is determined to overcome a long-standing self-perception of military and technological inferiority. To achieve this, the government in recent years has taken steps to both transform its foreign policy and security doctrine and acquire sophisticated weaponry. In addition to reported investment in WMD (weapons of mass destruction) precursors, Tehran is purchasing state-of-the-art advanced conventional systems while actively pursuing digital technologies and military-related information technology (IT) research and development.

Estrangement from Washington traditionally gave the leadership a useful pivot with which to garner popular support for its regional policies and ambitions. It also provided a justification, or excuse, for developing asymmetric warfare capabilities of all types.[184] More recently, the collapse of Saddam Hussein's army has reinforced Tehran's ambition to become a key political player in Central Asia. Rising U.S. presence in the region is a thorn in the regime's side, perhaps strengthening the leadership's ambitions to play a credible "denial role" in the area.

While the Iranian leadership's primary goal is to continue to preserve and protect the Shi'a revolution, strategic and geopolitical considerations, rather than ideology, have in recent years assumed greater prominence in Tehran's formulation of its national security policies. In addition to strategic military investments, economic growth and job creation have become leading concerns.[185] Islamic and nationalist objectives have receded in importance in determining the

[182] According to the CIA's *The World Factbook* (2004), an Internet host is a computer connected *directly* to the Internet; normally an Internet Service Provider's (ISP) computer is a host. Internet users may use either a hard-wired terminal, at an institution with a mainframe computer connected directly to the Internet, or may connect remotely by way of a modem via telephone line, cable, or satellite to the Internet Service Provider's host computer. The number of hosts is one indicator of the extent of Internet connectivity. See CIA, *The World Factbook*, 2004 < http://www.cia.gov/cia/publications/factbook/docs/notesanddefs.html>

[183] ITU, 2004 Information Technology Statistics, available on-line at: <http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet03.pdf>

[184] The government's hostility (or restrictions on formal relations) toward the U.S. and Israel is said to remain "one of the strongest parts of the revolutionary legacy." With respect to continuing estrangement from the U.S., the current regime in Tehran, as one expert has written, "Cannot negate Khomeini's (anti-U.S.) principles with out negating itself." Anoushiravan Ehteshami, "The Foreign Policy of Iran" chapter in Hinnebusch and Ehteshami, *The Foreign Policies of the Middle East States*, 2002, p. 305

[185] A variety of sources indicate, however, that political and social imperatives have blocked progress toward market reforms. Oil earnings account for over 80 percent of annual revenue, but much of the oil wealth has been

goals of internal development. In describing this shift, experts note the government's more pragmatic approach: "Iran's policies…are increasingly prudent, with the Islamic Republic trying to calm regional tension and end its isolation…The Islamic regime has supported the status quo with regard to territorial integrity, has avoided major military provocations…"[186]

Moreover, according to analyst John Battilega, Iran's primary national security concerns are "local," relating to maintaining the internal security and territorial integrity in an unstable, threatening region. Battilega says Tehran seeks to avoid technological and economic isolation, which could doom any prospect of achieving the power base necessary to become a major political "player" in Central Asia.[187]

In this framework, the government has sought pragmatic ties with neighbors in Central Asia, such as Russia and India, to protect its economic interests and raise its political profile in the region. The regime, through its intelligence services, continues to provide covert support to anti-Israeli terrorist groups. Available open source evidence suggests that Tehran will continue to play an opportunistic role, particularly as regards the significant covert activities of its intelligence services supporting international terrorism.[188]

4.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

U.S. officials have consistently included Iran on a list of "rogue" states with the capacity and motive to launch a cyber attack against U.S. interests. In public testimony, former CIA Director George Tenet, for example, has pointed to the efforts of potential foes of the U.S. to interfere with U.S. computer networks. Richard Clarke, former chairman of the President's Critical Infrastructure Protection Board, has noted that Iraq, Iran, North Korea, China, and Russia are already training people in cyber warfare.[189] According to a declassified threat assessment in the U.S. Navy's Strategic Planning Guidance published in 2000, "Russia, China, India, and Cuba have acknowledged policies of preparing for information warfare," while "North Korea, Libya, Iran, Iraq, and Syria have some capability."[190] Persian Gulf military expert Anthony H. Cordesman writes that Iran is improving its capabilities in information warfare, "although it seems unlikely that it is capable of advanced attacks on protected US military and government computer, information, and battle management systems."[191] However, with regard to generalized

---

squandered by government support to loss-making factories and hand-outs to private companies that hire workers. See "The World of the Ideologues-Defiant Iran", *The Economist*, September 4, 2004

[186] Daniel L. Byman, et. al., *Iran's Security Policy in the Post-Revolutionary Era,* RAND Corp. 2001, p. xiv.

[187] John A. Battilega, Randall Greenwalt, David Beachley, Daniel Beck, Robert Driver, and Bruce Jackson, "Transformations in Global Defense Markets and Industries: Implications for the Future of Warfare," National Intelligence Council, December 20, 2001 <http://www.cia.gov/nic/PDF_GIF_research/defensemkts/iran.pdf>

[188] See, for example, U.S. Department of State publication *Patterns of Global Terrorism, 2002,* p. 77

[189] "US Foes Targeting American Computer Networks," in Post-Newsweek Business Information, Inc. Newsbytes, June 25, 1998. Also, see Dickon Ross, The Guardian, February 20, 2003

[190] John M. Donnelly, "Navy Names Nations Posing Cyber Threats," King Communications Group, Navy News Week, September 11, 2000, p. 1

[191] Anthony Cordesman, Center for Strategic and International Studies, "U.S. Policies Ten Years After the Gulf War: The Impact of Changes in the Regional Military Balance," in *The Gulf and Transition*, December 2000 <http://www.csis.org/gulf/reports/submilbalance.pdf>

cyber attacks, "Iran probably has more capability to attack the US private sector and the systems of the Gulf States."[192]

Jay Valentine, former head of Infoglide, a database analysis company and contractor to the U.S. government, noted in 1999 that "There are at least six nations right now who have active groups, paid by their governments, trying to formulate tools and procedures to cause computer terrorism in U.S. corporations…Those countries are Syria, Iran, China, India, Pakistan, and Israel."

More recently, the July 2002 Riptech Internet Security Threat Report indicated that, among seven countries designated as "state sponsors of terrorism," Iran was the source of 90 percent of attacks against Riptech clients in the first half of 2002.[193] In terms of countries with fewer than one million Internet users, Iran and Kuwait were "by far the most prolific" in terms of originating attacks, according to an early 2003 study released by Symantec.[194]

For more than a decade, Iran's military leaders have expressed inadequacy in the face of modern "information warfare" (as practiced by the U.S. and other powers).[195] This, and other factors, induced the leadership to restructure defense priorities and domestic R & D efforts in the 1990's. According to a study sponsored by the National Intelligence Council in 1999, Iraq and Iran are examples of states that "will likely explore the usefulness of information technology in pursuit of asymmetric conflict…To counter U.S. military capabilities—current or those that emerge from the RMA [Revolution in Military Affairs]—these states will explore ways to exploit U.S. vulnerabilities, including through the employment of information warfare and cyber-terrorism."[196]

In 2002, Iran had approximately 250 Internet Service Providers. Most of these are government owned or belong to state agencies, such as Universities and think tanks.[197] The few ISPs that operate independently from the government reportedly provide access only cautiously to

[192] Robert Lowry "Information Warfare: Choose Your Weapon in the New Century," Financial Times News Service, Global News Wire, December 1, 2000, p. 2

[193] Tom Regan, "The Hidden Dangers of Information Warfare," *Christian Science Monitor Service*, June 26,1999

[194] Computer Crime Research Center, "Who Were the Cyber Terrorists of 2002?," February 3, 2003 <http://www.crime-research.org/news/2003/02/Mess0602.htm> and Manoj Nair, "Iran, Kuwait Most Active in Mideast for Cyber Attacks," Al-Nisr Publishing LLC, *Gulf News*, February 5, 2003 <http://www.gulfnews.com/Articles/news.asp?ArticleID=76358>

[195] John M. Shields, *Military Industries in the Islamic Republic of Iran: An Assessment of the Defense Industries Organization (DIO)*, Center for Nonproliferation Studies, Monterey Institute, May 1996, p. 42.

[196] "Buck Rogers or Rock Throwers?" Conference Report, October 14, 1999, p. 8 <http://www.cia.gov/nic/pubs/conference>

[197] The academic Internet link, for example, is via a single satellite link from IPM (Institute for Theoretical Study of Physics and Mathematics) Microvax to Archway/UUNET in Italy. According to a 1997 report, commercial Internet access is offered through seven ISPs: Neda Rayaneh Institute, Data Communication Company of Iran, Compuserv, IRNET, Apadana, Virayeshgar Corporation, and Pars Supala.

individuals and charge prices that essentially limit the use of the Internet to users in upper economic brackets.[198]

Publicly available computer terminals are said to have spawned a new "sub-culture" in the principal cities, such as Tehran.[199] One media report indicates that the proliferation of cyber cafés, coupled with rudimentary attempts by the government to filter content and control public access, has spawned a hacker mentality.[200] Disgruntled or bored youth, according to this source, take out their frustrations through clandestine computer hacking.[201]

The Iranian government in 2001 reportedly was drafting rules and preparing software-filtering equipment to control Internet service and content. The leadership deems Internet use by researchers and University students a positive and necessary step. The ISPs associated with these state entities use leased lines under government control. On the other hand, some cyber cafés, using ISPs linked to satellites, remain out of the government's reach.[202]

4.3 FOREIGN MILITARY RESEARCH

As stated above, Tehran accords high priority to military modernization to shore-up perceived security vulnerabilities. As one analyst put it in 1996 with respect to the defense sector: Tehran is "widening the technological threshold of its industrial complex."[203] In recent years, the government has allocated a significant share of its oil revenues to military R&D required to manufacture or exploit weapons of mass destruction, advanced conventional weapons, and diverse electronic warfare technologies.[204]

---

[198] The Iranian, October 27, 1999. The government carefully controls the issuance of Internet service permits because of security concerns—not income derived from fees. See interview with Minister of Communications Motamedi, "Internet, Mobile, and Satellite in Iran," September 27, 2001

[199] Molly Moore, "Cybermania Takes Iran by Surprise," *Washington Post,* July 4, 2001 <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A16095-2001Jul3&notFound=true> Farhang Rouhani, "The Spatial Politics of Leisure: Internet Use and Access in Tehran, Iran," NMIT Working Paper, April 2000, available at <http://nmit.georgetown.edu/papers/frouhani.htm>

[200] "Iran: Special Judiciary Branch to Deal with Internet Offenses," Global News Wire, May 22, 2003

[201] Although cost factors limit the accessibility of Iran's Internet cafés (known as Coffeenets), the rapid proliferation of Internet cafés, offering chat rooms and opportunities for virtual contact with foreigners, renders precise numerical estimates difficult. In mid 2001, according to one source, there were about 450 cyber cafés in Tehran; a more recent estimate is 1500. In 2001, the fee for Internet use was about $2 per hour. Per capita GDP in Iran in 2001 was about $7000. A separate source indicates that access to the Internet is provided gratis to students, with nearly all universities in Iran connected.

[202] "Iran Begins to "Filter" Internet Access," BBC Monitoring International Reports, May 12, 2003

[203] Anoushiravan Ehteshami, "Iran Strives to Regain Military Might," *International Defense Review*, July 1, 1996 <http://web.nps.navy.mil/~relooney/Iran_25.htm> According to reliable sources, while Iran enjoys annual oil revenues approximating $24 billion and in 2003 allocated an estimated $4.3 billion to military expenditure, revenues are often wasted on government investment in state-owned or controlled industries to boost employment. "The World of the Ideologues", *The Economist*, Sepember 4, 2004

[204] See "Threat Assessment II, CIA Analyzes International WMD Capability," *Global Security Newswire*, January 31, 2002, and National Intelligence Council Conference Report available at <http://www.cia.gov/nic/pubs/conference>

In the aftermath of the 1991 Gulf War, Iran grasped the value of information technologies for military ends. Tehran moved to ensure its armed forces are "digitized." With respect to military-technical training, for example, a July 1997 report from Tehran stated that 15,000 new recruits were being tested for admission to the regular Army's officer training college; those who pass the entrance exams will be eligible to pursue a broad range of academic subjects, including computer software.[205] Defense Minister Ali Shamkhani stated in December 2000 that "Iran relies on its indigenous strength and domestic hardware and software potentials for national security."[206]

More recently, Defense Minister Shamkhani signaled the importance of IT investments in boosting military defense capabilities.[207] The Ministry of Defense seeks to strengthen the link between Information Warfare infrastructure requirements and academic research in the IT sphere. In February 2003, Shamkhani visited Malek Ashtar University of Technology in Isfahan province to discuss information technology. According to reliable sources, Shamkhani participated in the first Iranian state conference on "the development of technology in defense." He announced that a "University complex" in these fields will be established to attract the necessary manpower in keeping with defense sector improvement and modernization. "All capabilities in information technology and communications manufacturing in software education and infrastructure and research are concentrated in the defense sector, and this capability cannot be seen in any other sector," the Defense Minister noted.[208]

Malek Ashtar University, in Shahinshahr, Isfahan Province, is also known as the University of Sciences and Technology. Cursory examination of open source documents reveals that the University is engaged in a range of R&D activities, including aerospace, information and communication technology, and genetic biotechnology.[209] Anecdotal evidence indicates links between institutes such as the Advanced Information Communication Technology Center (Sharif University of Technology) and the ICT Department at Malek Ashtar University with respect to teaching in the field of "advanced computer networks… filtering and firewalling…"[210]

[205] "Army Officer School Seeks Recruits," Iran Brief, July 3, 1997

[206] Source: "Iran Says Iran-Russia Relations Enter New Phase," Xinhua General News Service, December 28, 2000 <http://english.people.com.cn/english/200012/29/eng20001229_59104.html>

[207] Iran-Daily.com, February 5, 2003 and see also: Middle East Media Research Institute, "Iranian Defense Minister on Iran's Defense Doctrine," Special Dispatch No. 502, May 9, 2002 <http://www.memri.org/bin/articles.cgi?Area=sd&ID=SP50203>

[208] FBIS translation, "Iran: Defense Minister Discusses Importance of Information Technology," Iranian Students News Agency, Tehran, IAP20030204000076 February 4, 2003

[209] Malek Ashtar University, in Shahinshahr, Isfahan Province, evidently has a link to the Iranian Air Force. The Aviation Complex at the University reportedly designed a trainer aircraft for the Air Force. According to the website of the Moscow State Aviation Technological University, which includes a faculty of informatics and computing science, Malek Ashtar University of Technology is included on a list of "partner" institutes and Universities. Although this link between the Russian and Iranian bodies may be confined to aircraft technology, it nevertheless suggests a potential conduit for transmitting technical expertise in the IT domain.

[210] See professional CV posted by Amir Foroutan, Sharif University of Technology, Tehran, Iran <http://mehr.sharif.edu/~foroutan>

4.4 INFORMATION TECHNOLOGY INVESTMENT

Despite U.S. export sanctions, Iran has access to computer hardware and software of various types and sophistication. For example, although exports of Silicon Graphics work stations to Iran are banned, a Tehran-based company in 1993 nevertheless imported such a work station which ran SoftImage graphics software developed by a Canadian company. [211] According to an ITU statistical series on computer penetration in individual member countries, Iran had 56 PC's per 1000 people in 1999. This number rose to 63 per 1000 or 4 million computers overall in 2000, and to 75 per 1000 or 4.9 million PC's in 2003.[212]

Iran reportedly imports large amounts of computer software. Indigenous firms, such as SENA Soft, are involved in "updating" this software. The Iranian Software Producers Association signed an agreement in 2003 with Dubai Electronic City to permit Iranian software firms to cooperate with foreign companies in Dubai.[213] Beginning in the 1990s, several U.S. software producers, such as Microsoft and IBM, explored the market in Iran.

According to several sources, Iran Electronic Industries (aka SA Iran) is the major producer of electronic systems and products in Iran.[214] In the military field, IEI's activities embrace a wide range, such as optics, electro-optics and laser communications, telecommunications security, electronic warfare, radar tube manufacturing, and missile launchers.[215] IEI's website asserts that the Corporation has "six subsidiaries and 5,000 experienced personnel including 700 qualified and highly trained engineers in different disciplines.[216] IEI has developed a high capability in research and development (R&D) which is the technological backbone of the company."[217] IEI's subsidiaries include: Shiraz Electronics Industries, Sharif University of Technology/Iran Electronics Research Center, Information Systems of Iran (ISIRAN), and Electronic Components Industries (Microelectronics.)[218] In addition, IEI is linked to Isfahan University of Technology (IUT), particularly in the aerospace field.[219]

---

[211] "Foreign Computer Firms in Iran: Deals," <http://www.gpg.com/homePages/peik/foreign.html>

[212] ITU statistics on information technology available on-line at: <http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet03.pdf> Not all computers would have access to the Internet.

[213] "Information Technology in Iran: Computer Hardware and Software," June 6, 1997 and "Iran: Signing Cooperation Agreement with Dubai Electronic City," Global News Wire, June 10, 2003

[214] See Shields, op. cit. p. 21 and "Iran Electronic Industries" (SA Iran) company profile available at <http://www.rahyar.com/ipas2002/Final/Sa_Iran.htm>

[215] Source: "Iran Electronic Industries," SA Iran, 2002 <http://www.rahyar.com/ipas2002/Final/Sa_Iran.htm>

[216] Sources: "Integrated Electronics Industries," <http://www.ieicorp.com/about.htm> and "Welcome to Iran Electronic Industries," <http://www.iran-export.com/exporter/company/sairan>

[217] Source: "Integrated Electronics Industries," <http://www.ieicorp.com/about.htm>

[218] Several sources state that Shiraz is known as the "electronic center of Iran" because of the important industries in the city. Shiraz Electronic Industries is engaged in a variety of activities including electronic warfare, missile electronics, naval electronics, etc. Sharif University reportedly is a front organization for technology procurement.

[219] Iran today has 23 full universities and 19 technological institutes. "Iran: Country Profile" Quest Economics Database, Middle East Review of World Information, October 2, 2002, p. 3. According to a research study, the Sharif Electronics Research Center was established by the merger of the Electronics Research Center and the Sharif University of Technology following the revolution in 1979. The main research priorities at the Center are: Speech ciphering, Speech processing and recognition, Cryptography and data security,Digital and radar signal processing, VLSI circuit design and testing, Radio communication circuits

Another Iranian military production entity, the Communications Industries Group, is a subsidiary organ to the Defense Industries Organization (DIO). The Group, which manufactures equipment for Iranian military, law enforcement, and internal security bodies, was formed in 1989 as part of an overall reorganization of the military industries. It also reportedly has links to Iran's civilian Ministry of Posts, Telegraph, and Telephone (PTT).[220]

CIG is believed to oversee the activities of: 1) GAM Electronics and Communications Industries, and 2) Tactical Communications Industries, formerly known as ICI (Iran Communications Industries). According to the GAM website, GAM is a private corporation with offices in Tehran.[221] Since 1978, it has "designed, developed, and supported computer applications and systems for government and private enterprises." ICI, according to one source, is Iran's "leading manufacturer of military communications equipment and systems. More than 75 products in the field of tactical communication and encryption systems meet a wide range of the army's requirements."[222]

Computer penetration is projected to rise in the future in response to expanding Internet access. A Taiwanese firm, BenQ, estimates that approximately 800,000 PCs will be sold in Iran in 2003. BenQ collaborates with Iran's largest PC producer, Isiran.[223] Recently, Malaysian and other Southeast Asian producers have targeted Iran as a market for laptops and desktops.[224]

4.4.1 EXTERNAL CONNECTIONS

Iran's military has moved to cultivate relations with foreign suppliers for advanced technologies.[225] As area expert Anoushiravan Ehteshami writes:

---

design and programmable logic controllers. "Iran's Telecom and Internet Sector: A Comprehensive Survey," June 15, 1999, Ch. 5

[220] According to a report from the state-run news agency, IRNA, in April 2003, the Islamic Consultative Assembly approved changing the name of the PTT to the Ministry of Communication and Information Technology (CIT). "The new title will help the ministry to widen its scope of activities and responsibilities in the field." FBIS English translation of IRNA report, April 9, 2003. This report could not be confirmed elsewhere.

[221] Source: "Gam Electronics," <http://www.gamelectronics.com/aboute.htm> see Google's site cache of "Gam Electronics" located at: <http://216.239.41.104/search?q=cache:pdQGiaPa2bMJ:www.gamelectronics.com/aboute.htm+&hl=en&start=1>

[222] Source: "Iran Seeks Arms Plants in India," *MedNews*, January 11, 1993 <http://www.science-arts.org/Internet/node196.html>. In a separate, unconfirmed report, Iran sought assistance from India in 1992 in setting up a nation-wide Iranian defense communications grid. Included would be mobile communications systems, which Tehran wanted to manufacture in facilities then operated by ICI.

[223] For additional details, see "Information Systems Iran," <http://www.isiran.com/solution/index.asp>

[224] "PC Suria Now Targets West Asian Markets," Bernama, July 22, 2002

[225] According to Cordesman, op. cit., Iran has largely recovered from its defeat by Iraq in the 1980's, but has not been able to offset the obsolescence of its overall inventory of armor, ships, and aircraft. More recently, a U.S. Congressional Research Service researcher assessed in 2003 that Iran has "come a long way" toward its objective to manufacture sophisticated armaments, including ballistic missiles and chemical agent. But "in the aggregate Iran remains reliant on foreign suppliers." CRS, Iran: Arms and Weapons of Mass Destruction Suppliers, January 3, 2003, p. 2

In recent years, Iranian leaders have spoken of the need to become progressively more self-sufficient in R&D and to produce major weapons systems. This view has been repeatedly reinforced by the (United States) policy of 'dual containment' and Iranian isolation. However, without considerable outside assistance—and in the absence of an efficient infrastructure—this is still proving too difficult to realize materially. Iran's arms-making potential, therefore, will depend as much on its own efforts and available resources as the continuing good will of its closest military partner, Russia.[226]

Reporting from Moscow (thus far unconfirmed anywhere else in the open source literature) indicates Iran decided in mid-2000 to invest in a "25-year military development program."[227] Little is known about the details of this reported program, however.

In keeping with the shift in 1997 toward a security strategy based mainly on cold calculation of national interest (to borrow a phrase from Daniel Byman's *Iran's Security Policy in the Post-Revolutionary Era* published in 2001), Tehran actively seeks economic and military contacts with foreign technology producers.[228] The election of President Vladimir Putin in May 2000, for example, is reported to have triggered "a new era" in bilateral Russo-Iranian trade relations. Since then Tehran has made significant moves towards the acquisition of Russian defense technologies and production licenses. India, another country embracing information technologies both for civilian and military uses, has agreed to cooperate with Iran on information technology, training, and international terrorism issues. As outlined in another section of this study, both Russia and India have declared cyber attack doctrine and operational capabilities.[229]

In the period immediately after the 1979 revolution ousting the Shah, Iranian government interest in the electronics industry as a main pillar of the defense industrial base rose in response to the perceived evidence of a weak indigenous R & D infrastructure. A key bottleneck, however, was the flight of scientists and technicians to the U.S. and Europe in the 1980s.[230] In response, the Rafsanjani government took steps to: establish educational and research centers, both within Iran's Universities and within the armed forces; identify overseas partners for technology sharing, student exchanges, and collaborative R & D; and provide incentives to lure educated Iranians back to serve the nation.[231]

During the Cold War, Iran was often able to use East-West tensions to further its foreign assistance agenda. Following the break-up of the Soviet Union the Iranian leadership was no longer able to leverage one great power against the other. In 1997, the Khatami government

---

[226] Anoushiravan Ehteshami, "The Foreign Policy of Iran" chapter in Hinnebusch and Ehteshami, *The Foreign Policies of the Middle East States*, 2002, p. 26

[227] Lyuba Pronina, "Arms Producers Take Aim at Wider Clientele," *Moscow Times,* December 19, 2001 <http://www.avia.ru/english/articles/doc85.shtml>

[228] For a thorough discussion of supply arrangements with foreign technology providers, see Kenneth Katzman, "Iran: Arms and Weapons of Mass Destruction Suppliers," Report for Congress, updated January 3, 2003, available at: <http://www.usembassy.it/pdf/other/RL30551.pdf>

[229] See Chapter III on India and Chapter VII on Russia

[230] Shields, op. cit. p. 41

[231] Although Iran attempted to leverage contacts and exchanges with foreign universities and research centers and established several military academies and technical universities, a study published in the mid-1990s asserts that Iran's investment in research and S & T education remained low. In 1995, the total number of scientists, engineers, and technicians in the country was placed by Iranian sources at about 300,000. Source: Shields, op. cit., p. 41 and 43

initiated significant contacts with Moscow, Pyongyang, Beijing, New Delhi, selected EU members, and others. Of these overtures, ties with Russia and India deserve further attention.

Several sources indicate that senior Russian and Iranian leaders recently have "coordinated" on long-term political strategy and policies with respect to the Middle East and Central Asia (including development of the Caspian Basin). Russia's motives for pursuing closer ties with Iran are complex and subject to interpretation. According to an academic assessment published in Tehran after Defense Minister Sergeyev's December 2000 visit, Russia aims to:

- Use Iran to prevent NATO from expanding into Central Asia
- Frustrate and re-balance ambitions of regional competitors, such as Turkey
- Thwart U.S. objectives to dominate the Persian Gulf.[232]

Iranian President Khatami asserted in Moscow in March 2001 that Russian-Iranian ties are of a deep-rooted nature, "are not a limited tactical move…"[233] An account of Khatami's visit published by Iran's Chamber of Commerce, for example, quotes the President: "The officials of the two countries decided to broaden and deepen their ties in all fields. So, they signed a treaty of basic relations, which will set the ground for all the future cooperation.[234] On the Russian side, the Director of Moscow's Center for Iranian Studies, Rajab Safarov, commented in July 2002 that "Russian-Iranian military technical cooperation should not be a subject of bargain and should be interpreted as 'natural trade and economic interaction'..." [235]

Beyond the rhetoric, however, informed observers suggest that closer Russo-Iranian ties rest largely on pragmatic necessity. The two countries' interests in the defense sector, for example, are complementary (and mutually profitable): Russian industry depends significantly on foreign consumers since it cannot survive solely on domestic procurement, while Tehran has made a key commitment to upgrade and transform its military and has sufficient oil revenues to pay.[236] As one expert notes:

> Arms sales generate only an estimated $3 billion per year, clearly insufficient for maintaining and converting the fast-decaying remains of the once mighty Soviet military industrial complex…Under these conditions, Iran is very attractive –it represents one of the largest Asian arms sales markets and is generally off-limits to Western producers."[237]

The election in Russia of Vladimir Putin in May 2000 triggered a drive in Iran to strengthen bilateral military cooperation.[238] Recent media reporting discusses a significant Iranian military

[232] "Iran Paper Views Russian Motives for Defense Cooperation," BBC Worldwide Monitoring, February 27, 2001, p. 2

[233] Alexei Kravchenko, "Russia-Iran Cooperation is Not a Tactical Move," TASS, March 14, 2001

[234] "President Khatami Visits Russia," ICCIM, 2001, p. 3 <http://www.iccim.org/English/Magazine/iran_commerce/no1_2001/09.htm>

[235] "RF-Iran Military Ties Should Not be a Subject of Bargain," TASS, July 31, 2002

[236] "Weapons Trade is an Intimate Business," *Gazeta*, (Moscow) February 27, 2002

[237] Alexander Pikayev, "Strategic Dimensions of Russo-Iranian Partnership," Center for International Trade and Security, Winter 2001, Vol. 7, No. 1

[238] Iran's cultivation of Moscow started during the 1980-1988 war against Iraq. Soviet-manufactured arms substituted for U.S. and other embargoed Western arms. The first supplies of Soviet-type equipment

development program. The total value of the arms sales program, of which Russia might expect one-third of the business, is estimated at $25 billion.[239] In late 2000, reports from Moscow noted that Russia's involvement in the program would proceed in phases: 1) fulfill the previously contracted conventional arms sales to Iran booked in 1989-1991; 2) negotiate an agreement in 2001 covering sales of advanced conventional defense systems.[240]

Of greater potential interest to Iran in the longer run, however, is the training and access to technological "know-how" prescribed in the framework military cooperation agreements and related documents. (Often such access to training is linked to purchases of military hardware.) Reportedly, Tehran has entered into agreements with the Soviet military in which each year Iranian military officers will receive training in Russian academies.[241] Finally, as noted above, Iranian universities, such as Malek Ashtar University of Technology, have ties to Russian universities and research institutes that provide funding and technical expertise to Iranian researchers.[242]

In addition to long-term bilateral cooperation agreements in the military sector, Moscow and Tehran have shown increasing interest in government-sponsored scientific exchange, building on established arrangements in this field.[243] In general, each side enjoys significant scientific resources and a well-developed institutional framework of research centers and scientific academies. Iran's Academy of Science, for example, opened its doors in 1990. It was constituted to promote science and technology, study the experience of other countries that might apply to available facilities in Iran, exchange views and research with other countries, and award scholarships and sabbaticals to establish links with scientific academies elsewhere.[244] Provision of scientific training by Moscow reportedly is an important element of overall bilateral cooperation with the Iranian government.[245]

---

reportedly came from North Korea and China, followed by direct arms agreements with Moscow. According to some experts, the business arrangements with Moscow were on a "cash-and-carry" basis, not involving any alliance of mutual interest. This relationship was reflected in the 1994-1999 period (some $4 billion in arms sales), when Moscow delayed and postponed the delivery to Iran of three Kilo-class submarines.

[239] "Russia-Iran Pact Paves Way for Defense Contracts," Agence France Presse, March 12, 2001

[240] With respect to its principal military partner, Russia, Tehran, in the short run, is interested mainly in buying advanced conventional weapons, including "air defense systems, anti-tank systems, and operative-tactical missile systems." The clerical regime is also interested in acquiring licensed production of a number of arms systems. According to sources in Russia, the Iranian military wants mobile air defense systems is to protect troops and "strategic facilities," including nuclear installations. Source: Novichkov, "Iran Imports Russian Weapons," (Russia), October 3, 2001. Igor Shiskhov, "Russia-Iran Cooperation not Aimed Against Other States," ITAR-TASS News Agency, October 1, 2001

[241] "Iran and Russia Move to Military Ties Despite U.S. Worries," *Agence France Presse*, December 28, 2000

[242] See Moscow State Aviation Technology University Website <http://www.mati.ru/english/> and the Iranian air force website <http://www.iiaf.net/home.html>.

[243] An agreement on scientific and technological development was signed in November 1999. As part of the agreement, Tehran hosted an exhibition of Russian advanced technologies in late 1999. Source: Gennady Khromov, "Russian-Iranian Relations and Unilateral U.S. Sanctions," Center for International Trade and Security, Winter 2001, Vol. 7, No. 1, p. 5

[244] Source: Iran Academy website <http://www.ias.ac.ir>

[245] According to Khromov, op. cit., p. 5. 350 Iranian students were studying in Russia in 2001. Training offered by Moscow in the military-technical field has received wide attention in the context of proliferation of WMD and delivery systems. In January 2002, a Russian specialist at the Moscow Aviation Institute told the Washington Post that "Russian engineers have visited Iran throughout the 1990's in order to provide

In March 2001, for example, President Khatami visited Russia to discuss mutual strategic interests and to prepare several specific agreements in the energy, trade, military-technical, and scientific-technical cooperation fields. The two sides signed a memorandum of understanding regarding the development, manufacture, and launch of a geostationary telecommunications satellite. [246] In July 2002, Moscow reportedly committed to provide Iran additional assistance in the nuclear development field as part of a 10-year cooperation effort. According to a *New York Times* story from Moscow, "the initiative (not yet approved by either side) also calls for expansion of economic, industrial, and scientific cooperation with Iran."[247]

With respect to scientific developments potentially relevant to electronic warfare, Russia was awarded a $200-300 million contract to build a telecommunications satellite called the Zohreh. The Zohreh—with capacity to broadcast about 12 channels (seven for television and five for telecoms)— is to be the first of six satellites funded by Tehran to be stationed in geostationary orbits to "boost Iran's telecommunications services."[248] Although some procedural and legal issues reportedly still must be resolved between Moscow and Tehran[249], the plan was to launch the satellite using Iran's solid fuel rocket, Shahab-4, reported to have been "in the engine design and test phase" in 1999.[250] According to U.S. Navy Vice-Admiral Thomas Wilson's Congressional testimony in March 2002, "During the next ten years, many states will seek to augment their weapons of mass destruction, missiles, satellite reconnaissance, and global positioning systems, designed to counter key U.S. concepts."[251]

During an official visit to India in January 2003, President Khatami signed a formal declaration setting forth the "vision of strategic partnership between India and Iran…" Several reports indicate closer ties will be built on "mutual trade," i.e., Iran will increase sales to New Delhi of crude oil while India will export information technologies (software) and agricultural commodities to Iran. The "New Delhi declaration" embraces several aspects of bilateral cooperation, such as economic, energy, science and technology, information technology, training, and addressing the problem of international terrorism. The two sides also agreed to

technological information relating to missile development." See "Missile Exports to Iran: Training and Know-how," November 6, 2002, <http://www.nti.org/db/nisprofs/russia/exports>

[246] Francois Bonnet, "Moscow Determined to Sell Arms to Tehran," *Manchester Guardian Weekly*, March 28, 2001

[247] Steven Lee Myers and Michael Wines, "Russia's Overtures to 'Axis of Evil' Nations Strain Its Ties With U.S.," *New York Times*, September 1, 2002, p. 2 <http://www.nytimes.com/2002/09/01/international/europe/01PUTI.html>

[248] "Iranians Inspect Russian Telecommunications Plant," *Asia Pulse*, (Moscow) June 1, 2001

[249] Reports conflict from the state-run IRNA regarding the status of the Zohreh satellite. One IRNA report from February 1 says that the Zohreh satellite was cancelled outright, but that Iran was negotiating with Russia on a different satellite, "Mesbah". Later in February, IRNA reported that Iran had signed a deal with Italy to build Mesbah, with no further mention of Russia. In June, IRNA ran a story saying that Zoreh is delayed due to Russia's "refusal to provide necessary guarantees".

[250] "Iran Develops Launch Vehicle," *Satellite Today*, February 8, 1999

[251] See Keith Stein, "Attack on Satellites Possible by 2010," King Communications Group, March 28, 2002 and Vice Admiral Thomas Wilson, "Global Threats and Challenges," Defense Intelligence Agency, March 19, 2002 <http://www.iwar.org.uk/homesec/resources/senate-mar-19-02/Wilson.pdf>

explore opportunities for cooperation in agreed areas and called upon the business communities of the two countries to promote bilateral trade and investment.[252]

During his visit to India, President Khatami observed the activities and programs of HITECH City in Hyderabad, a primary center for information technology in India that has hosted business visits by a variety of world leaders. According to various accounts, HITECH city specializes in both software production and formal training of computer specialists. Reportedly, the city exported approximately $11 million in computer software in 2002.[253] Khatami also visited the eSeva Center in Andhra Pradesh, accompanied by the Minister of Defense and the President's information and communications technology special envoy, Dr. N. Jahangard. eSeva specialists explained the Andhra Pradesh e-governance initiatives.

In addition, Iranian intelligence could penetrate or exploit the considerable Iranian expatriate communities in the U.S., U.K., and other countries. The Iranian diaspora, consisting mainly of citizens who left the country to reside in North America or Europe in the early 1980s, reportedly plays a significant supporting role in promoting the IT sector.[254] Many of the refugees who fled after the Islamic Revolution are trained engineers, skilled in computer science.[255] Some have returned to Iran either to assist in improving the telecommunications infrastructure or to invest in Internet cafes. Evidence of information sharing can be seen in e-mail discourses between Iranian expatriates in the U.S. and University research centers in Iran, for example.[256] In view of its ambitious telecommunications plans, the government in mid-2002 officially invited Iranian IT experts living abroad to apply for jobs to supplement the indigenous supply of technical or engineering manpower.[257]

4.5 CONCLUSION

Iran is opening up to information technologies in response to both military and economic needs. Disentangling the various contradictory influences and impulses with respect to information technology provides insights into Iranian strategy. It appears the government's current policy objective is to "transform" the IT sector, albeit with a monopoly over the telecom backbone. Selected activities (such as state enterprises and University research centers) receive official

[252] "Documents Signed Between the Governments of Iran and India, January 25, 2003 <http://www.meadev.nic.in/economy/ibta/agreements/indiran>

[253] "Iran: President Khatami Visits Information Technology Center in India," Financial Times Information, BBC Monitoring International Reports, January 28, 2003

[254] See SiliconIran, a magazine intended to create a bridge among "high-tech Iranians" globally. Available at <http://www.siliconiran.com/magazine/index.shtml>

[255] Sauleh S. Etemady, to cite one example, is a U.S. citizen who reportedly is a member of the technical staff of Portnet Multimedia Company in Portland OR but resides in Iran. According to Etemady's CV, his specific areas of interest at Sharif University of Technology's Department of Computer Engineering include computer networks and information warfare and security. Etemady's CV is available on-line at <http://www.egr.msu.edu/~etemadys/right3.htm>

[256] See Payman Arabshahi, "The Internet in Iran: A Survey," Points of Contact in Iran and Seattle, Washington, July 1996, available at <http://www.iranian.com/July96/Features/InternetIran/InternetIran.html>

[257] "Official Invites Iranian IT experts Abroad to Apply for Jobs Back Home," BBC Monitoring International Reports, July 4, 2002. A website in the remote village of Shahkooh was built by a member of the Iranian Diaspora in the United States on a return visit to his birthplace. The village owns three computers. Shahkooh was connected to the online world in August 2000 <http://www.honco.net/os>

backing, but elsewhere government regulates through the licensing and control of private ISPs, installation of content filtering devices and other monitoring devices. Access to personal computers (PCs) and the Internet, even in cyber cafés, is mostly limited to Iran's elite through price rationing. Government limits and restrictions foster widespread "black" activity, such as the purchase of private satellite dishes, software piracy, and computer hacking. The mixture of IT investment, computer talent, and underemployed youth has spawned a culture in Tehran that is potentially ripe for exploitation or manipulation by Iran's intelligence services.

Iran's sense of military and economic inadequacy, isolation, and vulnerability in the post-Cold War world is driving on-going interest in non-conventional weapons and technologies, including advanced information and communications technologies. In this framework, there is considerable anecdotal evidence that Iran has begun to emphasize the link between defense modernization and academic research in the computer engineering field. This evidence suggests the government is sponsoring the development of a cyber warfare capability as a potential force multiplier.

We assess that Tehran may be actively exploring a cyber warfare capability, based on the following:

- Leadership frustration with Iran's outdated and under-manned conventional military, especially in the aftermath of the 1991 Gulf War.

- Presence of a highly-educated elite committed to acquisition and exploitation of state-of-the-art communications and Internet technologies.

- Evidence that the regime is funding, training, and harnessing human resources in the ICT field, drawing, for example, on Iranian expatriates trained in computer network engineering, information warfare, and security matters.

- Ministry of Defense funding of dedicated R&D facilities linking the armed services and technical universities (such as Malek Ashtar) concerned with information technologies and national security.

- Evidence suggesting that the clerical regime has taken steps to obtain technical help and training in the computer hardware and software fields from Russia and India—acknowledged leaders in cyber warfare matters.

Annex 1
Government Plans in the ICT Investment Field

In July 2002, the Secretary of Iran's Supreme Information Technology Council, Nasrollah Jahangard, announced that the regime plans to spend the equivalent of $125 million in 2002 to develop information technology and to create jobs.[258] According to the PTT's Acting Deputy Minister for Planning and Development, future infrastructure goals are as follows (through the first phase of the Third Year Plan):

- Providing data network services in 420 points embracing over 180 cities
- Building required infrastructure for "inter-organizational" networks and point to point communication with the capacity of 7000 ports and speed of 64 Kbps up to 2Mbps, covering 1 million end-users
- Providing Internet service and IP national network with a total capacity of 10,000 ports, covering 1000 ISP's and 1 million end-users
- Establishing more than 200 ADSL ports for live video and multimedia services at a speed up to 8 Mbps in 8 large cities[259]

According to Iran's Acting Deputy Minister, the government aims to acquire the capacity to serve 15 million Internet users by 2005 (including 60,000 high-speed line subscribers.) The core network layer will consist of:

- 12 router switches in 10 Iranian states
- Domestic and international STM-16 and STM-4 lines for linking core network switches
- Allocating 10 gateways to PSTN network to transmit domestic and international voice traffic in VoIP form for 8 states in Iran

International connections are planned as follows:

- Fiber optic link with capacity of STM-4 (622Mbps) through Jusk-Fojaireh
- Fiber optic support link with capacity of STM-4 (622 Mbps) through Bandar Abbas-Gheshm-Dubai
- Satellite connections with capacity of 34 Mbps in 8 Iranian states
- STM-1 link with Turkmenistan, Azerbaijian, Armenia, Pakistan, Turkey, and Iraq

[258] Source: RFE/RL: Iran Report, July 15, 2002. Iran Telecommunications Research Center (ITRC). The ITRC is a leading R & D institute that sponsors international workshops in IT and places its engineering prototypes at the disposal of manufacturing centers. According to an authoritative source, ITRC has the following priorities, with the cooperation of Iranian Universities and other research centers: Intelligent networks, Optical Networks, ATM, B-ISDN, High capacity digital switching, VSAT Security, SDH technology, Rural telephony systems, "Iran's Telecom and Internet Sector: "A Comprehensive Survey," Open Research Network, June 15, 1999

[259] "ICT Status in the Islamic Republic of Iran," presented by Masoud Ghazvin, Acting Deputy Minister for Planning and Development, MPTT, at the AIIS Meeting in Brunei, August 5-9, 2002

Overall, the goal of the PTT by 2005 is to connect 300 cities to the national data network. Capacity of each urban connection and international lines would be 80 Gbps and 3.4 Gbps, respectively.[260]

[260] Ibid Ghazvin 2002

V. NORTH KOREA

CHARLES BILLO

Our party's military-first ideology explains the need to push ahead with the revolution and construction through the constant enhancement of the revolutionary army's position and role. By comprehensively embodying the demands of military-first ideology, great Comrade Kim Chong-il is wisely leading the advance of the 21st century in order to achieve the victory of the independent cause.

Excerpt from Democratic Peoples Republic of Korea's
Military First Doctrinal Declaration, published in Nodong Sinmun, March 21, 2003

I believe that the North Koreans, whatever their limitations, have a capacity to think deeply and innovatively about military affairs…And what I have observed over the years convinces me that they are devoting considerable attention to cyber war."

John Arquilla, RAND consultant, *Wired News*, June 2, 2003

In a report to South Korea's National Assembly's National Defense Committee, the country's Defense Ministry warns that North Korea has developed an advanced cyber warfare capability that could be used to gather intelligence or launch cyberattacks against South Korea, the United States or Japan. According to the report, North Korea has trained 500 computer hackers in advanced cyber attack techniques, and the recluse state's cyber warfare capabilities "have reached the levelof advanced countries."

Agence France Presse report from Seoul, October 4, 2004

The DPRK does have several dozens of modern telecommunications facilities and academic research institutes with sophisticated telecommunications equipment, allowing them access to and use of modern telecommunications technologies, including wireless radio and telephone, satellite communications, and the Internet…The real puzzle is how the North Korean telecommunications personnel are still able to maintain in good working condition most of the telecommunications facilities and equipment, despite enormous material, technical, and financial difficulties facing them today.

Alexandre Mansourov, "Bytes and Bullets: Impact of IT Revolution on War and Peace in Korea," October 2002

5.1 BACKGROUND

Episodes such as Operation "Eligible Receiver," a 1997 Pentagon exercise in which a red team assembled by the U.S. intelligence community posed as North Korea, have fostered popular interest in Pyongyang's putative cyber capabilities. In reality, the Democratic People's Republic of Korea (DPRK) represents a complex, enigmatic puzzle. On the one hand, the regime obsesses about national security and espouses a rigid "military first" doctrine that dictates priority funding to the Korean People's Army (KPA). On the other, North Korea's documented dependency on outside economic and technical aid and illicit foreign trade suggests economic backwardness and impaired military readiness that calls into question offensive capabilities.[261]

[261] In the 1980's and early 1990's, conventional wisdom in Western military circles held that the KPA was well-trained and disciplined but its weaponry lacked the sophistication and reliability of the NATO arsenal. More recent information indicates that "chronic fuel shortages…have curtailed the military's ability to conduct exercises and to maintain combat readiness." <http://www.asiaint.com/acr/North_Korea/security.asp>

It is generally accepted that the Hermit regime led by Party Chairman Kim Jong-il has long been paranoid about national defense and military preparedness. In addition to sparring politically with Seoul, the civilian and military leaders obsess about the possible military threat from South Korea—supported by the United States. The presumptive threat "justifies" popular sacrifice.[262]

Given North Korea's modest GDP (estimated at only $22 billion in 2002, about equivalent to El Salvador or Lithuania but with a population 6 times greater) and meager natural endowments, the government's room for maneuver is severely limited. Aid agencies note the DPRK's dependence on outside food and fuel assistance and dearth of investment capital.[263] Visitors with access to cities and regions beyond the capital assess civilian transportation and communications infrastructure as rudimentary at best.[264]

A decade ago, Pyongyang adopted a military strategy based on asymmetric advantage to leverage its meager financial resources, i.e., leveraging a relatively modest investment in resources to obtain a disproportionate impact in influence or deterrence.[265] In this context, the DPRK began to develop or acquire sophisticated military technologies such as long-range missiles and nuclear devices, which would not only deter adversaries in Northeast Asia and earn the regime potential export revenue, but also provide diplomatic bargaining chips in securing concessions from its neighbors. At the same time, the regime stepped-up investment in military-related R&D in the computer hardware and software domain.[266]

The DPRK currently allocates an estimated 25 to 35 percent of its GDP to military expenditures.[267] Despite the budgetary weight given to the military, experts assess the armed forces are only "modestly digitized." For example, Alexandre Mansourov, a former Soviet diplomat stationed in Pyongyang, observes that the Korean People's Army (KPA):

> Is still predominantly an 'analog and tube' force equipped with 'appropriate' technology, often going back to the days of the Korean War, not 'cutting edge' technology. The level of IT expertise within the KPA and the North Korean defense industry is low, and we tend to overestimate it.[268]

---

[262] South Korea exceeds its rival to the north in military strength and the military gap continues to widen, according to a military expert at Kyungnam National University. South Korea has been focusing on building up the quality of its military power through further "informatization" while acknowledging its inferiority on a strict numerical basis. "ROK Militarily Overpowers NK," *Korea Times*, April 25, 1999

[263] "North Korea: Economic Reforms Paying Off?," AsiaInt Reference Library <http://www.asiaint.com/arl/arl3865.asp?action>

[264] See CIA, *The World Factbook*, 2003

[265] See, for example, Jonathan B. Tucker, "Asymmetric Warfare," *Forum for Applied Research and Public Policy*, p. 6, available at <http://forum.ra.utk.edu/1999summer/asymmetric.htm>

[266] Consistent with the "military first" doctrine, under which Internet access, laptops, wireless communication devices, and other technical advances are allegedly extended to senior party officials, military commanders, and state security operatives. See "DPRK Cabinet Paper Urges Raising Information Industry to World Class Level," FBIS Translation of North Korean news organ, December 18, 2002

[267] See Edward B. Atkeson and Peter Gillette, "North Korea: The Eastern End of the Access of Evil," *Landpower* Essay, November 2002, p. 3

[268] Alexandre Mansourov, "Bytes and Bullets: Impact of IT Revolution on War and Peace in Korea," October 2002

Figure 1: A Note on Sources and Disinformation

Assessing North Korea's military strengths, including its cyber warfare capabilities and intentions, entails distinct challenges.

First, the reclusive, Stalinist leadership and a closed society render reliable information difficult to obtain.

Second, DPRK leaders are reputedly masters of propaganda and deception. Deliberate "disinformation" campaigns are often used when the government wishes to hide lapses or tout accomplishments that may have never been achieved. Due to the government's authoritarian control, disinformation activities are often easier to conceal than in societies that are more open. Public relations campaigns notwithstanding, foreign observers generally agree that North Korea's underlying natural resource base, transportation and communications infrastructure, and technically competitive workforce are minimal.[269] Beneath the veneer of military-technical exploits, the reality is that North Korea is one of the poorest countries in the world.

Disinformation is not solely in the domain of the North, however. South Korea's intelligence services reportedly engage in propaganda and deception. Elements in South Korea's defense sector have a vested interest in misrepresenting the potential threat from the North. Placing fabricated or exaggerated reports in the popular media about Pyongyang's military plans is a means to promote continued U.S. military presence in South Korea, generate defense industry contracts, and sustain local investment in military research and development.[270]

A report that some experts attribute to the Defense Security Command in Seoul states, for example, that in 1986 a five-year program under the name Mirim College (later renamed the Automated Warfare Institute, according to South Korea's National Intelligence Service) was created for DPRK military forces.[271] The mission of the facility at Mirim is reportedly to "educate a corps of professional military technicians for creation and management of military

[269] North Korea lags considerably behind its neighbors in output and electric power generation. See country data in CIA *The World Factbook*, 2003. Electric power outages and brown outs have severely constrained domestic economic development for many years. David Van Hippel, Nautilus Institute, as quoted in *The* Asia Network," *Asahi Shimbun*, Tokyo, "2002, p. 2 <http://www.asahi.com/english/>. The collapse of the Soviet Union in 1990 and the withdrawal of Russian experts and aid to the DPRK resulted in the loss of approximately half of North Korea's annual supply of crude oil. See discussion by David Van Hippel, Nautilus Institute, op.cit., p.1. While subsequent barter arrangements with China have compensated to some degree, the DPRK nonetheless continues to experience severe energy (and electrical power) shortfalls.

[270] Brian McWilliams, "North Korea's School for Hackers," *Wired News*, June 2, 2003 <http://www.wired.com/news/politics/0,1283,59043,00.html>. In mid-2003, Major General Song Young-guen, South Korea Defense Security Command, reportedly observed that Pyongyang graduates "100 hackers annually." He added that he could not discuss the evidence. Sydney Morning Herald, "North Korea Suspected of Training Hackers," Seoul, June 10, 2003. The same individual reportedly stated in early 2004 that Kim Jong-il formed a hacking group to collect information from South Korea's institutions. <http://english.chosun.com/w21data/html/news/200405/200405270038.html>

[271] Original source of the information is South Korea's Ministry of National Defense. We have found no independent confirmation or sourcing for information relating to alleged official training for hackers in North Korea.

computer system[s], and … other fields such as electronic warfare…The institute's general curriculum is divided into five majors, including command automation, computers, programming, automated reconnaissance, and electronic warfare."[272] Reportedly, about ten percent of each class is assigned to work for "the People's Armed Forces Ministry surveillance bureau, where their duties consist of searching the Internet and also of carrying out hacking activities."[273] Disinformation from both countries complicates efforts to discern the truth about intentions and plans in the Hermit regime.

5.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

During the research for this report, no public DPRK statement of the regime's cyber war plans, capabilities, or intentions was found. Some evidence suggests, however, that KPA officers continue to engage in liaison and training exercises with their counterparts in China—a state that not only is an avowed proponent and practitioner of Information Warfare but also possesses a dedicated training facility, the Communication Command Academy in Wuhan.[274]

Western security experts have included North Korea in their assessments of countries that are developing a cyber attack capability. In 2002 Richard Clarke, a former Special Advisor to the President for Cyberspace Security, testified that North Korea was one of the nations "developing information warfare units, either in their military, or in their intelligence services, or both."[275] Former Australian Defense Force officials believe that North Korea is actively probing Australia's cyber infrastructure.[276]

An unclassified Canadian Intelligence Service publication, in reference to American military and Congressional reports, states "North Korea, Libya, Iran, Iraq, and Syria have some IO [information operations] capabilities."[277]

Western open source discussions of North Korea's military doctrine emphasize surprise and a rapid thrust into the South. Reportedly, the KPA's overall objective is to "disturb the coherence

[272] See Republic of Korea's National Intelligence Service, section on North Korea, "Automated Warfare Institute," <http://www.nis.go.kr/eng/north/education20.html>

[273] FBIS translation of Seoul Yonhap, semiofficial news agency of the ROK, article "Further on DPRK Developing Missile Guidance Control Software," December 3, 2001. See also FBIS translation of Seoul Yonhap article "Review of Digitization Level in DPRK," July 22, 2000

[274] See "North Korea Radio Reports Military Leaders' Meeting in China," BBC Monitoring International Reports, April 22, 2003 and Uri Fisher, "Information Age State Security: New Threats to Old Boundaries," Department of Political Science, University of Colorado, Boulder CO, 2001, p. 6, available at <http://www.isanet.org/noarchive/urifisher.html> For further information about China's cyber warfare capabilities see pages 25-40 of this report.

[275] Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security, February 13, 2002 Event: Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee, hearing titled "Administrative Oversight: Are We Ready for a Cyber Terror Attack?" Source: Tech Law Journal transcribed from its audio recording of the event.

[276] *Sydney Morning Herald*, "Internet Flaws Spark Alert on Cyber Terrorism" Feburary 16, 2002

[277] Canadian Security Intelligence Service, "Information Operations," May 6, 2002 <http://www.csis-scrs.gc.ca/eng/miscdocs/200111_e.html>

of South Korea defenses in depth—including its key command, control, and communications, and intelligence infrastructure."[278]

The countries neighboring North Korea have adopted a higher cyber alert status in response to a perceived threat increase.[279] South Korea's recent cyber defense initiatives, for example, reflect concern over potential vulnerability. The ROK military staged its first mock battle to practice Internet-related warfare in August 2001.[280] Although there is no open source reference to an attack scenario involving North Korea, the cyber battle—during the annual joint U.S.-ROK Ulji Focus Lens exercise—taught the military to defend computer networks from possible hacking and virus attacks. The drill reportedly ran through a cyber warfare defense system called Infocon at South Korea's JCS Headquarters.[281] The ROK's military is operating a Computer Emergency Response Team and has recently automated the security procedures for its officers.[282]

Figure 2: South Korea as a Potential Cyber Target

South Korea's network vulnerabilities are also well known. For example, it is widely recognized that the Slammer worm almost crippled all Internet access in South Korea.[283] ROK officials reported in early 2000 an increasing number of overseas web intruders exploiting South Korea's weak computer defenses to launch attacks on foreign sites. "Statistics showed that in January alone South Korea chalked up 32 cases up from 18 cases a year earlier, in which foreign hackers intruded into its computer systems and used them as launching pads to assail foreign websites," a KISA spokesman said. "We have a good network environment in this country but we are suffering from a great shortage of people in charge of security," the spokesman continued.[284]

South Korea represents an attractive target for potential cyber attackers in North Korea. Seoul is an acknowledged leader in broadband technology.[285] A May 2002 briefing by the ROK Ministry of Information and Communication noted that South Korea has "the world's best info-communications infrastructure and a dramatic increase of Internet users." At the end of 2001, South Korea had an estimated 25 million Internet users, and more than 7.8 million broadband subscribers.[286]

[278] See GlobalSecurity.org, "Doctrine," <http://www.globalsecurity.org/military/world/dprk/doctrine.htm> North Korea stations 70 percent of its army in offensive positions within 100km of the DMZ.

[279] "Almost 50 years after the establishment of the Japanese Self Defense Forces (SDF), the time has come for the forces to make adjustments to keep pace with the changing times, especially in terms of IT. It is crucial that the nation be ready to counter modern threats, such as cyber terrorist attacks….Since the 1991 Gulf War and the NATO bombing of Yugoslavia last year, computer warfare has become a reality." *The Daily Yomiuri* (Tokyo) August 8, 2000

[280] "Military training for Net attack," *Korea Herald*, August 14, 2001

[281] "Silicon Valley, Pyongyang," *Business Asia*, April 2, 2002

[282] *Korea Times,* "Army Tightens Operation Security," August 26, 2003

[283] *Washington Post,* "Internet Worm Hits Airline, Banks," January 26, 2003 <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A46928-2003Jan26&notFound=true>

[284] "South Korea faces increasing onslaughts from Web attackers," *Agence France Presse*, February 11, 2000

[285] For a thorough review of broadband availability in South Korea, see "Kyounglim Yun et. al. "The Growth of Broadband Internet Connections in South Korea: Contributing Factors," Asia/Pacific Research Center, Stanford University, September 2002, available at <http://APARC.stanford.edu>

[286] Korea Ministry of Information and Communication, "Briefing," May 21, 2002, p. 4

Seoul, according to the Ministry of Information and Communication, is experiencing both an increased dependency on IT systems (for business and education) and greater interdependence (and also vulnerability) because of various government, university, and business networks.[287]

South Korea's relatively unprotected networks and systems might provide a platform for clandestine attacks against Seoul or third countries. [288] A theoretical possibility would be a cyber-terrorist attack either directly against South Korea or exploiting the ROK as a proxy for a wider attack.[289] Linguistic, cultural, and other affinities between North and South would certainly facilitate hackers in Pyongyang compromising servers in South Korea. As noted above, academic IT experts and researchers in Seoul and Pyongyang often exchange information about professional matters of common interest.[290] In this context, university computer servers reportedly are especially vulnerable to hacking because security measures are lax and universities invest in networked broadband technologies.

Overall, the meager unclassified evidence suggests that the DPRK has a rudimentary electronic warfare capability (e.g., jamming). It is possible Pyongyang possesses a capacity to compromise IT networks or hack into protected South Korean or United States databases. However, this finding represents little more than conjecture based on doctrinal considerations, such as the military first strategy, and documented testing of adanced missile and other military technology components.[291]

5.3 MILITARY AND INTELLIGENCE AGENCY RESEARCH

CIA and other published sources estimate annual military expenditures in North Korea at slightly over $5 billion. This estimate compares with $12.8 billion in South Korea, $9.7 billion in Iran, $8.97 billion in Israel, $4.47 billion in Singapore, and $3.113 billion in Norway.[292] These comparative figures should be considered only as general orders of magnitude, however, because of issues with input data and different assumptions and accounting methods employed.

According to South Korea's Ministry of National Defense, sources of funds for the DPRK's military budget include weapons exports and profits "reinvested" in the budget from direct production of weapons and farming activities. Profits from illicit activities such as narcotics trade and remittances from the Chosen Soren (Korean nationals resident in Japan—see figure 3)

[287] Ibid Korea Ministry of Information and Communication p. 5

[288] "There are many places around the world from which [North Korea] could conduct cyberwar, places that have all the connectivity needed, and more." John Arquilla, RAND, as quoted in McWilliams, op. cit., p. 3

[289] As discussed above, North Korea has a long history of involvement in international terrorism. Its intelligence services have targeted South Korea and other countries, such as Japan.

[290] For example, as recently as two years ago, an ROK official noted that South Korea's sites are weaker than foreign sites. Reportedly hackers log into overseas servers through South Korea's sites, op. cit., *Agence France Presse,* February 11, 2000, p. 2. In one case of web "infiltration" in South Korea, Hungarian police in 1999 arrested a Web attacker who invaded databases of hospitals. It turned out that the assailant was using a server computer of a University in South Korea.

[291] See "DPRK Cabinet Paper Urges Raising Information Industry to World Class Level," FBIS Translation of North Korean news organ, December 18, 2002

[292] See CIA, *World Fact Book*, 2003 and GlobalSecurity.org, "World Wide Military Expenditures," <http://www.globalsecurity.org/military/world/spending.htm>

reportedly also contribute significantly to supporting military investment. [293] Reliable published information on Pyongyang's programmatic or weapons systems outlays under the overall military budget, however, is non-existent. Regardless, it is clear that the DPRK annually has far less to spend on its military priorities than its neighbors in East Asia. To compensate, the regime resorts to various stratagems to obtain hardware, software, and engineering plans on the cheap from sympathetic foreign governments and private entities.

U.S. military and civilian experts assess that the DPRK is adept at collecting proscribed foreign technologies necessary to compete militarily in East Asia.[294] For example, in addition to exploiting unwitting high-tech investors and visiting academics, North Korea employs various assets, such as embassy defense attaches overseas and intelligence collection services engaged in industrial espionage, to obtain proprietary information and prototype hardware. The Chosen Soren, through front companies and similar techniques, procures state-of-the art hardware and software on behalf of North Korea.

Figure 3: General Association of Korean Residents in Japan (Chosen Soren)

Chosen Soren, the association of Korean residents in Japan, was founded in May 1955. Media sources estimate the organization has about 200,000 members. Its structure embraces a headquarters in Tokyo, regional head offices and branches, and 23 business enterprises. The name "Chosen" derives from the period of Japanese occupation of the Korean peninsula. Korean residents in Japan who choose not to adopt South Korean citizenship remain "Chosen nationals" under Japanese law.

Through several illicit activities and enterprises under its control, the Chosen Soren remits hard currencies to North Korea. According to published reports, the Japanese police testified in 1994 that about $600 million annually was remitted to Pyongyang, although the annual amount has since declined.

Gakushu-gumi is Chosen Soren's underground organization. It is connected to the North Korean Workers Party. Reportedly the Gakushu-gumi engages in intelligence activities of various types, such as information gathering and diversion of advanced technologies for use by North Korea. [295]

The State Security Agency (SSA), under the direction of Kim Jong-nam, the eldest son of the DPRK leader, covers a range of counter intelligence and security duties normally associated with the secret police. According to an informed source, the SSA "has counter intelligence responsibilities at home and abroad, and runs overseas intelligence collection operations…The agency also guards national borders and monitors international entry points."[296]

[293] ROK Ministry of National Defense, "Comparison of Economic Indices between North and South Korea," February, 1999 <http://www.mnd.go.kr/english/html/02/1999/sub8.htm>

[294] See "North Korea: Background Information," pp. 12-13, available at <http://www.ironsides.8m.com/army/kn.html>

[295] GlobalSecurity.org, "General Association of Korean Residents in Japan," July 15, 2002 <http://www.globalsecurity.org/intell/world/dprk/chosen_soren.htm>

[296] GlobalSecurity.org, "State Safety and Security Agency State Security Department," July 15, 2002 <http://www.globalsecurity.org/intell/world/dprk/ssd.htm>

Media reports state that the Chairman's son, Kim Jong-nam, head of the National Defense Commission, consolidated the SSA's overseas intelligence gathering unit, which engages in hacking and monitoring foreign communications, into the Korean Computer Center (KCC) in Pyongyang. Recent reports indicate that the KCC is the hub of the Hermit regime's information technology planning. The facility reportedly is technically equipped and houses some 800 employees. Despite industrial country agreements restricting access to dual-use technologies such as advanced computers, the KCC and other North Korean facilities nevertheless obtained these illegally from Europe, Japan and other suppliers.[297] A South Korean firm, BIT Computer, reportedly has a contract to train the KCC's work force.[298] According to a journalistic account:

> The KCC, which used to be understood merely as a research institute developing software, is confirmed to have carried out, under Kim Jong Nam's initiatives from the outset, functions of a 'clandestine overseas information command center' under the jurisdiction of the SSA. Having been involved since the late 1980s in the SSA's overseas information gathering through communications monitoring and computer hacking, Kim reportedly found it necessary to reinforce the information gathering functions and develop the computer industry at the same time.[299]

One of the current functions of the KCC, according to a recent article on IT developments in North Korea, is to monitor the web sites of major government agencies and business establishments: "Its activities include communications monitoring and hacking, putting even innocent seeming work like language and voice software in a different light."[300] The DPRK reportedly is interested in blueprints or technical specifications (or any vulnerabilities and loopholes) in foreign systems and technologies. South Korea's technology firms, as well as academic and quasi-government defense research agencies, represent potential targets.[301]

Assuming published reports about the SSA's involvement in the work of the Korea Computer Center are accurate, these reports would support the case that Pyongyang is pursuing a cyber attack capability involving computer hacking against foreign targets. An academic center with a number of legitimate activities would provide a reasonable cover for computer software development and other techniques applicable to cyber warfare.

5.4 INFORMATION TECHNOLOGY INVESTMENT

The senior leadership in Pyongyang is paying growing attention to the IT sector. A reputed "media junkie," Chairman Kim Jong-il has experimented with the Internet and the World Wide Web.[302] According to numerous journalistic accounts, the DPRK leader has personally promoted inward direct investment in computer software and communications technologies. He also supported the creation of a domestic intranet to facilitate communication among military,

---

[297] AsiaInt, "Political and Strategic Review," September 2001 p. 4 <http://www.asiaint.com/psr/indexfree.asp>
[298] See "Head of South Korean IT Startup to Visit N. Korea Next Week," *Asia Pulse*, (Seoul) January 26, 2001
[299] "True Aspects of the Korea Computer Center," *The Chosun Ilbo*, May 13, 2001
[300] Ibid *The Chosun Ilbo* p.1
[301] Source AsiaInt, "Political and Strategic Review," September 2001 <http://www.asiaint.com/psr/secure/hal.pdf>
[302] See "DPRK Cabinet Paper Urges Raising Information Industry to World Class Level," FBIS Translation of North Korean news organ, December 18, 2002. The favorite Internet sites of Kim Jong-il, who allegedly likes computers and is very interested in information technology, include such South Korean sites as National Intelligence Service and the Unification Ministry. "NK Leader Regularly Surfs ROK Websites," *Korea Times*, April 12, 2002

political, and academic elites.[303] In the last decade, the DPRK is reported to have studied Internet firewall applications to shield sensitive domestic communications and databases from outside intrusion.[304] In addition, the Chairman's son Kim Jong-nam, controls the programming activities at the North Korean Academy of Sciences, the Pyongyang Information Center, Yakchon Research Institute, Kim Il Sung University, and Kim Chaek Institute of Technology.[305]

In the mid-1990s, the gradual reduction in tensions between Seoul and Pyongyang and the loosening of international trade restrictions helped accelerate the rate of political and economic change on the peninsula and in the region as a whole.[306] Various reports indicate Kim Jong-il and his associates—based on outreach to China, Japan, and other neighbors—embraced the IT sector as a potential source of future economic competitiveness and growth.[307] For example, the demise of the Soviet Union and transformation of China to a quasi "market" economy forced Pyongyang to fend for itself to a greater degree and develop alternative sources of foreign exchange. The leadership calculated that participation in the global digital economy as a software exporter might generate foreign exchange over the longer term and offer North Korea an escape from its endemic economic woes. At the same time, however, the regime recognized that distributed communications connectivity at the grass roots level was potentially dangerous if it implied loss of central political control.[308] The DPRK in recent years has successfully attracted IT infrastructure and related scientific investment from South Korea, China, and Japan, even though the DPRK has a long standing reputation as an opportunist and "deadbeat" in international commercial and investment circles.[309]

As mentioned earlier, the information technology sector in North Korea is designed primarily for military, governmental, and industrial use; expansion and development of telecommunications networks and facilities are not consumer-driven. Gunter Unterbeck is vice president of KCC Europe, a firm that delivers Internet service to the state-run Korea Computer Center. According to a report in *Newsweek*, Jan Holtermann, a fellow German who co-founded the company, "in January [2004] announced a contract to provide Internet service in partnership with the state-run Korea Computer Center. The Germans have since invested an estimated $1 million in computer equipment and a satellite link to Internet servers in Berlin. The link works, but so far Pyongyang

[303] Under the direction of the Central Science and Technology Information Agency, several North Korean organizations, such as the Kim Il Sung University, the Patent Bureau, the Korean Computer Center, and the Pyongyang Informatics Center, are linked to an internal computer network. This so-called "Intranet" provides: S &T database search (Kwangmyong-16.5 million items), E-mail system, File Transfer system, and Electronic News System. For a lucid discussion of the activities of the CSTIA, see: Stephen C. Mercado, "Hermit Surfers of Pyongyang," *Studies in Intelligence*, Vol. 48, No. 1, 2004 <http://www.cia.gov/csi/studies/vol48no1/article04.html>

[304] Lee Kyo Kwan, "NK Nearly Ready to Access Internet," *The Chosun Ilbo* September 13, 2001

[305] See "True Aspects of the Korea Computer Center," in *The Chosun Ilbo*, May 13, 2001, p. 1

[306] "Rise in Overseas Travel by NK officials Indicates Shift in Policy," *Korea Herald*, January 14, 2000

[307] See, for example, "Silicon Valley, Pyongyang?" *Business Asia*, April 2, 2001, p. 12-13; and Scott Snyder, "The Winds of Change: Fresh Air or Pollution?," *Comparative Connections*, April 2001 <http://www.csis.org/pacfor/cc/0101Qchina_skorea.html>

[308] Alexandre Mansourov, op. cit.

[309] As an indicator of DPRK commercial opportunism, see Pyongyang's recent efforts to link electrical power supplies (to North Korea) to its approval of proposed investment projects in the technology sector. See, for example, "Conditions for ROK to Provide Aid to DPRK Examined," FBIS Translation of *Chungang Ilbo*, (Seoul) December 23, 2000 and "North Korea calls for Power Supply from South," FBIS translation of *Seoul Yonhap*, December 28, 2000

has not yet opened it to the public."[310]

North Korea's civilian telecommunications technology lags far behind that of South Korea.[311] According to figures in the CIA *World Factbook*, the North has 1.1 million main telephone lines in use compared to 24 million in the South.[312] A recent South Korean report noted that the phone systems in Pyongyang and major cities are automatic but systems in rural areas remain hand operated.[313] Pyongyang may have as few as 2700 public telephones in a city with a population of about two million.[314] More fundamentally, as Peter Hayes of the Nautilus Institute has pointed out, the DPRK's lack of basic necessities—such as a reliable electrical grid—poses an obstacle to infrastructure development.[315] The primitive state of the domestic telecommunications infrastructure contrasts sharply with North Korea's emerging effort to provide to favored official elites international fixed line, wireless, and satellite communications options. Basic service reportedly is available to senior party, government, and military officials and to foreign guests. Recent developments in fiber optics, mobile telephones, and rudimentary Internet and email connectivity are of particular interest. [See Annex 1]

During the last decade, a growing number of South Korean and Japanese business investors and academic computer experts visited Pyongyang. In the course of such visits to DPRK institutes and universities, several recorded their observations. One expert, for example, reported observing PC's and work stations in the following range: 386, 486, Pentium, NEC 9801 series, SUN, Sony, DEC (Alpha Chip).[316] Civilian computer access is extremely limited. According to a report, North Korea is said to have "only about 100,000 plus computers for private use, most of them in the 386 class."[317] Reportedly, North Korea produces 32-bit microprocessors and is actively researching 64-bit computers.[318]

Pyongyang announced in May 2001 that it had produced 1300 "up-to-date" computers in February and distributed them to local educational institutions.[319] A June 2001 report from a DPRK news organ in Tokyo indicated that North Korea "has opened its first PC manufacturing plant and has already produced hundreds of Pentium and Celeron-class machines."[320] The

[310] Ron Gluckman, "Beyond the Net's Reach," *Newsweek*, October 18, 2004

[311] According to published statistics, there are about 2 million televisions, 2.5 million radios, and 1.1 million telephones. This translates to 1 per 11.5, 1 per 9.2, and 1 per 21 people, respectively. Chan-mo Park, "Current Status on IT in DPRK and Mutual Cooperation Between South and North," [PowerPoint Presentation], November 13, 2000 p. 13 <http: www.cgvr.postech.ac.kr/cmpark>

[312] CIA, *The World Factbook*, 2002

[313] "KT Kicks Off Campaign Against 'Digital Divide'," *Chosun Ilbo* (Seoul) June 24, 2002

[314] "KT Kicks Off Campaign Against 'Digital Divide'," *Chosun Ilbo* (Seoul) June 24, 2002. On the subject of Pyongyang's population, there are no official statistics. Thus an estimate is given based on a number of sources. The estimate here is derived from the Federation of American Scientists, "WMD Around the World: Urban Areas," June 11, 2000 <http://www.fas.org/nuke/guide/dprk/target/urban.htm>

[315] McWilliams, op. cit. p. 2

[316] See Chan-mo Park, op.cit. p. 10

[317] "Pentium-class Computer aid to North Korea debated," *The Chosun Ilbo,* February 2001 <http://nk.chosun.com/english/news/news.html?ACT=detail&cat=10&res_id=3692> See also <http://www.koreascope.org/english/sub/2/nk3>

[318] Chan-mo Park, op. cit., p. 9

[319] Source: <http://biz.yonyapnews.co.kr> as reported in CanKor, University of British Columbia, "Program on Canada-Asia Policy Studies," <http://www. pcaps.iar.ubc.ca>

[320] IDG News Service, "North Korea Making Pentium-class PC's," in *Computer World* (Hong Kong), June 11, 2001

computers reportedly are being installed in educational institutes intended to provide computer-training courses to talented youth.

In September 2002, Panda Electronic Group of China and the DPRK's Ministry of Electronics Industry established a joint venture to develop, manufacture, and market computers and peripherals.[321] A 2003 report outlines a yearly production figure of 135,000 computers.[322] TASS, the Russian state-controlled news agency, reported in July 2003 that computers assembled in North Korea were displayed for sale at an international industrial exhibition held in Vladivostok.[323]

Figure 4: Technical University R & D

There is credible evidence that the leadership in Pyongyang gives priority to applied scientific research. The quality and breadth of technical and professional journals in the electronics, information technology and related fields demonstrates the regime's commitment to advanced sciences.[324] Second, Pyongyang continues to exploit the post-Cold War relaxation of tensions in East Asia to attract foreign direct investment in communications infrastructure improvements.

Several North Korean academic institutions offer scientific research and training programs that in some cases are directly applicable to integrated information technologies and computer systems, software development, programming, and information warfare. Computers and software reportedly are accessible to leading academic research bodies. Both theoretical and practical work has been advanced through the use of this advanced technology.

As with the investment liberalization measures currently under way in the Info-Tech sector (see page 5 above), the leadership seems to have adopted China's approach by employing academic research institutions to facilitate research in military information warfare programs. In recent years, for example, key technical academic institutions, such as the Academy of Sciences and Kim Il Sung and Kim Chaek Universities, have opened computer colleges and expanded computer teaching and research faculties. Sources deemed to be reliable also assert that similar North Korean institutions, such as the Korea Computer Center and the Pyongyang Informatics Center, are directly engaged in national security work, especially information gathering and potential cyber warfare activities such as malicious hacking. Reportedly, these institutions enjoy significant budgetary resources.[325] The following passages outline examples of the programs and research in these institutions.

The Academy of Science's computer division reportedly is engaged in theoretical and practical research in computer science. According to an informed observer, its long-term plan embraces development of computer programs for domestic use and export; manpower training; and

[321] "North Korean PM Praises Joint Venture with Chinese Computer Firm," BBC Monitoring International Reports, September 17, 2002

[322] BBC Monitoring Service, "North Korean-Chinese Joint venture reportedly Producing Computers," March 17, 2003

[323] ITAR-TASS News Agency, "North Korean computers displayed at Vladivostock exhibition," July 4, 2003

[324] See "DPRK S&T Report: Electronics" FBIS translation of NK Journal, April 10, 2002, and "NK also has Digital Leaders: Researchers," in *Asia Pulse*, June 23, 2000

[325] "True Aspects of Korea Computer Center," *The Chosun Ilbo*, May 13, 2001

distribution of software technology and products. Among the Academy's current research interests are: Korean character recognition, machine translation, data compression, relational data base systems, bank management systems, and voice recognition. Reportedly, the Academy has been responsible for many application and edutainment programs, some of which are marketed by the Paeksong Trading Corporation.[326] According to a North Korean media report, a new school of "information technology" was established at the Academy in early 2002. Training embraces subjects such as programming digital controls, semi-conductor design, and precision machinery, with a teaching staff that includes prominent scientists and technicians drawn from various institutes within the Academy.[327]

Kim Il-sung University is engaged in research and development in cooperation with computer science faculties elsewhere. The university's computer center was established in 1985. An informed observer states that the university in 1994 had more than 200 PC's for student use. The university has been responsible for development of the following software: Intelligent Locker (Hard Disc protection program); Worluf Anti-virus (broadband anti-virus program); SIMNA (simulation and system analysis program); a war game program; Hepatitis Diagnosis and Prescription System; and FC 2.0 (A highly portable C++ program development tool).[328]

Kim Chaek University of Technology, founded in 1948, underwent a significant reorganization in the late 1990s. According to a 2002 article, the university has established three colleges addressing computer science, information science and technology, and machine science.[329] Over 2000 students graduate from the University annually.[330] In an interview published by The People's Korea, a Tokyo based unofficial web site of the DPRK, Chong Gwang Chon the Chief of Academic Studies at Kim Chaek University said "our University has been doing academic exchanges with neighboring countries such as China…It is planned to increase opportunities to hold exchange meeting [sic] with foreign Universities such as Universities in Europe.[331] Among the software programs listed at the university are Computer Fax (communications software) and Materials Security Software (SGVision.) SGVision is an image-reprocessing program with a steganographic function.[332]

Pyongyang Informatics Center (PIC) was established in 1986. The PIC reportedly hosts more than 120 research scientists and is equipped with an average of 1.5 computers per person. This institution is reportedly a leader in Korean language processing and word processor

[326] Chan-mo Park, op. cit. p. 17

[327] "North Korea's Academy of Sciences Sets Up It [sic] School," BBC Monitoring, text from *KCNA*, January 14, 2002

[328] Chan-mo Park, op. cit. p. 19-20

[329] "DPRK's Recent Moves to Foster IT Industry Viewed," *Financial Times Information*, Global Newswire, November 23, 2002

[330] FBIS report, "Kim Chaek University of Technology Profiled, Software Programs Listed," from DPRKorea Infobank, May 15, 2002

[331] The People's Korea, "Interview with Chong Gwang Chon" (Date unknown) <http://210.145.168.243/pk/171st%5Fissue/2001120203.htm>

[332] The specifications for the Materials Security Software (SGVision) are provided in a marketing brochure that was prepared in connection with the April 20-22, 2002 DPRK software expo in Beijing. The brochure notes: "When transmitting secret materials through the Internet, much time and vigor (sic) are saved, and commercial profits are defended." FBIS Report, "Software Touted for Hiding Data on the Internet," from DPRKorea Infobank, May 16, 2002

development. The latter program accepts Japanese, Chinese, and Russian characters, in addition to Korean and English.[333] The PIC is responsible for developing the Chang-duk system for MS-DOS and Windows. The Center reportedly has an internal LAN using Novell Netware 3.11.[334] According to a 2002 article, the PIC programming institute is "teaching the development and technology of computer network and multimedia programs, database (Software Information Center) construction programs and others…with a goal of around 2000 people each year."[335]

The DPRK continues to exploit the post-Cold War decline in tensions to seek direct investment in the IT sector and technical assistance from abroad.[336] Pyongyang places high priority on importing advanced technologies and parts for eventual integration into equipment for export. To achieve this, the government recently reorganized and consolidated its foreign trade promotion bureaucracy to facilitate joint ventures and imports from China and South Korea. The Kwangmyongsong Guidance Bureau, for example, through the Kwangmyongsong General Corporation, plays a role in channeling parts from abroad to computer manufacturers in North Korea. [337]

North Korea, for a variety of motives, including a desire to compete in the global Info-Tech economy, is striving to advance in digital technologies and related R & D. Although the Korean Workers Party must remain vigilant in the face of the information revolution to avoid losing political control over the populace, the regime is clearly allocating significant resources to improvements in telecommunications infrastructure, hardware and software acquisition and development, programming research, and related technical training and education. The contribution of foreign assistance to this endeavor is crucial. [See Annex 2]

5.5 CONCLUSION

The totalitarian, paranoid make-up of the regime in North Korea renders leadership intent in the cyber field, military plans, and degree of technical sophistication among the elites difficult to pin down.

A gradual loosening in travel restrictions and international trade in recent years has spawned discussion in the media regarding Pyongyang's interest in digital Internet technologies; acquisition and exploitation of advanced (Western) computer blueprints; experimentation with e-mail and Intranets connecting local universities and scientific institutes; computer science

[333] Chan-mo Park, op. cit. p. 24
[334] Chan-mo Park, op. cit. p. 25
[335] "DPRK's Recent Moves to Foster IT Industry Viewed," *Financial Times Information*, Global News Wire, November 23, 2002
[336] According to South Korea's National Intelligence Service (NIS), beginning in the late 1990s, there was a significant rise in overseas travel by North Korean officials. The NIS reported that North Korean officials made 134 and 222 overseas visits in 1998 and 1999, respectively. This represents a sizable increase from the 99 visits North Korea recorded in 1997. See "Rise in Overseas Travel by NK officials Indicates Shift in Policy," *Korea Herald*, January 14, 2000 and Bae-Seong-in, op. cit. In 1998, South Korea's Ministry of Unification began tracking "Inter-Korean Exchanges and Cooperation" and posting cumulative statistics on its Website <http://www.unikorea.go.kr.en/interkorean>
[337] "Role of DPRK's 'Kwangmyongsong Guidance Bureau' Detailed," *Financial Times Information,* Global news Wire, December 3, 2002

training; and formation of government/academic/enterprise R & D networks patterned after institutions in China. [338]

There are numerous reports beginning in the 1990's describing the DPRK leadership's ambitions to achieve a "digital economy."[339] The unclassified evidence to date, however, suggests that this goal is nothing more than a distant dream on the part of Kim Jong-il and his immediate advisors. As one authority recently observed:

> Grossly underdeveloped electronics and computer industrial infrastructure, morally and physically obsolete and dysfunctional national telecommunications infrastructure, perennial national macro-economic crisis and virtual collapse of the nation-wide power grid, a closed and highly politicized society, and inter-agency rivalry present considerable obstacles in continued development of IT-based C4ISR and EIW capabilities.[340]

Nevertheless, the "military first" doctrine, coupled with a proven capability to focus resources, train personnel, and illicitly procure foreign technical assistance, suggests it is possible that the regime has a rudimentary, exploratory or "pilot" capability to hack or compromise unprotected IT networks or data bases in South Korea or other neighboring countries. This finding represents little more than conjecture, based on extrapolating from North Korea's proven engineering achievements in its missile and related high-technology military programs.

[338] "Universities join hands to form sci-tech centre in Guangdong," BBC, October 18, 2000

[339] See, for example, Bae Seong-in "North Korea's Policy Shift Toward the IT Industry in Inter-Korean Cooperation," *East Asian Review*, Vol. 13, No. 4, Winter 2001, p. 64-65

[340] Mansourov, op. cit. p. 7. C4ISR stands for command, control, communications, computers, intelligence, surveillance, and reconnaissance. EIW stands for Electronic and Information Warfare

Annex 1: Infrastructure Investment

After initial technical and other assistance from the ITU and UNDP in the early 1990s, the DPRK erected a factory for local production of fiber optic cable for use in domestic and international communications.[341] The factory has a research institute to develop replacements for imported materials. By 1998, the DPRK was reported to have connected 36 cities and counties with coaxial fiber optic cables.[342] A 2001 media report noted that North Korea had connected Hamhung, Chongin, Najin, and China's Hunchon with fiber optic lines.[343] In addition, in August 2001 Loxley Pacific (headquartered in Thailand) won a 30 year telecommunications network concession for the "Rason International Telecommunications Center." The latter is used to provide access to international networks from the DPRK.[344] According to sources in South Korea, it is now possible to get international direct dial service to 170 foreign cities from Pyongyang. AT&T has been servicing calls between North Korea and the United States since 1995.[345]

Mobile telecommunications service is mostly limited to military purposes.[346] Early in 2002, the DPRK tested a pilot mobile telecommunications service for 300 users run by Loxley Pacific. The test system is reported to have been based on the European GSM mobile system.[347] This is potentially controversial, however, because South Korea relies on the U.S.-based CDMA system.[348]

The DPRK's limited access to the Internet comes from satellite links provided by a company in South Korea and by landlines from China. According to an informed academic, although North Korea has been assigned the Internet domain name "kp" and Pyongyang may have successfully tested an Internet connection with Australia, the link was not implemented for "political reasons."[349] There are a few North Korean websites hosted in China and Japan, for example <http://www.korea-dpr.com/> and <http://www.dprkorea.com/>.

Kim Chol Hwan, CEO of South Korea's Gigalink Ltd., stated in 2001 that the DPRK has completed the construction of a firewall to protect its intranet (inter-linking domestic science

[341] Mansourov, op. cit. p. 3

[342] See Asian Technology Information Program, "Information Technology in Korea—South and North," 1997 <http://atip.org/ATIP/public/atip.reports.97/atip97.060r.html>

[343] "South Korean IT specialist to attend forum in North Korea," *Yonhap News Agency* (Seoul) January 26, 2001 See also Asian Technology Information Program, "Information Technology in Korea—South and North," 1997 <http://atip.org/ATIP/public/atip.reports.97/atip97.060r.html>

[344] See FBIS report, "4 March Factory Serves Fiber Optic Communications Infrastructure" January 3, 2003.

[345] North Korea participates in Intersputnik and Intelsat. It has an Intelsat earth station in Pyongyang which was erected in 1986. Kim Hoo-ran, "Telecom service in North Korea much like that of South in mid-1970s," *Korea Herald*, June 24, 2000. DPRK officials signed the Intelsat operating agreement in May 2001. "North Korea Joins Intelsat," *Satellite News*, June 4, 2001.

[346] See Manourov, op. cit. p. 4

[347] "North Korea to Build GSM Network," Crain Communications, Global Wireless, December 20, 2002.

[348] The US government opposes the Inter-Korea joint venture to develop the Code Division Multiple Access (CMDA) mobile phone system in North Korea. Seoul's Information Ministry announced in June 2002 a plan to carry out the communication business jointly with the North. The US government controls exports to North Korea, and the CDMA technology belongs to a US company, Qualcomm. Seoul, *Chungang Ilbo*, as translated by FBIS, July 18, 2002

[349] Chan-mo-Park, op.cit., p. 13

institutes and universities) from eventual connection to the Internet. [350] According to media reports, the North has conducted a study on firewalls with Japanese scholars. This is seen as part of preparations for accessing the Internet.[351]

In late 2001, China's Shenyang Public Information Industry Co. Ltd announced the availability of e-mail services to North Korea. [352] Charges for sending and receiving e-mail through this service, called Silibank, are based on the amount of data sent. This service is aimed at corporations rather than individuals. Users must provide contact information including nationality, identify business partners in North Korea, and pay a registration fee of $100. The Silibank e-mail service is available only to registered users and relies on two servers, one in Shenyang and the other in Pyongyang. Outside the DPRK, users connect to the server using an e-mail client such as Microsoft Outlook to send and receive e-mail over the Internet.

Representatives of a Seoul software company, Hoonnet, reported in 2002 that North Korea's Chosun International Communications Center recently opened an Internet network employing landlines. The fiber optic cable allegedly connects Pyongyang and Sinuiju with the Chinese cities of Dandong, Beijing, and Shanghai under a contract with China Telecom. According to this source, the North Korean computer server is in Pyongyang where the so-called "Chosun Internet Joint Venture Company" is located.[353]

The advances made in the telecommunication field have also been seen in computer technologies. The relaxation of tensions on the Korean peninsula beginning in the mid-1990's facilitated South Korean technology exports to the North. Trade between the countries increased from $18.8 million in 1989 to $333.4 million in 1999.[354] According to a recent report from Seoul, through 1999 South Korean civic groups sent a total of 450 sets of computers to North Korea, including 100 sets delivered in September 1998 to Kim Chaek University of Technology by South Korea's Kyungnam University.[355] Such exports are limited by law to 386 class computers.

[350] Op. cit. *The Chosun Ilbo*, September 13, 2001
[351] Op. cit. *The Chosun Ilbo,* September 13, 2001
[352] Silibank can be reached at <http://www.silibank.com> Source: IDG News Service, November 6, 2001 <http://www.itworld.com/Tech>
[353] FBIS translation, "NK Believed to Have Built Internet Network Cable," Seoul Yonhap, 27 March 2002
[354] See Aidan Foster-Carter, "North Korea's Tentative Telecoms," *Asia Times*, July 6, 2002, and U.S. Department of State background note: North Korea, available at <http://www.state.gov/r/pa/ei/bgn/2792.htm>
[355] Kim Ji-ho, "Seoul in dilemma over computer aid to P'yang," *Korea Herald*, January 8, 2000

Annex 2

The following paragraphs highlight a few of the joint business ventures in the IT sector, academic research partnerships, and technical assistance programs involving Japan, China, ROK, and other partners.

Japan

As stated above, the Chosen Soren is a principal conduit of technical assistance to North Korea. It is said to act as North Korea's unofficial embassy in Tokyo.[356] Reportedly, it also assists the DPRK in foreign intelligence operations.[357]

The Chosen Soren develops businesses and "front companies" abroad that benefit the Pyongyang regime by generating hard currency. One such business venture is Unikotech, established in July 2000 with an initial capitalization of 100 million yen. The firm plans to sell software developed by the Korea Computer Center. According to several sources, Unikotech is a joint venture between IMRI (a South Korean producer of computer monitors) and CGS Company, a computer software producer in Tokyo.[358] A press release notes that CGS and KCC in Pyongyang "have been exchanging technological cooperation over the past decade."[359] CGS President RyangYong Bu reportedly played a key role in restoring advanced computer hardware to the KCC following the fire at its headquarters in 1997.[360]

China

Beginning in 1994, experts and specialists from North and South Korea began a bottom-up approach to address information technology issues. An International conference on Korean computer language was held in Yanbian, China in 1994 and each year thereafter.[361] Agreement was reached in four areas: IT vocabulary, keyboard arrangement, character ordering, and coding system.[362] As discussed previously, "top down" initiatives—involving government ministers and/or CEO's of private companies--have accelerated in the last few years, reflecting both a loosening in international political tensions and the high priority accorded to IT expansion.[363]

DPRK leaders have pursued especially close IT cooperation with China. Kim Jong-il has visited China at least twice to study information technology reforms. In May 2000 Kim visited Legend

[356] Federation of American Scientists, "General Association of Korean Residents in Japan," December 22, 1997 <http://www.fas.org/irp/world/dprk/chosen_soren/>
[357] Ibid Federation of American Scientists 1997
[358] See <http://www.imri.co.kr/english/company/company_intro.asp> and <http://www.cgs.com.tw/cgsen/CompanyHistory.htm>
[359] *Japan Economic Newswire*, September 20, 2000. CGS Company sells computer software that enables users to compose text files in hangul. The software is used on computers running the Japanese version of the Windows operating system
[360] See Aidan Foster-Carter, "Pyongyang Watch: Whither the Web," March 1, 2001 <http://www.atimes.com/koreas/CC01Dg01.html>
[361] "IT-In the North," available online at <http://atip.org/ATIP/public/atip.reports.97/atip-97=060-ext-03.html>
[362] Chan-mo Park, op. cit., p. 4
[363] Bae Seong-in, op. cit., pp. 64-65

Computers, Ltd. in Shanghai.[364] Three months later, Pyongyang established an English-language website (providing information on North Korea) on the Internet in Beijing.[365] In 2001 Kim visited China for a week. He toured Shanghai's Pudong Sci-tech district accompanied by 20 high-ranking officials, including the Head of the General Political Department of the KPA.[366] Reportedly, Kim Jong-il's outreach to China has been facilitated by the close relations between his son, National Defense Commission Chairman Kim Jong-nam, and PRC former Chairman Jiang Zemin's eldest son, Stanford-educated Jiang Mianheng.[367] The latter is considered a leading architect of the PRC's IT industry, including the introduction of Linux in China.[368] Jiang Mianheng, Vice President of the Chinese Academy of Sciences, visited IT firms in South Korea in September 2002. He held discussions at a Samsung Electronics factory, met with the Chairman of the Samsung group, and visited Hanaro Telecom.[369]

In April 2002, Pyongyang exhibited its software products at the first session of North Korea Computer Software Expo in Beijing. The products exhibited included a computer operating system developed by Pyongyang, as well as letter/character identification, translation, and finger-print recognition software. The Expo was co-sponsored by the North Korean Academy of Sciences, Panpacific North Korea National Economic Development Promotion Association, and Reese International Group. Panpacific represents the association of Koreans resident in Japan.[370]

Republic of Korea

In the IT domain, many businesses have been interested in inter-Korean opportunities. According to media accounts from 2001, "representatives of IT firms in the South have visited the North in droves this year, as if floodgates have opened."[371] Observers comment that the South

[364] "North Korea Eager to Develop IT Industry," Korea.net, Korean Government Home Page, Ministry of Unification, May 31, 2001

[365] DPRKorea Infobank is a project of the DPRK operated by the Panpacific Economic Development Association of Korean Nationals (Chongnyon). The site carries articles released by the official Korean Central News Agency (KCNA). *Japan Economic Newswire*, May 29, 2001

[366] AP Press Online "NKorea Unveils Software Industry," April 20, 2002; "Eye opener for Kim in Pudong," in *Asia Times* <http://www.atimes.com/Koreas> January 19, 2001; "Danish Reporter Visits North Korean Software Exhibition in Beijing," FBIS translation, April 28, 2002

[367] Kim Jong-nam reportedly has ties to the DPRK State Security Agency (SSA). According to South Korean sources, Kim Jong-nam "assumed the task of collecting overseas information through computer hacking under the jurisdiction of the SSA." *The Chosun Ilbo*, May 15, 2001

[368] In 2001, Kim Jong-nam reportedly visited Shanghai United Investment, a company which controls the local broadband cable industry, and top Internet companies in Shanghai. See "North Korean, Chinese leaders' sons said behind Kim Jong-il's recent visit to Shanghai," *The Chosun Ilbo* (Seoul) as recorded by BBC Monitoring Service, July 4, 2001

[369] Also, Hanaro Telecom, Inc. signed an MOU with China Netcom in September 2002 committing to a joint IT digital media complex in the special Shinuiju economic region in North Korea. See Global News Wire, October 1, 2002

[370] Asia Info Daily China News, February 28, 2002 and FBIS Translation of Copenhagen Berlingske Tidende, April 28, 2002. Pyongyang is saying yes to all comers but, if experience is a guide, relatively few proposals will actually run to completion because of obfuscation and pre-conditions on the part of the DPRK

[371] "North Korea's Fledgling Information Technology Industry," *The Chosun Ilbo*, April 22, 2001

Korean business rush north is competitive and uncoordinated.[372] An illustrative list of proposed projects includes:

- NTrack, a South Korean e-commerce company, has joined with the North's Kwangmyongsung group to build the first ever IT center in Pyongyang. The center is purportedly planned as a $3 million complex where IT components will be produced and North Korean IT experts trained. A 15-story business center is planned for 2002. The DPRK provides the site, water, and electricity, while Ntrack is responsible for all materials, technical manpower, and finance.[373]

- BIT Computer Corporation (Seoul) signed an agreement in June 2001 with the Korea Computer Center to establish satellite Internet links.[374] Under the terms of the contract, BIT would become the sole supplier of satellite Internet equipment to North Korea for five years. BIT President Chol Hyun Jung said the entire venture had the approval of Kim Jong-il.[375] The President of BIT computers, a medical data start-up, lectured at the KCC in February 2001 to 500 local IT experts. KCC reportedly asked for teaching materials.

- Giga Link, Cubic TRC, and Herbmedi.com plan to create a trial broadband network at the Pyongyang Informatics Center. Under terms of the arrangement, they will also sell software developed in the North to customers in Seoul.[376]

- Samsung Group, on November 9, 2000, announced plans to invest $1 billion to build an electronics complex in the DPRK by the year 2008. The complex will likely be in the Western North Korean port city of Sinuiju. After the first phase of construction which will be completed in 2002, Samsung said it would be able to produce $500 million worth of appliances which will mostly be re-imported into the South. Once completed, Samsung will be able to produce $3 billion worth of electronics products annually at the industrial complex.[377]

Government entities both north and south of the 38th parallel are coordinating some activities. For example, an ROK Ministry of Unification has been established in Seoul. The ministry's purpose is to coordinate, facilitate, and regulate steps leading to potential North-South unification. In this context, government-sponsored bodies, such as the Information Technology

[372] A growing number of SK firms of all sizes are expected to build manufacturing lines or industrial complexes in North Korea, according to the Government's policy of inter-Korean economic cooperation. Nominally, Seoul still bans selling to North Korean entities Pentium or even 486 computers, while South Korean firms make them in Pyongyang. "Silicon Valley, Pyongyang" *Business Asia*, April 2, 2001

[373] "Silicon Valley, Pyongyang," *Business Asia*, April 2, 2001

[374] "S Korean Firm To Set Up Satellite Internet Link for N Korea" *Asia Pulse*, (Seoul) June 27, 2001

[375] "North Korea Joins Intelsat," *Satnews Asia*, June 4, 2001; more recent information indicates, however, that the venture failed to get off the ground. Ron Gluckman, "Beyond the Net's Reach," *Newsweek*, October 18, 2004

[376] "Inter-Korean Ties Reboot with IT Issues," *Korean Information Service*, February 13, 2001

[377] Source: <http://www.korea-np.co.jp/pk> and <http://210.145.168.243/pk/071st_issue/98112603.htm> and "S. Korean Business Bodies May Send Delegations to Sinuiju," *Asia Pulse,* September 27, 2002

Forum for Unification (ITFU), have been created. According to a Website, it is a "forum for professionals in the IT domain." The stated purpose of the ITFU is:

- Research and analysis of North-South Korean IT interchange trends
- Formulation of an alternative policy on North-South Korea IT cooperation
- Move to international standards on a uniform basis
- Transfer technology/skills/intelligence between the North and South
- Further support between North and South through IT.[378]

DPRK government officials have visited the ROK on a number of occasions to study its economy.[379] For example, Mr. Park Nam-ki, Chairman of North Korea's State Planning Commission, visited South Korean information technology companies in October 2002. Mr. Pak is reported as saying "I hope Samsung will bridge cooperation between North and South Korea... IT brings North and South Korea close".[380] Samsung is the world's largest manufacturer of computer memory chips. Reportedly, the visiting delegation included Chang Sung Taek, the North Korean leader's brother in law.[381]

Numerous steps have been taken by academics in the South (acting in their personal or official capacities) to forge cooperative relations and programs with counterparts in the North. Pohang University in South Korea, which also performs national-security related research for Seoul's Agency for Defense Development, is one such institution.[382] Professor Chan-mo Park of Pohang, a specialist in virtual reality, has lectured in Pyongyang at the Pyongyang Informatics Center. He recently initialed an agreement with PIC officials to conduct joint research in IT software, including virtual reality programs.[383] He has also described (in writing) contacts and conversations with leading North Korean physicists and other prominent scientists in the IT field.[384] Media reports of South Korean academics teaching computer courses in the North have surfaced in the last year.[385]

Kyungnam University, in South Korea, hosts the Institute for Far Eastern Studies (IFES) in Seoul. According to the IFES website, the institute is staffed by more than 100 scholars and researchers and, as such, is the largest institute of its kind in the country, distributing research materials to about 1000 members. The website indicates the institute will fulfill its function as

[378] Source: ETNews, <http://www.etimesi.com>
[379] Associated Press Worldstream, "Amid rising nuclear tension, North Koreans wrap up study tour of South Korean economy," November 2, 2002
[380] Nautilus Institute, "NAPSNET Daily Report," October 28, 2002 <http://www.nautilus.org/archives/napsnet/dr/0210/OCT28.html>
[381] Associated Press Worldstream "Amid rising nuclear tension, North Koreans wrap up study tour of South Korean economy," November 2, 2002
[382] See Reference 8, Agency for Defense Development, <http://www.mnd.go.kr/mnden>
[383] The Postech Newsletter, Summer 2001, <http://www.postech.ac.kr/e/newsletter>
[384] "Academic Reports on Encounters with DPRK Scientists," FBIS translation of a South Korean journal April 1, 2002, pp. 16-18
[385] For example see "Professors Return from NK Exchange" from NKchosun.com <http://nk.chosun.com/english/news/news.html?ACT=detail&res_id=7312>

an "open library" for those who are interested in North Korean issues by providing information on the Internet.[386]

IFES reportedly offers a 10-week program aimed at fostering economic opportunities on the Korean peninsula. A segment of the course, taught by a Hanzbiz executive, addresses IT industry cooperation between the two Koreas. IFES also offers a 16-week course (on-line) which covers the Internet and North Korea. [387]

In March 2001, a Christian charity in Seoul agreed with the North Korea Education Ministry to operate jointly an Information Technology University in Pyongyang. According to press reports, North Korea has promised to provide land, while the planning, building, and running of the institute—due to open in 2003-- would be arranged by the two sides. Kim Jin-kyong, President of the Yanbian, China University of Science and Technology (which has a large ethnic Korean population) has been appointed director of the Institute.[388]

Russia

Russia, after a hiatus of almost a decade due to a bilateral political rift, resumed high-level contacts with the DPRK beginning with a visit to Pyongyang in 2000 by President Putin. In 2001, Defense Minister Kim Il-Chol paid an official visit to his counterpart in Moscow. According to journalistic accounts, the North Korean delegation discussed military cooperation and also consulted with the Vice-Premier in charge of Russia's "military-industrial complex," Ilya Klebanov.[389]

United States

Kim Chaek University of Technology is now in its second year of cooperative research with the Maxwell School at Syracuse University in New York State.[390] According to the Maxwell School's *Information & Computing technology Newsletter,* the "two universities have agreed to conduct joint research in the area of integrated information technology." The Maxwell School expects to "host visiting researchers" from the DPRK.[391] *The Chronicle of Higher Education* reported in May 2003 that the North Korean scholars are working on "computer and network security," planning to publish papers, and construct "facilities identically configured."[392]

Overall, the DPRK continues to spare no effort to acquire state-of-the art technologies and technical assistance in the form of "know how" from a variety of external sources. Whether the government leadership's ambitions in the information technologies field can be converted into a

[386] See Kyungnam University, "The Graduate School of North Korean Studies," <http://ifes.kyungnam.ac.kr/ifes/sns/eng/>
[387] See Kyungnam University, <http://ifes.kyungnam.ac.kr>
[388] <http://www.Asiaint.com/psr/secure/hal/pdf> September 2001, p.4.
[389] "DPRK Defense Chief Arrives in Moscow for Military Cooperation," April 27, 2001 <http://english1.people.com.cn/english/200104/27/eng20010427_68725.html>
[390] "Research Activities," Information and Computing Technologies, Maxwell School, Syracuse University <http://www.maxwell.syr.edu/ict/research/research_activities.asp>
[391] Ibid Information and Computing Technologies, Maxwell School p. 1
[392] *The Chronicle of Higher Education,* "North Korean Scholars Visit Syracuse U," May 9, 2003

practical national economic strategy remains an open question. As one informed observer notes, "I think they [The DPRK leaders] see technology pay-offs for their military and for the party. And over the longer term, they hope to be able to find a niche of sorts in the global markets, where they might, for example, be writing software.[393]

[393] Professor Kyong Soo Lho, Seoul National University, as quoted in EBIZ Asia, September 1, 2001.

VI. PAKISTAN

WELTON CHANG

We have successfully launched an organization to support with computer security/virus infection issues in Pakistan. The name of the organization is "Pakistan Computer Security Response Team" (PAKCERT). The two recent viruses affecting large number of companies and effectively crippling IT industry of Pakistan made us realize it is time for PAKCERT. We will very much like your organization to be a member and part of this collaborative effort. Looking forward to your response and membership.

Asim Mughal, Pakistan Computer Security Response Team
About Us, <http://pakcert.com.pk/pages/about.htm>

6.1 BACKGROUND

Well-documented hacker activity in Pakistan and likely ties between the hacker community and Pakistani intelligence services suggest that Pakistan possesses a cyber attack capability. However, the evidence is lacking in the open source domain to determine the exact nature of the capability, and it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program. The evidence collected for this report indicates that the main target of this offensive capability is India—Islamabad's rival in the Kashmir dispute. Pakistan's developed IT industry, well-educated computer programmers, and somewhat supportive government that is concerned with security in Kashmir and parity with India could provide an environment that may support a cyber warfare program.

Since 1947, the year Pakistan gained independence from India, tensions between the two countries have alternately risen and abated, recently peaking with the 2001 Kashmiri conflict and the security stalemate stemming from the development of nuclear weapons. The resulting conventional arms conflicts and nuclear weapons build-up have greatly destabilized the region by creating an insoluble security dilemma. The primary focus of conflict has been over Kashmir, the disputed area to the east of Pakistan and to the north of India. Both countries claim the territory. Armed conflict has resulted, with minimal progress towards a resolution of the territorial dispute. Achieving military objectives and nuclear parity with India are the prime national security concerns of a nominally democratically elected government in Islamabad that is highly influenced by the military.

In the Kashmir conflict in South Asia, cyberspace is becoming increasingly contested. Pakistan and India each control Internet sites that spread propaganda in line with their stance in the conflict. There has been an increase in the popularity of sites that feature propaganda for both sides, including chat rooms, polls, interactive message boards, photos, and other types of propagandist literature.[394] Messages such as "Indians, you people are losers… this is a piece of advice to Indians to free their hands from Kashmir and stop dreaming about it",[395] posted after an

[394] Charu Lata Joshi, "World: South Asia Kashmir's cyberwar," BBC News, <http://news.bbc.co.uk/2/hi/south_asia/380179.stm>

[395] FBIS Transcription, AFP, "Indian Hacker Raids Pakistan's Official Website in 'Retaliation'," December 21, 2000

attack on www.zeetv.com (a site owned by Indian media magnate Subhash Chandra), are typical of the political intent of the cyber war going on between Pakistan and India. Although Pakistan denies that it is funding these efforts, Islamabad does provide open diplomatic support for Kashmiri freedom fighters and there is rumored contact between the Pakistani intelligence services and Pakistani hacker groups.[396]

The problem of a potent Pakistani cyber warfare program is two-fold. First, it could pose destabilizing effects in the South Asian region,[397] with attacks on the civilian IT infrastructure and businesses, as well as cyber intrusions into highly-restricted nuclear and and other national security-related operations. The extent of damage caused to Indian websites, for example, has been considerable. In 2002, over 90% of Indian businesses with an online presence detected a security breach within the previous year and of those, 80% of businesses reported financial losses due to those computer security breaches.[398] Simple defacements and other trivial annoyances from cyber war could spill into the realm of truly detrimental losses.

A second potential problem is that of a wider-scale cyber "arms-race" on the subcontinent. The Canadian Security Intelligence Service identifies the hacker war between Indian and Pakistani citizens over Kashmir as an example of a cyber war that has already left the theoretical realm.[399] Pakistan's cyber warfare ability, left uncontained, could develop into a program that rivals in offensive capability the more developed cyber warfare pioneers such as China and Russia.

6.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

As of this writing, no official U.S. government reports have discussed Pakistani cyber attack capability. In 1998, an article published in the Pakistani *Defence Journal* by Syer M. Amir Husain proclaimed a genuine need for a Pakistani cyber warfare capability. The article followed the milw0rm raid on India's nuclear secrets stored at the Bhabha Atomic Research Centre (BARC) and a 1996 attack launched from the U.S. by three expatriate students, which penetrated a Pakistani military computer system. Husain cited these two incidents as revealing the necessity of an indigenous cyber warfare program.[400] The article detailed potential uses of such a program: industrial espionage, prevention of telecommunications disruptions, the potential launching of denial of service attacks, propaganda and defamation, intelligence/data mining, and support for Pakistan's armed forces. The article recommends creation of a team similar to the Computer

[396] Ibid AFP 2000

[397] India may also developing an information warfare capability. See the chapter on *India* in this report.

[398] FBIS Transcription, Anand Krishnamoorthy, "Tech Not Enough to War Off Attacks," *New Delhi Financial Express*, August 27, 2002

[399] Canadian Security Intelligence Service, "Information Operations," *Perspectives*, November 2001, <http://www.csis-scrs.gc.ca/eng/miscdocs/200111_e.html>

[400] In 1998, a small hacker organization named milw0rm accessed five megabytes of classified text regarding India's nuclear program. The obvious inference from the article is that the national security objectives of Pakistan include countering an increased Indian presence in cyberspace, and disruption of Indian critical infrastructures linked to networks that can be remotely accessed. Syed M. Amir Husain, *Defence Journal*, "Pakistan needs an Information Warfare capability," July 1998 <http://www.defencejournal.com/july98/pakneeds1.htm> and <http://www.defencejournal.com/july98/pakneeds2.htm>

Emergency Response Teams (CERT— ex. CERT from Carnegie Mellon) that operate in the U.S. and also details how to construct a cyber warfare program.[401]

The Pakistani government is certainly concerned with national IT security and has legislation in place to arrest, process, and prosecute cyber criminals. In 2003, when Interior Minister Faisal Saleh Hayat was asked if the country's top secret documents stored in computers were safe from hackers, he responded "We have already made foolproof arrangements at our institutions that are of sensitive and strategic interest."[402] Indeed in 2002, a special unit of the Punjabi police force was designated as the "Electronic Crimes Unit" (ECU) with broad powers to fight cyber crime directed against Pakistani targets. Its goals include prevention, detection, recovery, and deterrence of cyber crimes and the authority to prosecute anyone who commits hacking "intentionally, without authorization to access any computer of any institution, department or agency of the government which is exclusively for the use of that outfit, and such conduct which may adversely affect the use/operation of such computer."[403]

Cyber attacks on Pakistani government websites have resulted in efforts to improve network security. In October 2003 the Pakistani government formed a "Cyber Crime Wing" comprised of the representatives from the Ministries of the Interior and Telecommunications. This new center, along with the National Response Centre which formed a few months earlier, is responsible for securing the computer networks of government officials. The new ministry was formed as a response to the efforts of Indian hackers earlier in the year, when they delivered viruses (dubbed "Indian Snacks") in emails to Pakistani officials.[404] The ability of the Pakistani government to effectively secure its own computer systems is a primary concern of the Ministry of Information. The Pakistani government has also formed a National Response Centre for Cyber Crime (NR3C). The stated mission of the NR3C is that it should serve as

"the national focal point for gathering information on threats to critical infrastructures. It is the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The NR3C includes investigators and analysts experienced in computer crimes and infrastructure protection. It is under process of being linked electronically to the rest of the federal and local governments. The NR3C provides law enforcement and intelligence information and reports to relevant federal, state, and local agencies. Before disseminating such information, the NR3C coordinates with the intelligence community to protect national security interests."[405]

[401] Ibid Syed M. Amir Husain 1998
[402] FBIS Transcription, Islamabad PTV World, "Pakistan Government Considers Legislation to Counter Cybercrime," February 25, 2003
[403] FBIS Transcription, Awais Ibrahim, "E-crime unit to fight terrorism," October 10, 2002
[404] Imran Ayan, "Cyber Crime Wing meets today to co-ordinate efforts," *The International News*, Islamabad the Nation, October 2003 <http://www.jang.com.pk/thenews/oct2003-daily/04-10-2003/business/b1.htm>.
[405] National Response Centre for Cyber Crimes, "Services," <http://www.nr3c.gov.pk/html/service.htm>

6.3 FOREIGN MILITARY AND INTELLIGENCE AGENCY RESEARCH[406]

The Pakistani military has not released any official publications in English on cyber warfare as of this writing. There has been theoretical discussion on the possible advantages of pursuing a cyber warfare capability. Major Ozair Ahmed,[407] in a 1998 *Defence Journal* article titled "Concept of Knowledge Warriors and Software Soldiers," writes that military information operations are more than just

"battlefield intelligence or tactical attacks on the other side's radar or telephone network, but [it is] a powerful lever capable of altering high-level decision [sic] by the opponent. In knowledge warfare, each side will try to shape enemy actions by manipulating the flow of intelligence and information."[408]

Major Ahmed argues that Pakistan "requires a different breed of computer specialists who will program, process and operate the military hardware and software behind the scene, these would be the nation's other asset Software Soldiers."[409] Much of the article references a policy memo that the U.S. Joint Chiefs of Staff presented on May 6, 1993, enumerating various uses of electronic command and control capabilities (C2).[410] However, this memo did not address cyber warfare in detail. Therefore, it is difficult to ascertain the weight of the article. Nonetheless, Ahmed does make a point about Pakistani recruitment of hackers that is consistent with the real life instances of recruitment of Pakistani hackers by its intelligence services.

"There is definitely a requirement to have a select group of trained people to be used as software soldiers. These are usually software developers, programmers and mostly machine operators on pre-defined machinery. Such talent is picked up normally from the student community."[411]

Although it may seem that the Pakistani military or intelligence services have considerable powers to wage cyber warfare, their skills may not be as powerful as perceived. In 1996, a group of three Pakistani teenagers operating out of the U.S. hacked into a former Pakistani Air Force chief's personal account and downloaded all of his files. The aforementioned milw0rm hacking incident brings into question just how capable and technologically adept Pakistan's Inter-Services Intelligence Directorate (ISID) is at protecting its own networks and, in turn, its offensive cyber warfare capabilities. In 2002, the official Pakistani government website was taken down by a rudimentary denial of service attack from Indian hackers employing the Yaha Worm—exploiting an easily fixed software vulnerability. In an incident of some embarrassment, officials in the Pakistani science and technology ministry said the information ministry lacked sufficient technical expertise to prevent attacks from determined hackers. A suggestion for better

[406] Pakistani intelligence services are regarded as one of the most competent intelligence services in the world. Federation of American Scientists, John Pike, Steven Aftergood, "Directorate for Inter-Services Intelligence [ISID]," July 25, 2002 <http://www.fas.org/irp/world/pakistan/isi/>

[407] According to the attached biography, "Maj Ozair Ahmed was commissioned in Army Service Corps in 1982. He is a graduate of Command and Staff College and has served as Chief Instructor Military Police School and participated in the Gulf War. He served as Deputy Assistant Adjutant and Quartermaster General, 24 Infantry Brigade." <http://www.defencejournal.com/july98/contentsjuly98.htm>

[408] Major Ozair Ahmed, "Concept of Knowledge Warriors and Software Soldiers," *Defence Journal*, July, 1998 <http://www.defencejournal.com/july98/contentsjuly98.htm>

[409] Ibid Ahmed 1998

[410] Office of the U.S. Joint Chiefs of Staff, Memorandum of Policy No. 3016, May 6, 1993

[411] Ibid Ahmed 1998

cyber security, ostensibly made because Pakistani website hosting services exhibited inadequate security measures, recommended finding a host for the website "through a third country where the rates are cheaper and the hosts have the responsibility for protecting the website."[412]

In response to the threat posed by Pakistani cyber warfare units and freelance Pakistani hackers, India has implemented data security training and IT support for its army officers. The threat that "India could be severely battered if a concerted cyber-offensive is launched by an enemy country" (the enemy country being Pakistan) was sufficient to prompt the Indian Army to outline its IT security goals in the "IT Roadmap-2008."[413] An Indian army institute in Hyderabad was established in 2001 to teach officers the fundamentals of information warfare.[414] India's response has grown more focused over the years, an indication of what the government likely perceives as Pakistan's growing cyber warfare capabilities. The Indian Defense Information Warfare Agency (DIWA) was formed in 2003 and will reportedly handle all "information warfare, including psychological operations, cyber war, electro-magnetic spectrum and soundwaves" activities for the Indian army.[415] New Delhi's response suggests that Pakistan does indeed pose a threat against computer networks.

Pakistan's Interior Minister Faisal Saleh Hayat stated that the U.S. Federal Bureau of Investigation is training Pakistani Federal Investigation Agency (FIA) officials in various methods to combat cyber crime.[416] According to the report, Minister Hayat said a "cyber threat was a serious issue since it originated from unknown places and its impact could not be assessed in the initial stage" and that "in the recent past nearly all the government sites had been under DOS [sic] attack."[417]

6.3.1 Pakistani Hackers

Although many of Pakistan's hackers operate independently and within self-contained units, there may nevertheless be ties between elements of this hacker community and Pakistani intelligence services. Within the population of Pakistan, there is a small and dedicated group of technically adept individuals that could be recruited into the intelligence services. Without a doubt, the hackers have political intentions behind their attacks. Some observers believe that several Pakistani hackers have been contacted by Pakistani intelligence services and some of these hackers now operate in service under the ISID's direction.[418]

India has repeatedly accused Pakistan of recruiting hackers for use by intelligence services. "There is a new breed emerging, in the age-group of 14-35 years, which feels it can create equal

[412] FBIS Transcription, Arshad Sharif, "Indian hackers block government's website," *Karachi Dawn*, June 29, 2002
[413] FBIS Transcription, Saikat Datta, "Info warfare agency for armed forces," *The Indian Express*, February 27, 2003; for a discussion of India's plans see Chapter III on India
[414] Chetan Krishnaswamy, "Information Warfare: Is India Ready for it?," *The Times of India*, May 12, 2001
[415] FBIS Transcription, Saikat Datta, "Info warfare agency for armed forces," *The Indian Express*, February 27, 2003
[416] *Daily Times*, "FBI training FIA officers on cyber crime," November 7, 2003 <http://www.dailytimes.com.pk/default.asp?page=story_11-7-2003_pg7_26>.
[417] Ibid *Daily Times* 2003
[418] FBIS Transcription, Kaajal Wallia, "Over 500 Indian Sites Hacked by Pakistanis, Others in Year 2000," *The Times of India*, December 19, 2000

havoc with a mouse and an AK-47," says [Indian] Deputy Commissioner of Police Himanshu Roy, head of Mumbai Police's cyber crimes unit.[419]

It should be noted that our research did not locate any sources that definitively confirm Indian claims that Pakistani intelligence-supported hackers have carried out cyber attacks against India. Hacker activity in Pakistan has been well documented.[420] A number of website defacements that these hackers performed have gained international notoriety. Computer hackers in Pakistan regularly attack computer systems and networks in India and have continually defaced Indian government websites. Pakistani groups such as Death to India, Kill India, and G-Force Pakistan look to spread information on how to hack into Indian websites and networks. Other named Pakistani hacker groups include "Nightman" and a group run by "Doctor Nuker." G-Force Pakistan has been fingered in attacking the Indian Science Congress site, the National Research Centre, and the Indian National Information Technology Promotion, while Doctor Nuker has targeted the Indian Parliament and Nightman has attacked the Lal Bahadur Shastri National Academy of Administration.[421] Indian intelligence officials say that these groups are run by adolescent Pakistanis and are not part of a military-backed cyber warfare scheme. However, they claim that these adolescents have begun to be recruited by Pakistani intelligence officials to wage cyber war against Indian targets.[422]

India has continually asserted that the ISID has been in the past, and is currently in the business of recruiting skilled hackers to wage cyber warfare.[423] According to Indian intelligence officials, one Pakistani hacker, the so-called Doctor Nuker, was identified by Pakistani intelligence as having superior hacking skills and directed to attack critical Indian government servers.[424] Ravi Prasad maintains that Indian intelligence should not dismiss the possibility of being attacked by cyber foes, especially Islamic militant groups operating out of Pakistan. India's security establishment has also ignored cyber warfare capabilities possessed by Islamic militant organizations. The Rand Corporation recently warned: "Osama bin Laden's Egyptian followers can immediately cripple the information infrastructures of Russia and India." Clark Staten, Executive Director, Emergency Response and Research Institute, Chicago, warned that Pakistani terrorist organizations had developed offensive capabilities in cyber warfare.[425]

Pakistani officials may not be well versed in IT protection, but Pakistanit hacking exploits have certainly had effects on U.S. webpages. Especially evident has been the Islamic fundamentalist rhetoric voiced since 9/11 which has frequently appeared in the content of website defacements.

---

[419] Ibid Wallia 2000

[420] For some recent media reports regarding the hacker war between India and Pakistan see:
Overseas Security Advisory Council, "BMC website caught in India-Pak hacker war," August 20, 2003 <http://www.ds-osac.org/view.cfm?KEY=7E4555424554&type=2B170C1E0A3A0F162820>;
Ndivhuwo Khangale, IOL, "SA site crash at the hands of foreign hackers," June 1, 2004 <http://www.iol.co.za/index.php?click_id=31&art_id=vn20040601030856365C382553&set_id=1>;
Azhar, Mahmood, "Hackers break into ATM's security system," July 22, 2003, <http://www.jang.com.pk/thenews/jul2003-daily/22-07-2003/business/b1.htm>

[421] FBIS Transcription, Kaajal Walia, "Over 500 Indian Sites Hacked by Pakistanis, Others in Year 2000," *The Times of India*, January 6, 2001

[422] Ravi Prasad, "Hack the Hackers," *Hindustan Times* December 19, 2000

[423] *Jane's Intelligence Review*, "Hackers take Kashmir dispute to cyberspace," October 2002

[424] Ibid *Jane's Intelligence Review* 2002

[425] Ravi Prasad, "Hack the Hackers," *Hindustan Times* December 19, 2000

The notorious GForce Pakistan hackers attacked several Defense Test and Evaluation Processional Institute website homepages, defacing them with pictures and text messages with terrorist and Islamic themes. The vandalized sites included <http://www.dtepi.mil>, <http://enduringfreedom.dtepi.mil>, <http://nasa.dtepi.mil>, and others; all sites that were supposedly being served by KCnet, a U.S. ISP based in Kansas City. The GForce message also included threats to deface 1,500 more U.S., British, and Indian websites.[426]

In 2000, more than 40 Indian sites had been attacked by Pakistani hackers. That number has increased in the past few years, due to increased availability of open source hacking knowledge, more exploits for software, and presumably because more attention has been paid to the development of cyber warfare capability.[427] According to Attrition.org, a top computer security organization, 72 top-level domain names (TLDs) in India were hacked in 2000, accounting for a 1700% escalation of cyber warfare activities between Pakistan and India compared to a year before. In January 2003, an 18-year-old Indian "ethical hacker" and noted cyber security expert Ankit Fadia stated that 40-50 Indian websites, including sensitive government and corporate sites, are hacked by Pakistani cyber criminals every month. Fadia has served as a cyber security consultant for numerous intelligence agencies, defense departments, and government and private organizations. He has also aided Indian law enforcement in tracking Pakistani "hacktivists," often anti-Indian. Fadia underscored the need for cyber security awareness and training in India, mainly as a response to the Pakistani development of cyber warfare techniques and strategies.[428]

According to the Internet security firm mi2g, individual hacker groups are joining together to launch cyber attacks against the U.S., Israel, and India. The ongoing conflict in the Kashmir region in the Indian subcontinent has been reflected in the tension online. The Unix Security Guards and the World's Fantabulous Hackers were responsible for 111 cyber attacks on sites located in India. D.K. Matai, mi2g's chairman and CEO said: "The most important lesson learnt from these events is the coming together of pro-Islamic groups to simultaneously participate in joint digital attacks on U.S./UK, Israeli and Indian targets. Historically, the U.S. has been allied with Pakistan. It seems that recent political and cyberspace events are both pointing towards a closer alignment of interests in the near future between the U.S., India and Israel."[429]

6.4 INFORMATION TECHNOLOGY INVESTMENT

The IT industry of Pakistan has enjoyed the support of the government since the late 1990s. Pakistani IT investment seeks to develop current state-of-the-art infrastructure. The "legacy systems" of older communication networks are currently being upgraded. Information technology training is broadly available in colleges and universities. Islamabad estimates that there are twenty-one million computer literate Pakistanis.[430] E-government initiatives are being

[426] Brian McWilliams, "Pakistani Group Strikes U.S. Military Web Site," *Newsweek: Newsbytes*, October 21, 2001
[427] K Yatish Rajawat, "Pakistan Declares Cyberwar Against India," *The Economic Times of India*, December 14, 2000
[428] *The Times of India*, "40-50 Indian sites hacked by Pak cyber criminals monthly," <http://timesofindia.indiatimes.com/cms.dll/html/comp/articleshow?artid=35386388>
[429] BBC World News, "Pro-Islamic hackers join forces," June 19, 2002 <http://news.bbc.co.uk/2/hi/sci/tech/2052320.stm>
[430] IT division of the Pakistani Ministry of Science and Technology, "Information Technology and Telecommunications: a report card," August 2002

developed in addition to changes in the legal and regulatory regimes. These four factors create an environment that may support a cyber attack capability.

The Pakistani government has initiated significant efforts to improve its economic conditions by investing in information technologies. Pakistan launched its first communications satellite, PAKSAT-1, in 2003.[431] According to an August 2002 report card on IT investment progress by the IT division of the Pakistani Ministry of Science and Technology, significant progress has been registered. This included the expansion of the availability of Internet bandwidth to a larger portion of the population and the development of a "world class infrastructure" within 24 months of initial deployment of IT policy. The IT division plans to launch a public key infrastructure program to support electronic commerce. In addition, a payment gateway and electronic clearinghouse initiatives are being developed.[432]

A lower-level threat that should not be minimized is the possibility that Pakistani software companies have embedded code to make the software vulnerable to attack. As countries such as the United States, Britain, and India outsource their programming of software to countries such as Pakistan, Philippines and Russia, the risk of rogue programmers using their access to commit acts of cyber terrorism rises. The possibility of abuse by hackers, organized crime agents, and cyber terrorists in countries not necessarily allied with the United States is great, and grows as more and more programming is outsourced to these countries for economic reasons.[433]

6.5 CONCLUSION

Pakistan's efforts appear to be focused on countering India's cyber warfare capability (the vice-versa is also true). However, the U.S. is still at risk of cyber attack from hackers that reside there. Pakistan has served as our ally against al-Qaeda in the current war on terrorism, and has at least served nominally as our ally in the past. However, the unstable situation on the sub-continent and the anti-U.S. sentiments harbored by some Pakistani citizens, combined with the mixed loyalties of elements within the ISID, increase the possibility that a cyber attack against the U.S. will come from Pakistan. Following 9/11, the hacker group GForce Pakistan attacked several U.S. .mil websites and defaced them.

Pakistan poses a threat to cyberspace with its growing army of young talented hackers. Regardless of state backing, these hackers have shown a penchant to involve themselves in real-world situations such as the Kashmir conflict and countering anti-Islamic sentiments in the West following 9/11. With the possible backing of the state, taking into account the reported ISID contact with Pakistani hackers, it would seem Pakistan may be investigating the possibility of building a more potent cyber warfare program capable of disrupting Indian computer networks. The immediate threat is to India's burgeoning IT industry and to the supervisory control or data

---

<http://www.pakboi.gov.pk/Presentations/IT/Report%20%20IT%20and%20Telecom%20%20Aug%202002_files/frame.htm>

[431] South-Asian Defence News, January 2003, <http://www.pakistanidefence.com/news/MonthlyNewsArchive/2003/Jan2003.htm>

[432] Op. cit. IT Division 2002

[433] John Schwartz, "Experts See Vulnerability As Outsiders Code Software," <http://query.nytimes.com/gst/abstract.html?res=FB0B15FA3C5A0C758CDDA80894DB404482>

acquisition computer programs that control sensitive, national security-related industries, such as nuclear installations.[434]

[434] Over the past decade, an evolution in data communications and process control has introduced potential systemic vulnerabilities. The data connections from Distributed Control Systems and Programmable Logic Controllers systems to the plant network are vital to production, yet can be an invitation to compromise if "problems on the business network can be passed on to the process network" through a utility's Ethernet and TCP/IP networking. Eric Byres, "Protect that Network: Designing Secure Networks for Industrial Control," <http://extranet.arcweb.com/cybersecurity//Shared%20Documents/IEEE%2099%20-%20Process%20LAN%20Protection.pdf>

VII. RUSSIA

WELTON CHANG

"Information warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation's decision-making system, on the nation's populous [sic] *and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets."*

Russian military officer in conversation with Lieutenant Colonel (ret.) Timothy L. Thomas
"Russian Views on Information-based Warfare," *Airpower Journal*, 1996

The circumstance that, as specialists believe, over half of the world population will be living in cities in the first third of the 21st century and can especially suffer in case of wars began to play a role of no small importance here. Therefore it is believed that to win victory with minimum victims among the civilian population and minimum property damage, it will be necessary to employ very precise lethal and nonlethal kinds of weapons in order to exert sufficient pressure on the opposing country's leadership directly or through the population masses of cities. Electronic weapons in particular can prove to be specifically such a means.

Major M. Boytsov
"Russia Information War," *In Foreign Navies*, February 6, 1996, FBIS-UMA-96-026-S

7.1 BACKGROUND

Russia's military services, working with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine.[435] "Information weaponry," weapons based on programming code, receives paramount attention in official cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have published discussions and debates concerning their official policy. It is likely that Moscow will continue to scout U.S. military and private sector networks and websites to obtain information about configuration of communications nodes. However, analysis of open source materials is inadequate to predict whether a Russian cyber warfare program would target U.S. networks, especially taking into account closer political and economic ties between the two nations in recent years.

The collapse of the Soviet Union in 1991 led to economic turmoil and a significant "brain drain" affecting various Russian industries and academic circles. Despite the wide-scale turmoil, the Federal Security Service (FSB), the Federal Agency for Government Communications and Information (FAPSI), and the high technology sector in Russia should not be taken lightly as regards potential to underwrite and develop a cyber warfare program.

Russian intelligence services have a history of employing hackers against the United States. In 1985 the KGB hired Markus Hess, an East German hacker, to attack U.S. defense agencies in the infamous case of the "Cuckoo's Egg."[436] Both FAPSI and the FSB, KGB successor organs, are believed to have potent information-gathering programs, which has led to increased suspicions over possible attempts at espionage.

[435] In official doctrine, the Russian government chooses to refer to cyber warfare and information warfare as information operations

[436] Ruth Alvey, "Russian hackers for hire: the rise of the e-mercenary," *Jane's Intelligence Review*, July 1, 2001 p. 2

The U.S. Department of Defense (DoD) remains wary of the threat posed by Russian hackers. These hackers reportedly took two million DoD computers offline in what the Pentagon suspected to have been a Russian electronic espionage campaign (then dubbed 'Operation Moonlight Maze').[437] However, there have also been cases of analysts over-estimating Russian cyber-capabilities. In February of 1998, break-ins into U.S. Department of Defense networks and the subsequent investigation (dubbed Solar Sunrise) were mistakenly attributed to Russian secret services. In actuality, the attacks were perpetrated by two Northern California teenagers under the direction of a handler in Israel.[438] The fact that FBI agents and then deputy Secretary of Defense John Hamre suspected that Russian secret services were behind the attacks, however mistaken, was understandable based on Moscow's past behavior and other evidence.

Currently, the three most significant struggles faced by the new Russian government are development of a cohesive democratic government, restructuring of a collapsed economy into a viable free-market alternative, and quelling of an open rebellion by Chechen rebels.[439] Renewed government attention to rebuilding aging infrastructure has led to an increase in economic confidence and a subsequent upswing in the Russian economy. In terms of this cyber warfare country assessment, the Chechen conflict is the most important because it has forced the Russian intelligence services to wage cyber war on the technologically adept Chechens. Oleg Gordievsky, the former London KGB section head, claimed at the 1998 Global Cybercrime Conference that "there are organized groups of hackers tied to the FSB and pro-Chechen sites have been hacked into by such groups… one man I know, who was caught committing a cybercrime, was given the choice of either prison or cooperation with the FSB and he went along."[440] At the conference in 1998, Gordievsky said that not only did his agents perform information operations; they also participated in industrial espionage. Gordievsky claimed that 12 of his 29 agents were involved in conducting intelligence on the attitudes of banks towards possible investment in Russian-owned industries. Sergei Pokrovsky, the editor of the Russian hacker magazine Khaker confirmed that the FSB employs hackers for both foreign and domestic espionage.

There are several indicators suggesting an active Russian cyber warfare capability at present. For example, active Russian foreign intelligence services possessing a high-level of technical expertise and the actions of government-sponsored hackers against the Chechens are suggestive; this evidence, in addition to the development of relevant doctrinal concepts, directly confirms research on cyber warfare.

Here, as was the case in the China country study, one must be careful to discern what constitutes disinformation and what parts of cyber warfare doctrine have actually been implemented. Extrapolating from the meager open source data is intriguing but risky.

The Russian press is quick to point out that American fears of an offensive cyber attack from Russia are largely unfounded. Such fears should not be so easily allayed. As evidenced by the Chechen conflict, Russian secret services under sponsorship of the government will not hesitate

[437] FBIS Translation Taras Lariokhin, "The Pentagon Fears Russian Hackers," *Moscow Izvestiya*, September 7, 1999
[438] SANS Institute, "What is Solar Sunrise?," <http://www.sans.org/resources/idfaq/solar_sunrise.php>
[439] CIA, *World Factbook* Russia, 2003 <http://www.cia.gov/cia/publications/factbook/>
[440] Ruth Alvey, "Russian hackers for hire: the rise of the e-mercenary," *Jane's Intelligence Review*, July 1, 2001 p.2

to use cyber warfare to further their agenda and to protect what they deem to be matters of national security.

7.2 U.S. GOVERNMENT REPORTS AND FOREIGN OFFICIAL STATEMENTS

Operating under government control, the Academy of Sciences in Moscow has been linked to unsanctioned intrusions into U.S. private sector IT networks. Although the military and intelligence services have faced severe budget cutbacks in the past few years and Russia itself is in the midst of an arduous economic restructuring, its information operations and cyber warfare research capabilities are still significant and potentially pose a considerable threat to worldwide computer security.

Existing open source literature and published statements by intelligence experts point to Russia as a nation-state whose abilities in cyber warfare are, next to the United States, the most developed among technically capable countries.[441] According to official U.S. analyses, Russia is an example of a country heavily involved with developing its own cyber warfare capability. Of the 15 criteria enumerated in a Defense Science Board report on technical prowess, Russia was listed as having a significant capability in seven categories and a good capability in four. This performance continues, even in the face of widespread economic difficulties.[442] In a summary of cyber warfare capabilities by *Jane's Intelligence Review*, Russia was reported to have a majority of the listed strengths in the areas of electronic attack and electronic protection.[443]

Testimony from both Lawrence Gershwin, top intelligence and science officer at the National Intelligence Council[444] and George Tenet, then Director of Central Intelligence (DCI),[445] coupled with official CIA analysis[446] on cyber warfare, have raised the prospect of an extensive Russian cyber warfare program. Richard Clarke, former White House senior advisor on cyber security, has also testified to the existence of Russian cyber warfare capabilities.[447] The NSA has also fingered Moscow as having an "aggressive" cyber warfare program.[448] U.S. intelligence officials believe that Moscow has been sponsoring cyber warfare research.

---

[441] A summary of Lieutenant Colonel (ret.) Timothy Thomas's analysis of Russian views on information operations can be found in Figure 2. For more doctrinal sources see Chapter 6 and Chapter 7 of "Noncontact Wars" by retired Major General Vladimir Ivanovich Slipchenko, January 1, 2000 pp. 80-120

[442] Defense Science Board Task Force, "Report of the Defense Science Board Task Force on Information Warfare-Defense," 1996 <http://www.acq.osd.mil/dsb/reports.htm>

[443] *Jane's Intelligence Review*, "Asia Focus: Chart 4- Summary of IW Capabilities," December 2000

[444] *Express India*, "Russia, China working on cyberwarfare: US," <http://www.expressindia.com/news/june22/world1.shtml> Lawrence Gershwin's complete testimony can be found here: Federation of American Scientists, <http://www.fas.org/irp/congress/2001_hr/062101_gershwin.html>

[445] George Tenet, "Testimony by Director of Central Intelligence George J. Tenet Before the Senate Committee on Government Affairs," <http://www.cia.gov/cia/public_affairs/speeches/archives/1998/dci_testimony_062498.html>

[446] CIA, "Buck Rogers or Rock Throwers? Conference Report," <http://www.cia.gov/nic/pubs/conference_reports/buck_rogers.htm>

[447] Richard Clarke, "Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security," <http://www.techlawjournal.com/security/20020213.asp>

[448] James Adams, NSA Advisory Board, "30 nations now have aggressive cyberwar programs," *Foreign Affairs*, May/June 2001

U.S. government analysts also believe that the Russian military is the spearhead of cyber warfare program development and that Russian intelligence services are involved with cyber warfare research and usage. In 2000, CIA analyst John Serabian cited unnamed Russian sources as revealing a burgeoning cyber warfare research program operating within the Russian Federation. Following the release of this CIA report, several newspapers in Russia printed vehement denouncements of American claims that these cyber warfare programs would be used for offensive purposes. Following attacks on U.S. e-commerce sites, the CIA and Pentagon both reported to the press that they were aware of the ongoing development of cyber warfare programs in Russia, insinuating that Russian hackers had something to do with the attacks in question. In response, Russian journalists, citing military sources, were quick to point out that there was absolutely no evidence to link Russian cyber warfare with these attacks and that U.S. intelligence services, by having an "external computer threat" to direct actions at, would be able to make their investigative positions extremely "advantageous."[449]

In Moscow, information security and defensive cyber warfare development matters have been discussed as early as 1996 in the Duma Subcommittee for Information Security, when there was some suspicion that recently purchased telecommunications devices from the United States were implanted with devices that could cause irreparable damage to Russian telecommunications systems when triggered by remote device. In response, information security in Russia became an urgent matter, with efforts to secure cyber space a top priority.[450] In 1999, an administration in charge of computer and information security was set up in the FSB. Additional new faculty with expertise in the areas of computer and information security were hired for the FSB academy.[451]

Russia's official cyber warfare doctrine appears to be a product of fear of U.S. superiority in the cyber field.[452] Former Russian Federation Secretary of the Security Council (Minister of Defense), Sergey Ivanov said that the Russian government was in support of the development of "international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."[453] The possession of an advanced IT capability by the U.S. military and intelligence services apparently raises Moscow's fear of losing an all-out cyber war between the two nations. Ivanov said that "in our view, there is a danger of the outbreak of 'cyberwars' using worldwide computer networks and other lines of communication, which demands that preventive steps be taken." He further stated that these technological breakthroughs could lead to an "arms race," one that Russia could compete in but could not possibly win.[454] In 2001, General Vladislav Sherstyuk, the RF Security Council deputy secretary, said that the appearance of a new information area of confrontation is

[449] FBIS Translation, Alena Miklashevskaya "CIA Scared of Computers—Chinese and Russia," *Moscow Kommersant*, February 25, 2000

[450] FBIS Translation Akesey Romashkin, Oleg Kotov, "'We Are Being Dragged Into a New Form of Arms Race,' Russian Power Departments Believe," *Moscow Kommersant,* January 30, 1999

[451] Ibid Kotov and Romashkin 1999

[452] The Russians, like the Chinese, have translated and/or co-opted American views on IO to be their own. An example of this is "In Foreign Navies" by Major M. Botysov, published in the Russian Military Naval Forces publication on October 19, 1995

[453] FBIS Translation Interview with Security Council Secretary Sergey Ivanov, "Security Council's Ivanov Fields Questions on New Military Doctrine, Information Warfare, Echelon System," *Moscow Nezavisimoye Voyenneoye Obozreniye*, June 2000

[454] Ibid Ivanov 2000

capable of provoking the beginning of the next spiral of arms race. The development of strike-capable military computer viruses, in contrast to strategic nuclear missiles, requires no special expertise beyond what is available in the general civilian realm.[455]

As early as the mid-70's (some experts place these events around the mid-80's), the Russian military had begun researching the next revolution in military affairs (RMA). According to Mary Fitzgerald of the Hudson Institute, Marshal Ogarkov, then Chief of the Russian General Staff, first used the phrase "revolution in military affairs" in publication, referring to the usage of electronic command and control in military units.[456] Since then, Russian military theorists have evaluated the "impact of computer viruses, [and] other types of information weapons, logic bombs, special microbes, and micro-chipping."[457]

The Russian technology sector and academic community, in conjunction with the Russian military, have developed cyber warfare doctrine beyond what any other country, save the U.S., possesses. The Russians recognize that information warfare requires the simultaneous conduct of offensive and defensive measures in order for cyber warfare to be successful.[458] According to a prominent Russian expert, the fact that cyber warfare provides a new means to affect the military and civilian population of a target changes its principles, tactics and permissible conditions from that of conventional warfare.[459]

Software weapons receive great attention in the Russian cyber warfare doctrine. Development and use of such weapons requires long-term planning, technical expertise, and intelligence on targets, all of which Russian secret services such as FAPSI and the FSB possess. The list of weapons includes the viruses (the best of which break down security and self-propagate), reprogramming memory chips (causing loss of long-term stored data), Trojan horses, rewriting software programs through remote-access tampering, and destruction of critical infrastructure from remote areas.[460] Exploration into how these weapons will be used is detailed in Figure 1 below.

7.3 FOREIGN MILITARY AND INTELLIGENCE AGENCY RESEARCH

During the investigatory phase of Operation Moonlight Maze, Michael Vatis, then head of the FBI's National Infrastructure Protection Center (NIPC), attributed hacking and data theft in Pentagon networks to Russia. Vatis said that the hackers had stolen "unclassified but still-sensitive information about essentially defense/technical research matters," and that the

[455] FBIS Translation Sergey Ishchenko, "Before the verdict is in: Computers on the attack: Cyberwars already are being depicted on Staff Maps," *Moscow Trud,* June 28, 2001

[456] This statement is corroborated by Woondo Choi of Yonsei University. "Woondo Chio, RMA and Strategic Intelligence: The Case of China and Japan," <http://www.iews.or.kr/lib/wdchoi/strint.pdf>

[457] Mary C. Fitzgerald, Hudson Institute, personal correspondence to George Smith, editor of *The Crypt* <http://www.soci.niu.edu/~crypt/other/fitz.htm> the report being referred to is here: Fitzgerald, Mary C. "Russia's New Military Doctrine," *RUSI Journal,* October 1992

[458] FBIS Translation Professor Aleksandr V. Fedorov, "Information Weapons as a New Means of Warfare," Russian Academy of Natural Sciences, *Moscow PIR Center,* August 1, 2001 pp. 69-109

[459] Ibid Fedorov 2001

[460] Ibid Fedorov 2001

intrusions had occurred in "Defense Department, other federal government agencies, and private-sector computer networks."[461]

During Moonlight Maze,[462] U.S. Senator Robert Bennett argued that the threat from this area was very real and even supposed that the three-year long attack on government networks also stretched into hacking of networks in the private sector. Senator Bennett believes that the unsanctioned intrusion was perpetrated by people physically located at the Russian Academy of Sciences.[463] The FBI attempted to determine whether the Academy of Sciences was responsible for the attacks; trace-backs and initial collection of forensic evidence revealed compelling details that could be inferred as actions attributable to an active Russian information operations program. The 1998 intrusions were traced back to seven dial-up connections in Russia. With respect to two attacks in July 1998, intrusions were detected from Lab 1313, a then unknown group that was using an Internet connection from the Russian Academy of Sciences. These two attacks attempted to steal information from Meganet Corp., a private company which develops cryptographic software. This was a significant detail because most cryptographic software is not available for export. During the investigation of Moonlight Maze, analysts found that there were many instances in which technical defense research data was downloaded and transferred back to Russia.[464]

In a possibly related incident that occurred in February of 1999, a Hewlett Packard printer at the Navy's Space and Naval Warfare Systems Command Center (Spawar) in San Diego was programmed to send copies of printed documents to a remote location in Russia. Spawar provides electronic security for the Marine Corps and other government federal agencies. In conjunction with its responsibilities for the cyber security of various government agencies, Spawar also provides the Navy with intelligence codes. Oleg Kalugin, a former head of Soviet counterintelligence now resident in Maryland, has reported that such facilities were prime targets for Russian intelligence.[465] Kalugin notes that FAPSI, which specializes in electronic methods of espionage, would use the Internet to spy on assets in the United States. The technical data that is reported to have been stolen is in line with what FAPSI would be looking for. "That's what they're good at," Kalugin said. "Russia is quite good at producing technology but can't afford to finance the research."[466]

Moscow's information security defenses to counteract cyber warfare have also been a focus of the vast military-industrial complex that exists in Russia. According to official but unconfirmed information, the government of the Russian Federation sent out a directive in March of 2000, ordering Russian enterprises to provide new information security measures as well as preparatory

[461] Aerotech News and Review, "Russia spies no link between hackers, Kremlin," October 15, 1999 <http://www.aerotechnews.com/starc/1999/101599/Hackers.html>

[462] Bob Drogin, "US Scurries to Erect Cyber-Defenses," *London Times,* October 31, 1999 <http://www.deaddrop.org/security/Papers/ZenithStar.html>; see conclusion chapter of this report for more a more detailed discussion of Moonlight Maze

[463] FBIS Translation Sergey Ishchenko, "Before the verdict is in: Computers on the attack: Cyberwars already are being depicted on Staff Maps," *Moscow Trud,* June 28, 2001

[464] Bob Drogin, , "US Scurries to Erect Cyber-Defenses," *London Times,* October 31, 1999 <http://www.deaddrop.org/security/Papers/ZenithStar.html>

[465] Matthew Campbell, "Russian Hackers Steal US Weapons," *London Sunday Times*, July 25, 1999

[466] Ibid Campbell 1999

operational security measures, usage of American operating systems (UNIX and Microsoft Windows) by the Russian military.[467] However, there are Russian technology experts who decry this government intervention into IT security saying that it will stifle the ability of the technology sector to develop adequate tools to counteract cyber attacks. Maksim Otstanov, head of the Laboratory of Civilian and Financial Cryptology of the Institute of Commercial Engineering, said that "government intervention in present-day Russia, unfortunately, most often leads to the fact that operators of telecommunications services are 'weighted down' with an unthinkable number of licensing conditions, which leads to their consolidation and erosion of the smaller segments of the market."[468]

Secret service officials in Moscow are also growing increasingly concerned about the low level of funding that FAPSI's 'Electronic Russia' (Russia's national IT security program) is receiving and going to receive in the future. An article released in late 2002 included FAPSI opinions on the current state and the future of Russian national IT security:

> The program Electronic Russia allocated about 2.5 percent of the total funding of the program for measures related to developing information and data protection systems in 2002; and about 0.66 percent in 2003. In the opinion of FAPSI [Federal Agency for Government Communications and Information] representatives, this money is not enough either to analyze the degree of protection of the program, or to develop means of information protection. The Agency believes that the funding of this work should be 20 percent, as in similar programs in foreign countries.[469]

7.3.1 Russian involvement in the Chechen cyber war[470]

An analysis of the information war between the Chechens and the Russian military during the mid-1990s to the year 2000 shows that the Russian military and intelligence services possess cyber warfare capabilities. In the first conflict (1994-1996), the Chechens originally had the upper hand in the public relations war because the Russian government denied the press access to many of its own military actions, allowing the Chechens to spin events through their own media outlets. The Chechens, on the other hand, welcomed the presence of the press as a way of getting out their message and favorably shading their coverage. By the start of the second conflict (1997-2001) however, the Russian government saw the need to control the information coming out of Chechnya. Moscow decided to control both the amount and type of information being released. Both groups in the conflict used news websites to portray their accounts of

[467] FBIS Translation Annaa Mayorova, "The Pentagon in Cyberspace," *Moscow Izvestiya*, November 28, 2000

[468] FBIS Translation Ivan Shvarts "Computer Experts on 'Information Warfare'," *Moscow Kommersant*, January 30, 1999

[469] FBIS translation, Cnews.ru, "Electronic Russia: There Is No Money for Protection," *Cnews.ru* December 23, 2002

[470] Russian hackers and cyber criminals linked to the Russian mafia have had their profiles raised by recent exploits catalogued by the open media. See: Ludmila Goroshko, "Russian Computer Crime Statistics," July 30, 2004, <http://www.crime-research.org/news/30.07.2004/530>; Oliver Bulloughs, Reuters, "Police Say Russian Hackers Are Increasing Threat," July 28, 2004 <http://www.reuters.com/newsArticle.jhtml?storyID=5800359>; Deborah Radcliffe, SecurityFocus, "Companies adapt to a zero day world," July 13,2004, <http://www.securityfocus.com/news/9100>; *Techweb News*, "Malicious Worms Still Probing Microsoft Vulnerability," May 27, 2004 <http://www.informationweek.com/story/showArticle.jhtml?articleID=21400173>; John Blau, *IDG News Service*, "Viruses nip Russia after Cold War," May 25, 2004, <http://www.infoworld.com/article/04/05/25/HNrussianviruses_1.html>

events. Along with Chechen-controlled websites such as kavkaz.org, there were also sites that were run by allies outside of Russia, such as qoqaz.net.my based in Malaysia. This network of sites allowed allied third parties to access information such as pictures and statistics and disseminate the information on the web.

What did each side do with an electronic broadcast capability? Moscow used officially sanctioned state-controlled radio and television broadcasts to show its side of events. The Russians also used websites to spread their message, including infocentre.ru that prescribed how reporters should be reporting news about the conflict. The Russians also published a book version of events and their history of the conflict. On the other side, the Chechens had a different response to cyber warfare. On their site, www.qoqaz.net, it was possible to download videos of attacks on Russians, view photos of Chechens in action and of Russian prisoners of war, find news items, read profiles of Chechen commanders, and read interviews with various Chechen leaders and fighters. In case this site was down, alternate sites were listed: www.qoqaz.net.my, www.qoqaz.com, and www.qoqaz.de. The evidence from these two conflicts shows that as cyber warfare and the IT communications revolution develop, it becomes increasingly difficult to control the kinds of information that becomes publicly available, which, counter intuitively, warrants the development of more cyber warfare capability.[471]

In 2002, Chechen rebels claimed that two of their websites, kavkaz.org and chechenpress.com, crashed under hack attacks by the Russian FSB security service. The website crashes were reportedly timed to occur concurrently or shortly after Russian Special Forces troops stormed the Moscow Theater in which the rebels had taken hostages. "On October 26 ... our Web Site kavkaz.org was attacked by a group of hackers," said a spokesman for the Chechen rebel site run by Movladi Udugov. Following the attack on the site, which is based in the United States, Udugov said that he was "amazed Russia's special services can operate so freely on U.S. territory."[472] The attacks on one site, chechenpress.com, fell under the category of brute-force denial of service (DoS) attacks, while on the other site, kavkaz.org, the attacks appeared much more sophisticated. According to Chechen sources, the website was hijacked by hackers from the FSB. The FSB hackers reportedly accomplished this by changing the domain registration of the site and then eliminating the data for the site from the hosting server. Upon learning of these attacks, the rebels moved the information on the sites to kavkazcenter.com. However, that site was attacked just a week later, also apparently the work of FSB hackers.[473]

7.3.2 Russian cyber warfare doctrine compared

Moscow's cyber warfare does have similarities with its Chinese counterpart and other cyber warfare programs. A common aspect for almost all cyber warfare programs is that the ultimate goal of an offensive doctrine is the planning of and subsequent execution of an effective cyber "first-strike" against the enemy. This "digital pearl harbor" (discussed theoretically) is an ideal

[471] Lieutenant Colonel (ret.) Timothy L. Thomas, Foreign Military Studies Office, Fort Leavenworth, KS., "Manipulating The Mass Consciousness: Russian And Chechen 'Information War' Tactics In The 2nd Chechen-Russian Conflict," <http://fmso.leavenworth.army.mil/fmsopubs/issues/chechiw.htm>

[472] Oliver Burroughs, Reuters, "Russians wage cyber war on Chechen websites," November 14, 2002 <http://www.intellnet.org/news/2002/11/14/13396-1.html>

[473] Ibid Burroughs 2002

cyber attack strike when it is able to defeat the enemy without the attacker actually having to resort to physical battle. According to Professor Major General Vladimir Belous, "it can be predicted that the battlefield of the future will begin to shift more and more into the area of intellectual effect. An aggressor country is capable of developing, and under certain conditions executing, a scenario of information war against another state in an attempt to demolish it from within. In that way it is possible to force the enemy to surrender without using traditional kinds of weapons."[474]

Russian cyber warfare doctrine also addresses the optimum time to strike. Prior to an "information strike", all targets should be identified (including enemy information systems), enemy access to external information should be denied, credit and monetary circulation should be disrupted, and the populace should be subjected to a massive psychological operation--including disinformation and propaganda. This would be accomplished by careful pre-strike planning and long-term investments in reconnaissance and covert penetration into enemy systems.

"Computer networks and databases are penetrated in advance before the beginning of combat operations by agent and other methods, and microorganism cultures are introduced that eat away electronic components. The employment of information weapons in the concluding phase of a major regional conflict is similar to their use in peacekeeping operations. Estimates have shown that the use of information weapons must be constantly accompanied by the limited use or threat of use of conventional weapons, especially high-precision weapons."[475]

Officially, the Russian government has a globally non-interventionist stance regarding the application of cyber warfare. Former Minister of Defense Ivanov spoke on the new military doctrine of the Russian Federation in 2001. One of the questions asked of him was whether there had been any measures undertaken to create a capability to wage cyber wars using computer networks and other types of communication. The response was somewhat circular and evasive with the first part of it stating that the "fundamental stance of Russia is to observe the principles of non-application of force, non-intervention in internal affairs, respect for the human rights and freedoms, and not permitting achievements in the sphere of information sciences and telecommunications to be used for purposes that are in contravention of the UN Charter."[476] A thinly veiled barb at the "overwhelmingly" advanced state of U.S. cyber warfare capabilities, Ivanov's statements were made in response to the "existence of the Anglo-American Echelon global spying system." When asked about the Echelon program, the National Security Agency's (NSA) SIGINT gathering system, Ivanov said that "FAPSI, the Ministry of Defense, the FSB of Russia, the State Technical Commission of Russia, and other federal executive authorities are taking suitable steps aimed at raising the level of protection for information being transmitted." This statement provides evidence that Russia has at least some measure of a defensive cyber warfare capability.[477]

[474] FBIS Translation Sergey Ishchenko, "Before the verdict is in: Computers on the attack: Cyberwars already are being depicted on Staff Maps," *Moscow Trud*, June 28, 2001

[475] FBIS Translation Professor Aleksandr V. Fedorov, Russian Academy of Natural Sciences "Information Weapons as a New Means of warfare," *Moscow PIR Center,* August 1, 2001, pp. 69-109

[476] FBIS Translation Interview with Security Council Secretary Sergey Ivanov, "The Military Doctrine of RF," *Moscow Krasnyy Voin* April 25, 2001

[477] Ibid Ivanov 2001

However, Russian intelligence and security services and the Russian government deny accusations of official involvement as regards an offensive capability. Boris Labusov, spokesman for Russia's SVR (Foreign Intelligence Service), asked, "Do you think Russian special services are so stupid as to engage in such activities directly from Moscow? For decades, everybody has written about how clever the KGB and Soviet intelligence are. Why should one think we suddenly became less clever enough not to allow themselves to be traced?"[478] According to Russian media analysis, fears of Russian hackers may have been the factor that spurred funding for NIPC in 1999, as the Clinton administration sought to develop programs for the defense of computer networks.[479]

7.4 CONCLUSION

Much of the initial Russian research and development in cyber warfare has been conducted in response to what the Russian government considers an aggressive development of a U.S. information warfare program. Although relations between Washington and Moscow have improved since the end of the Cold War, beneath the new peaceful rhetoric some tensions remain. Russian actions against the Chechens have drawn increasing ire from the international community and recent refusals to back the U.S. military action in Iraq signal that the relationship between the two countries remains fundamentally wary. If the recent revelation of Robert Hanssen as the most damaging mole in U.S. history is any indication, Russia's active secret services still have considerable resources and energy to spend on espionage in the United States. This, coupled with an advanced cyber warfare doctrine, documented technical expertise, and dedicated intelligence services (as discussed above), makes Russia a considerable cyber-threat to U.S. computer systems. As described in this study, Moscow has demonstrated a willingness to use cyber warfare against perceived threats, as evidenced by the actions of the FSB against Chechen rebel websites in the ongoing conflict.

Although it is unlikely Russia would launch a pre-emptive cyber strike on the U.S. absent a state of war, it is highly likely that Russian intelligence services will continue to scout U.S. military and private sector sites in order to gain information.[480] Add to this the fact that intelligence gathering from a remote location is very hard to trace and also fairly inexpensive, cyber warfare represents a viable solution to the Russian government's cost-cutting in the areas of military and intelligence services.[481]

---

[478] Aerotech News and Review, "Russia spies no link between hackers, Kremlin," <http://www.aerotechnews.com/starc/1999/101599/Hackers.html> October 15, 1999

[479] Arseniy Kapitonov, "Clinton is Afraid of Russian Hackers. United States Prepares for Information Wars which 'Could Bring America to its knees'," *Moscow Nezavisimaya Gazeta*, October 2, 1999

[480] For a counter-view, George Smith, editor of Crypt News, purports that Russian information warfare is a concocted story. George Smith, Crypt News 44, "Ghost Stories Seen Through a Mirror," <http://www.soci.niu.edu/~crypt/other/fitz.htm>

[481] For a further discussion of Russia's network warfare capabilities, see Lieutenant Colonel (ret.) Timothy Thomas's article "Russia's 'netwar' capabilities," *Jane's Intelligence Review*, July 2002

Figure 1[482]

- Means of effect on components of electronic equipment and its power supply.
- Temporary or irreversible disabling of individual components of electronic systems.
- Means of power electronic suppression: ultrapowerful microwave generators (gyrotrons, reflex triodes, relativistic magnetrons, turbutrons); Explosive magnetic generators; Explosive magnetohydrodynamic generators. Means of power effect through an electrical network.
- Software for disabling equipment (hard drive head resonance, monitor burnout and so on).
- Software for erasing rewritable memory.
- Software for affecting continuous power sources and so on.
- Means of disabling electrical networks.
- Means of effect on programming resource of electronic control modules
- Disabling or changing the algorithm of functioning of control system software by using special software.
- Means of penetrating information security systems. Means of penetrating enemy information networks. Means of concealing information collection sources. Means of disabling all or specific software of an information system, possibly at a strictly given point in time or with the onset of a certain event in the system.
- Means of covertly partially changing the algorithm of functioning of the software. Means of collecting data circulating in the enemy information system. Means of delivery and introduction of specific algorithms to a specific place of an information system. Means of effect on facility security systems.
- Means of effect on programming resource of electronic control modules.
- Stopping or disorganizing the functioning of data exchange subsystems by an effect on the signal propagation medium and on the algorithms of functioning.
- EW assets, especially ground-based and airborne (helicopter and UAV) communications jammers (possibly with elements of artificial intelligence.) Droppable expendable jammers.
- Means of effect on data transfer protocols of communications and data transfer systems. Means of effect on addressing and routing algorithms. Means of intercepting and disrupting the passage of information in its technical transfer channels. Means of provoking a system overload by false requests for establishing contact.

[482] This figure details some of the research the Russian Academy of Natural Sciences has conducted into cyber warfare. FBIS Translation of Professor Aleksandr V. Fedorov, Russian Academy of Natural Sciences "Information Weapons as a New Means of warfare," *Moscow PIR Center* August 1, 2001 pp. 69-109

Figure 2

The Russian military seeks to use the Federal Agency for Government Communications and Information (FAPSI much like the National Security Agency or NSA) to combat unsanctioned access to government and military materials. The Russian military and FAPSI have also been looking into using viruses as a method of warfare, especially as a force multiplier unleashed at the start of the conflict. A primary goal of the Russian intelligence agencies is to gain superiority in "information accumulation, processing and adaptation..., and especially in reconnaissance and electronic warfare systems." The Russians also seek to achieve significant capabilities in disrupting the enemy's information support system. All of these things are used in attempting to control the actions of the enemy; they amount to the general Russian view of information warfare. Priority problems for the Russian military that they are attempting to tackle include: "creating a telecommunications environment and its lash-up with nation-wide communications and data-transmission systems; developing and incorporating base problem-oriented systems; equipping the armed forces staffs and organizations quickly with the basics of information technology and personal computers, advanced communications and telecommunications gear, and improved organizational techniques to adopt a "paperless" information technology; improving tools and methods for developing software and the use of computer assisted technologies; assuring technical, information, linguistic, and program compatibility; improving the system of training, retraining, and skill enhancement of military specialists; and creating standardized, advanced means of information technology…[483]

[483] Excerpts of Lieutenant Colonel (ret.) Timothy L. Thomas, "Russian views on Information-Based Warfare," Foreign Military Studies Office, Fort Leavenworth, KS. <http://fmso.leavenworth.army.mil/fmsopubs/issues/rusvuiw.htm> and as published in the *Airpower Journal*, <http://www.airpower.maxwell.af.mil/airchronicles/apj/thomas.pdf>

VIII. CONCLUSION

"Whatever the direction the cyber threat takes, the United States will be confronting an increasingly interconnected world in the years ahead…A major drawback of the global diffusion of information technology is our heightened vulnerability. Our "wired" society puts all of us—US business, in particular, because they must maintain an open exchange with customers—at higher risk from enemies. In general, IT's spread and the growth of worldwide digital networks mean that we are challenged to think more broadly about national security."

Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, Statement for the Record to the Joint Economic Committee, U.S. Congress, June 21, 2001

"There are a large number of [cyber] threats: hackers, cybercriminals, other countries. It goes beyond al-Qaeda."

Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division
USA Today, August 2, 2004

"This brings about the principle of 'Information Age' conflict: that with a little bit of disruption, you may do a lot more than by focusing strictly on destruction."

John Arquilla, Professor at the Naval Post-Graduate School
International Relations in the Information Age interview, UC Berkeley, March 17, 2003

"The rise of cheap computing, networked via the Internet, has changed the way work is organized to such an extent that executives and policy makers are struggling to understand the opportunities and consequences. One consequence is the battle to keep business information private and secure; companies spend billions trying to address risks unimagined 10 years ago."

Eric Johnson, Professor of Operations Management, Tuck School of Business,
Financial Times, August 18, 2004

The evidence laid out in the previous six country studies shows that governments and foreign militaries have varying means and motivations in pursuing cyber warfare capabilities. Different countries have different motives in penetrating or "intruding" on our systems. Among these are intelligence gathering, software theft, compromise of data integrity, and perception management.

This chapter brings together several features of the cyber warfare landscape that assist in placing the country assessments in this report in better perspective. Conceptually, a hack (into an electronic network) could begin with an approach as simple as hiring a skilled individual to exploit a vulnerability in software on a desktop computer. As cyber warfare programs progress and evolve, the conceptual becomes increasingly complex. Nevertheless, as an overall principle, we distinguish between attacking networks (the "target") and using the Internet (as a carrier) to attack critical infrastructure.

Although the countries examined in the report may demonstratre varying degrees of potential, a logical deduction is that these countries will use their capabilities in an offensive fashion, a deduction that becomes more and more of a concern as network technology becomes a ubiquitous part of the invisible infrastructure that makes daily life possible in advanced industrial countries.

In this chapter, we discuss how serious the vulnerabilities to critical infrastructure are. The current state of affairs suggests that the U.S. public and government and corporate leaders must be vigilant to an apparent rise in the number and sophistication of politically motivated software attacks. Based upon this analysis, we outline policy recommendations and courses of action to help create a more secure cyber infrastructure.

8.1 BACKGROUND: THE NATION-STATE ADVANTAGE

According to the U.S. intelligence community, "only government sponsored programs" are developing the cyber tradecraft with the future prospect of targeting U.S. critical infrastructures.[484] While intrusions and attacks are not the exclusive province of large, hierarchical organizations, larger organizations do have advantages in resources and longer time-horizon probes, i.e., probes designed to foil U.S. government and military systems encryption. The time-horizon for nation-states operating in this fashion is much longer because many of the reconnoitering activities are considered innocuous. Terrorists, on the other hand, generally have limited resources and thus will place their resources where the impact is largest (e.g., physical attacks).

A hostile nation-state conducting a cyber attack on the United States is likely to conceal its identity to minimize the likelihood of retaliation. In these circumstances, a hostile government might adopt the tactic of sponsoring terrorists or mercenary hacker cells who can attack without leaving clear national signatures.[485]

In addition to hiring or sponsoring cyber warfare "agents," a nation-state can spoof or conceal the origin of the digital "hops" through cyberspace in conducting an attack. Current technology permits a variety of methods to conceal points of origin. Such "laundering" techniques (described in the figure below), by masking the origin of the attack, tend to weaken conventional deterrence predicated on the threat of swift and accurate retaliatory response.

Figure 1: Laundering the Attack

- Spoofing: This represents an attempt by an unauthorized entity to gain access to a system by posing as an authorized user. There are several spoofing techniques involving faking the IP address of a legitimate neighbor using knowledge of the number of hops involved. More recently, a program called NCovert uses spoofing techniques (forging the source of the IP address to appear like the intended recipient of the information) to conceal the source of data that passes over a network.[486]

- Wireless: Proliferation of wireless access points permits access to the Internet by anyone within range of an unsecured 802.11b site. A recent article discussed "Wardriving"

[484] Lawrence K. Gershwin, op. cit. p. 6

[485] Nation states may sponsor terrorists or hacker cells, providing human and other resources to defeat encryption or corrupt distribution of hardware and software. National Research Council, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," 2002, p. 143

[486] "Hackers Look to Hide Communications," CNET News.com, July 31, 2003

in which individuals try to identify poorly-secured networks by driving with a laptop.[487]

- Universities: These usually have extensive Internet connectivity. PCs are often readily accessible to unauthorized persons and the large number of users requires significant bandwidth with minimal monitoring.[488]

- Internet Cafés: These provide services in locations where users are often transiting a country or where individuals may not be able to afford a computer and Internet connectivity. Little attempt is made to register or identify patrons.

- Direct Access Satellite: Direct satellite access requires authentication which can be traced back to a registered user having paid for that access. If the actual user, however, is different than the registered user then the authentication process is meaningless.

8.2 HOW VULNERABLE ARE WE?

This section introduces the general concept of targets and vulnerabilities and assesses some of the parameters. In section 8.2.1 we examine individual segments of the critical infrastructure in greater depth. How and what would nation-states attack using a cyber capability and how important a factor is internet architecture i.e., topology? The popular media discuss a Digital Pearl Harbor in which an adversary would attack the Internet, dismembering the cyberspace "backbone," plunging the economy into chaos and putting U.S. national security at risk. Conventional wisdom has it that the Internet backbone is quite resilient because of built-in redundancies. While a slow-down in service might occur, traffic would continue to flow through alternative nodes.[489] However, recent research and findings has shown that the Internet and networks in general may not possess the redundancies once thought, a result primarily due to the major Internet hubs that have grown as a result of the increase in Internet usage. In a major geographic study of network topology, Grubesic, O'Kelly and Murray concluded that because of the competitive nature of the Internet service, the "Internet backbone provider industry has created a situation where many backbones are prone to disconnection if there is a major failure in a hub city for a given network," which could have a potentially "economically catastrophic [effect] for businesses, cities, and regions."[490]

---

[487] "Hackers Wardrive on Wireless," *Mobile Radio Technology*, July 1, 2003

[488] In March 2001, the U.S. Navy Criminal Investigative Service was investigating the penetration of a Naval Research Laboratory unclassified system. According to media reports, the hack took place over the Internet on December 24, 2000. Although the hacker used the name Leeif on the system, the Swedish ISP Carbonide said the account was stolen. Carbonide was able to trace the attack on its network to a server at the University of Kaiserslautern in Germany. "Hackers Steal Military Source Code," *VNU Business Publications Newswire*, March 15, 2001

[489] "The Internet could be seriously degraded for a relatively short period of time, but this is unlikely to be long lasting…Destruction of some key Internet nodes would result in slowed traffic across the Internet, but the ease with which Internet communications can be rerouted would minimize the long-term damage." National Research Council, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," 2002, p. 137

[490] Tony H. Grubesic, Morton E. O'Kelly and Alan T. Murray, Ohio State University, "A geographic perspective on commercial Internet survivability," *Telematics and Informatics* 20, 2003 p. 66

An additional factor that is often overlooked is that potential attackers have an interest in maintaining the integrity of the Internet because it provides a vehicle for launching cyber attacks against critical nodes or systems in the United States and elsewhere. Moreover, the Internet allows one to mount an attack at a remote distance in a "relatively anonymous fashion, and in potentially undetectable ways."[491] It is therefore necessary to distinguish between the "carrier" of an attack (i.e., the Internet) and the target of an attack (i.e., a computer network or other embedded computer control and supervison systems.) In the most extreme of cases, the Internet itself could become the target of a concerted attack, however, as many attacks are executed across the connections fostered by the Internet, it is unlikely that such a concerted attack could be sustained.

Second, with respect to topology, compromise of national-level networks (including government, corporate/financial, and military/national security) carries more extreme economic and related consequences.

As depicted in Figure 3 below, successful attacks have targeted a broad gamut of local and national sites ranging from air and ground transportation and the banking system, to physical infrastructure (such as dams and power grids), to government services and military systems. The degree of disruption in these examples varied. In some cases, the attacks amounted to mere nuisances while in others the effects were economically costly.

It is therefore important to distinguish between targets that can be localized geographically and those, such as the systems of federal and state government agencies or the telecommunications infrastructure of the public switched network, which are regional and even national in scope. Reportedly, most telephonic and other communications and data networks in the United States tend to be restricted geographically (i.e., localized) and reparable relatively quickly. An attack that undermines confidence at a broader, national level, however, is likely to have more extreme economic or psychological consequences (impairment of "trust").

[491] National Research Council, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," (Washington D.C., National Academy Press, 2002), p. 143

Figure 2: Comparing Cyber Attacks by Degree of Disruptiveness

Local Geographic Impact

This category might include town governments, small businesses, and local hospitals.

1. Scanning (little or no disruptive consequence but could lead to wider implications)
2. Reconnaissance of vulnerabilities
3. Website defacements (hacktivism such as defacing the website with web graffiti)
4. Data, identity, and sensitive information theft (e.g., an individual's social security number)
5. Undetected alteration of data (your birthday on a website)
6. Denial of service attacks (attacks on a single website that do not permanently disrupt availability)[492]

National Level Impact

[Government Services]

Illustratively, this category would embrace agencies such as U.S. Social Security Administration; National Institutes of Health; Center for Disease Control; Department of Energy; Federal Reserve System, and more.

1. Web defacements (malicious intent, such as changing the site listing of indications of the SARS virus on the CDC website)
2. Semantic hacking (interference with search engines and news websites, such as CNN)
3. Denial of service attacks (sustained interference with a web service or site)

[Economic]

This category includes multinational corporations; global financial institutions; and critical components of the U.S. economic infrastructure (transportation, electricity, water, telecommunications, etc.)

1. Undermining the integrity of the banking system and inter-bank trust
2. Corrupting corporate data tables and degrading delivery schedules
3. Industrial espionage (stealing all of Ford motors car schematics for 2004)
4. Hacking SCADA systems

[National Security]

Examples of organizations in this category include the Pentagon, Armed Forces, intelligence organizations, FBI, and the National Labs (Sandia, Lawrence Livermore, among others).

1. Denial of Service attacks degrading military procurement, transport, and logistics[493]
2. Theft of classified data (e.g., plans about troop deployment in Iraq for March 2003)
3. Psychological and disinformation campaigns[494]

8.2.1 Vulnerabilities in Existing Critical Infrastructure[495]

Skeptics claim that computer networks are not vulnerable to cyber attack. Criticism comes in a variety of flavors, ranging from complete denial of the existence of vulnerabilities to the argument that although vulnerabilities exist, the built-in redundancy of networks make them inherently able to withstand concerted attacks from multiple locations. Another observation some experts have made is that cyber attacks are easily defended against, that the attack itself becomes

[492] Distributed denial of service attacks cause havoc among e-trading and e-commerce sites as they prevent transactions from being conducted in a timely manner. See footnote 522 for futher explanation of this type of attack.

[493] The Pentagon uses the Internet for selected activities, such as transportation and logistics. As RAND has pointed out, "Current or potential adversaries may also gain access through foreign suppliers to software encoded in U.S. transportation and other infrastructure systems. We could thus one day see actions equivalent to strategic attack on targets of national value within the U.S. homeland and on essential national security components and capabilities." RAND Research Brief, "Strategic War in Cyber Space," January 1996, available at <http://www.rand.org/purblications/RB/RB7106/RB7106.html>

[494] All of the methods of attack have the potential to undermine trust and raise the level of uncertainty and even fear among the population.

[495] For more vulnerabilities see Appendix A

regionalized or isolated as quickly as it appeared. Skeptics feel that any talk of cyber warfare having a "devastating" effect on computer networks has the appearance of being alarmist and Cassandra-like. This claim is strong and bolstered by the available open source evidence, suggesting that some of the effects of cyber attacks are local and do not warrant the efforts of a concerted program to solve vulnerabilities in the critical infrastructure and networks of states. What these critics lack is vision and imagination; it is a logical prediction that as network connectivity and dependency on the Internet increases, the number and the overall disruptive effect of vulnerabilities and exploits will also increase.

Before attempting to assess the degree of disruptiveness of attacks, we must set the boundaries of the universe of possible attacks. First, according to the National Research Council, cyber offense is aimed at four IT categories: 1) Internet; 2) telecommunications infrastructure (e.g., telephone, fax, satellite communications; wireless cell phones, etc.); 3) embedded real time computing (e.g., avionics; supervisory control and data acquisition systems [SCADA] systems controlling physical plants such as hydroelectric dams, power grids, pipelines, etc.); and 4) dedicated computing devices (e.g., desktop computers).[496]

Internet:

Cyber attacks against computer networks can occur along any point of the network, encompassing a wide range of possible entrance points including central routers (forming the crux of the Internet's connectivity), Domain Name Servers, central servers operated by Internet Service Providers, all the way to vulnerabilities at the end-user level. The Internet, similar to the cosmological concept of an open universe, has no beginning and no end when discussing the "direction of a cyber attack."

Telecommunications Infrastructure:

The vulnerabilities in a single part of cyber space may be the same in other parts of cyber space, as the ubiquity of software applications and operating systems[497] makes it likely that a zero-day exploit could cause significant damage because of the inability of programmers to fix all vulnerabilities within networks and software. A zero-day exploit is particularly damaging because it targets a previously unknown vulnerability, precluding any attempt by programmers to patch the targeted vulnerability. Viruses and worms spread in a nondiscriminatory fashion, affecting servers and end-users alike and diffusion occurs in the network from both central locations and peripheral locations. There are also vulnerabilities involved with software and electronic mail, server software and other applications.

Embedded Real Time Computing:

The increased reliance on SCADA systems in water treatment facilities, hydroelectric dams, electric grids, oil pipelines and other utilities increases the possibility of it becoming a target of cyber attack. Because these systems are often linked to commercial IT systems, a vulnerability

[496] NRC, op. cit., p. 138
[497] Some examples are Windows XP, Internet Explorer, Linux, Mac OS X

on a company's network can be translated into a vulnerability that could link to SCADA systems.[498]

Dedicated Computing devices:

Computing devices such as desktop computers and network servers, in particular those that are connected by "always-on" connections, are vulnerable to intrusions.

Figure 3: Historical examples of successful cyber attacks

In the open source realm, documented accounts of cyber attacks have been plentiful in light of the security danger such reports pose. There have been many serious instances of cyber attacks causing SCADA[499] systems and other computer networks to malfunction as a result of accidental or targeted and malicious intent. The summary below, presented by category, details incidents of recent attacks against and disruptions of critical infrastructure and sensitive computer networks.

Air and Ground Transportation

In January of 2003, Continental Airlines based in Newark, NJ was forced to ground flights due to system inoperability caused by the SQL "Slammer" virus.[500]

Banking Systems

In January of 2003, Bank of America had 13,000 ATM machines rendered inoperable due to the SQL "Slammer" virus.[501]

Dams and Waterways

A well-documented and oft-quoted incident refers to a known case in 1998 when a 12-year old hacker broke into the computer system controlling Arizona's Roosevelt Dam's floodgates. According to sources, the hacker had complete control of the command SCADA system for the dam and could have flooded the city of Phoenix.[502]

Another well documented incident refers to the April 23, 2000 arrest of Vitek Boden, a man who successfully intruded into a Queensland, Australia wastewater management system 46 times. For two months, the attacks were a mystery to investigators as Boden dumped hundreds of thousands of gallons of waste into parks, rivers, and commercial properties.[503]

[498] See Riptech Report, "Understanding SCADA Systems Vulnerabilities," January 2001, <http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf>

[499] See Appendix A for further discussion of SCADA utilities and systems

[500] Daniel Sieberg and Dana Bash, "Computer worm grounds flights, blocks ATMs," CNN, January 26, 2003

[501] Ibid Bash and Sieberg 2003

[502] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 2002 <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>

[503] *It's America*, "Internet-Based And Remotely-Controlled Public Infrastructure And Utility Networks More Vulnerable Than Previously Thought," June 27, 2002 <http://www.itsa.org/ITSNEWS.NSF/0/3f141fc26dcebd5a85256be600617016?OpenDocument>

A December 2002 report from Mechanical Engineering cites examples of "wardriving" into SCADA-controlled utilities. According to Paul Blomgren, manager of sales engineering at cybersecurity firm Rainbow Mykotronx based in Torrance, California: "Our people drove to a remote substation," he said. "Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords." "Within 10 minutes, they had mapped every piece of equipment in the facility," Blomgren said. "Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports. They never even left the vehicle." [504]

Telephones

On February 7, 2002 President Bush was notified of a serious vulnerability with the Abstract Syntax Notification 1 (ASN.1) data transmission standard that the FBI assesses could have been exploited to disable telephone networks and "halt all control information exchanged between ground and aircraft flight control systems."[505]

Power Grids and other Energy Related Infrastructure

In April of 2000 the "ILOVEYOU" virus rendered a petroleum refinery in Texas inoperable.[506]

In January of 2003, the SQL "Slammer" worm disabled the monitoring computers at Ohio's Davis-Besse nuclear power plant in Toledo, Ohio.[507]

Government Services and Military Systems

In 1994, a 16-year old English hacker took down hundreds of Department of Defense systems. Thankfully these systems were not classified.[508]

In September of 2003 the "Welchia" virus disabled the State Department's Consular Lookout and Support System (CLASS) which contained more than 15 million records from the FBI, State Department and U.S. immigration and provided consular offices assistance in processing visas to foreigners.[509]

[504] Alan S. Brown, , "SCADA vs. the Hackers," *Mechanical Engineering*, December 2002 <http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html>

[505] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 2002 <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>

[506] Asian School of Cyber Laws, "Securing critical oil infrastructure from cyber threats" <http://www.asianlaws.org/cyberlaw/library/cc/oil_report.htm>

[507] Jim Crane, "Hacker Danger for Power Supply?," CBS News, September 11, 2003 <http//www.cbsnews.com/stories/2003/09/11/tech/printable572770.shtml>

[508] Ibid Crane 2003

[509] Ted Bridis, "Virus its Federal Visa-Checking System," AP, September 24, 2003 <http://www.newsday.com/news/politics/wire/sns-ap-state-computer-virus>

Along with documented successful cyber attacks, there have also been several mass cyber exercises simulating an organized nation-state adversary carrying out cyber warfare against American assets and critical infrastructure.

Figure 4: Simulations

Exercise Eligible Receiver

In 1997, a NSA exercise employing 35 computer specialists used hacking tools from 1,900 documented hacker websites to disable large parts of the U.S. power grid. They were also able to disrupt the C2 system of Pacific Command based in Honolulu.[510] The exercise, conducted over 2 weeks in June of 1997 by the Joint Chiefs of Staff and the Department of Defense, attacked unclassified Defense Department computer systems and pieces of critical infrastructure in the United States. The Department of Defense owned approximately 2.1 million computers (1999) and hundreds of local area networks in the unclassified realm that were the targets of attack. The report that was released by Defense Department individuals in light of the results of the exercise pointed to a lack of knowledge about what hackers could do with computers and information readily available on the internet.[511]

Digital Pearl Harbor[512]

This seminar-style (no actual computer intrusion was performed) wargaming exercise was made possible through the joint efforts of IT professionals, Gartner Inc., and the U.S. Naval War College. The conference was conducted in July of 2002 over a period of three days to determine whether cyber terrorists could attack the United States in a "Pearl Harbor" type attack in terms of timing, magnitude, and planning. The exercise presupposed that a cyber terrorist organization would have access to $200 million and 5 years of planning along with Internet access to do their research in order to launch an attack of this magnitude.

The results of the attacks on financial institutions, telecommunications networks, the Internet, and the electric power grid showed that different areas would be affected differently due to security measures already in place. While it was fairly easy to shut down large portions of the Internet, create havoc on the financial markets, and shutdown the electrical power grid to a large region of the United States, it was very difficult to take out the telecommunications networks because of existing security.

OPLAN 3600

The name of the Pentagon's plan to defend against acts of cyber warfare. It also details how to enact cyberwarfare against another country.[513]

[510] Ibid Bridis 2003
[511] Kenneth H. Bacon, "DoD News Briefing," April 16, 1998 <http://www.defenselink.mil/news/Apr1998/t04161998_t0416asd.html>
[512] See Appendix A for a summary of the exercise and more specific details regarding its implementation <http://www3.gartner.com/2_events/audioconferences/dph/dph.html>

Energy Department Simulation

According to a Washington Post report, the Department of Energy conducted its own investigation into potential vulnerabilities within the power grid. "What they do know is that "Red Teams" of mock intruders from the Energy Department's four national laboratories have devised what one government document listed as "eight scenarios for SCADA attack on an electrical power grid" -- and all of them work. Eighteen such exercises have been conducted to date against large regional utilities, and Richard A. Clarke, Bush's cyber-security adviser, said the intruders 'have always, always succeeded.'"[514]

Livewire National Cyber Exercise

In October 2003, the Institute for Security Technology Studies at Dartmouth College designed and managed "Operation Livewire", a simulation sponsored by the Department of Homeland Security. The purpose of the exercise was to examine the challenges of responding to a large-scale cyber attack directed against the U.S. telecommunications, energy, banking, and finance sectors. The simulation involved an East Coast city, a West Coast city, and various private corporations in 14 locations throughout the country. An After Action Report assessed the response of law enforcement at federal, state, and local levels to the simulated attack.

Beyond these simulations, several incidents of intrusions and information theft in government computer systems in the late 1990's are now cited as prime examples of the dangers of cyber warfare.

Figure 5: Cyber attacks of importance to national security

Rome Labs Incident

In 1994, the Air Force's Rome Labs computers were broken into by two UK hacker youths, causing an estimated $500,000 worth of damage. At that time Rome Labs was the Air Force's center for command and control research.[515]

Moonlight Maze

[513] CNN, "U.S. Army kick starts cyberwar machine," November 22, 2000, <http://www.cnn.com/2000/TECH/computing/11/22/cyberwar.machine.idg/index.html>

[514] Barton Gellman, "Cyber-attacks by al-Qaeda feared," June 27, 2002, p. A01, <http://www.washingpost.com/ac2/wp-dyn/A50765-2002Jun26?start=48&per=16>

[515] "GAO reports DoD SBU Computer Security Inadequate," <http://www.ieee-security.org/Cipher/Newsbriefs/1996/960522.GAOrept.html>;
See also: Congressional Research Service, "Security in Cyberspace," June 5, 1996 <http://www.fas.org/irp/congress/1996_hr/>; and
Anthony H. Cordesman, "Critical Infrastructure Protection and Information Warfare," Center for Strategic and International Studies, December 8, 2003, *Defending America: Redefining the Conceptual Borders of Homeland Defense*

In March of 1998, U.S. officials discovered a "pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities and research labs, which had begun in March 1998 and had been going on for nearly two years."[516] The attacks were traced to the Soviet Union, to an Internet provider hub that was in close proximity to the Russian Academy of Sciences. Soviet officials denied having anything to do with them.[517]

Solar Sunrise

Originally suspected to be the work of Russian hackers, these attacks were eventually traced to two hackers in California and an Israeli youth working in concert. The attacks occurred in 1998, and the hackers were able to attain troop movement information for the U.S. military in the Gulf region. The nature of the attacks and penetrations were so well coordinated that it led Deputy Secretary of Defense John Hamre to say that it was one of the "most organized and systematic attack" on U.S. systems to date.[518]

In addition to the effects of cyber attacks on critical infrastructure, cyber warfare could also cause significant damage to a nation's economy. Although some believe that the estimates of the costs of virus outbreaks and disruptive worms are exaggerated, the result of a cyber attack on a company's "just-in-time" delivery system, for example, or a denial-of-service attack on an online retailer is not a monetary amount that can be easily dismissed.[519]

Professor Eric Johnson points out that in today's globalized, digitized world, workers often perform in extended enterprises involving disparate firms widely dispersed and communicating through the Internet. Through a web browser, business decisions and design changes can be communicated across borders and continents instantaneously. "Every one of those interactions could potentially be observed or disrupted by youthful hackers seeking a thrill, or other more malicious individuals pursuing competitive gain."[520]

[516] PBS Frontline, "Warnings?," *Cyberwar!*, 2003 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>

[517] Anthony H. Cordesman, "Critical Infrastructure Protection and Information Warfare," Center for Strategic and International Studies, December 8, 2003, *Defending America: Redefining the Conceptual Borders of Homeland Defense* p.60

[518] Anthony H. Cordesman, "Critical Infrastructure Protection and Information Warfare," Center for Strategic and International Studies, December 8, 2003, *Defending America: Redefining the Conceptual Borders of Homeland Defense* p.62

[519] See the work of Scott Borg, a former Senior Research Fellow, Institute for Security Technology Studies, summarized in Martin Wybourne, Director, "ISTS Categorical Assistance Progress Report, January 1-June 30, 2004," July 28, 2004 p. 21 <http://www.ists.dartmouth.edu/ISTS/library/briefings/ist0704.pdf>

[520] Eric Johnson, "The Safety of Secrets in Extended Enterprises: Globalization and the Internet Have Exposed Companies' Information Systems to New Security Threats," *Financial Times*, August 18, 2004.

8.3 SUMMARY AND RECOMMENDATIONS TO POLICYMAKERS

In approaching recommendations to policymakers and the IT industry, we suggest the following boundary conditions:

1) Our adversaries or potential adversaries have resources, expertise, training, and know-how that is world class. This factor should not be underestimated. It places a premium on "creativity" in fashioning response measures.

2) Defining a "catastrophic" attack is fraught with difficulty. Absent such a scenario, however, we believe that our adversaries are capable of inflicting significant material, financial, and psychological damage through denial of service and related attacks that inflict a disproportionate toll on our economic welfare and our standard of living, in some cases. We agree, however, that considerable additional work will have to be performed to calculate more accurately the economic costs that are passed from businesses to the consumer. The cost of "lost trust", on the other hand, is perhaps immeasurable.

3) As the IT revolution deepens and matures, civilian information technologies will increasingly be incorporated in the military and the defense sector. Hostile nation-states could, for example, employ cyber assaults to disrupt or impede the mobilization, deployment, or resupply of U.S. military forces.[521]

We have identified *three general areas of vulnerabilities*, which, if left unmitigated, would be cause for future concern:

A. Critical Infrastructure

Although the civilian critical infrastructure currently has known vulnerabilities, these vulnerabilities have only led to temporary outages, short-term economic losses and inconveniences. However, future outages of longer duration and intensity could cause significant disruptions.

B. Economic and Financial Sector

Again, the commercial sector has suffered only slowdowns and degradation due to unauthorized intrusions, but the rising costs of these actions and the fact that these costs are passed onto the consumer are not trivial consequences. The fact that trust is reduced as the availability of these services becomes more and more unpredictable could lead to longer-term economic losses. Moreover, cyber attacks might also disrupt by corrupting or deleting data. This has significant implications extending beyond simple congestion or Denial of Service experienced, for example, in recent computer worms.

[521] Some portions of the U.S. military transportation and logistics capability is contracted to the private sector and consequently may lie outside the firewall of protection.

C. Military and National Security Sector

As militaries and intelligence services rely more and more on IT in order to modernize efficiently, this reliance opens up more holes in critical military infrastructure, while fostering a spiral of deterrence as each side attempts to one-up the other in exploiting a cyber attack capability. Much of the Pentagon logistics chain flows over public-switched networks. Some of the intelligence gathering of U.S. intelligence agencies also flows over public networks. Secure IT is critical in making sure that the data received on both ends of an intelligence transmission is not compromised.

Fundamental considerations remain. Due to convergence, the way that information technology and telecommunications are morphing into a single entity, it will be difficult to discern all of the possible vulnerabilities in a network. Viewed from a global perspective, for example, the development of information technology has been seen as an efficient way to modernize and increase economic well-being. This global implication raises two concerns:

1. increasing connectivity and networking increases the amount of critical infrastructure that must be protected while simultaneously adding to the number of vulnerabilities in critical infrastructures, and

2. it dramatically expands the number of people that have knowledge and access to this critical infrastructure.

Information Technology is a reciprocal power: it can be used to benefit mankind, and it can be used to harm it.

8.4 RECOMMENDATIONS

What should the U.S. be doing about it?

1. *Technology is important—but no panacea.*

In recent years, software and hardware producers have begun to make their products more secure. Stronger operating system kernels, faster anti-virus software and virus detection, tougher firewalls and Internet browsers—these are just some of the steps taken to help cut down on the vulnerabilities present in today's network architecture. However, whatever patches or software re-design are devised and created by software manufacturers, vulnerabilities will always persist because users neglect to use the patches or creative hackers figure out a way to defeat the new security software code. As President George W. Bush once said: "There is no such thing as perfect security."[522]

Technology improvement points:

- Stronger security options in operating systems, more robust and user-friendly anti-virus software, firewalls that are tougher to penetrate, and stronger security configurations for Internet browsers and e-mail utilities.
- Reduction in the number of open virtual ports on a typical computer set-up.
- Faster patches and more innovative patch delivery systems.
- Resolve currently known software and hardware vulnerabilities in operating systems, server software, SCADA systems, and DCS systems.
- Educate and motivate code writers to provide secure code.

2. *Vigilance is critical.*

In the face of more sophisticated and numerous malicious or hostile probes, security awareness must receive greater attention. The Internet and related businesses (routers, servers, computers, et. al.) is 80 percent owned by private companies and individuals.[523] These "owners" so far have successfully resisted government regulation.

We recommend:

- A joint government and private sector assessment of cyber security progress mandated by Congress and overseen by the Department of Homeland Security, every two years, with some authority for oversight of systems related to national security.

3. *Raise consciousness*

As with the effort to bring the "rule of law" to the 19th Century American frontier, gaining acceptance of security procedures at every level of the economy and society will take time. In

[522] President George W. Bush, radio address, July 24, 2004.
[523] <http://www.cybergeogrphy.org/atlas.html>

the last five years, enormous strides have been taken, first to gain an understanding of the interconnections in our digital economy and second to engineer firewalls, patches, enhanced encryption, and other appropriate defenses. It does little good if a software company produces a patch for a security vulnerability if no one downloads it.

- Publicize "best practices" for computer security;[524] these best practices include
  - Operating systems and software should be updated regularly
  - Strong password policies should be enforced
  - All unnecessary services should be disabled
  - Anti-virus software should be installed and kept up to date
  - High fidelity intrusion detection systems and firewalls should be employed[525]
  - Passwords should be changed when employees leave a company or government agency
  - Access to networks should be given out cautiously and with forethought as to the security implications of such access if the network is part of the critical infrastructure system

Further action should be taken after closer examination is undertaken in the following areas:

4. *Indications and Warnings*

More research should be done into the cyber warfare developments of other countries and also terrorist groups. Mounting an effective civil defense traditionally relies on indications and warnings (I & W)[526] which we normally associate with weapons acquisition, movement of people and money, and all the other logistics required for typical combat operations. Traditionally, the more complex the operations, the more prominent the preparations and the greater the opportunity of defenders to detect the signs of impending attacks. What the country studies in this volume have shown is that traditional I &W may not capture the entire picture with respect to cyber attacks. Further investigation into intent of use and other factors is required to gain a more accurate understanding of observable signatures. In this regard, the U.S. scientific community, and particularly private-sector R&D, has historically risen to face challenges to our national security such as lack of functional I & W signatures.[527] We are confident that in the years to come the U.S. scientific community will fulfill that role again.

---

[524] See also: W. David Gardner, "Clarke Touts Broad Approach to IT Security," *TechWeb News*, August 27, 2004 <http://www.informationweek.com/story/showArticle.jhtml;jsessionid=DJ0LKLR4Y2FTYQSNDBCSKHY?articleID=45400035>

[525] Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, September 22, 2001, p.19 <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>

[526] For a discussion on the indications and warnings associated with cyber attacks see: W. A. Campbell, "Traditional Indications and Warnings (TIW) for Host Based Intrusion Detection , indicators, Barriers and Boundaries, Levels of Significance, Security I&W Approach," PRC, Inc., CERT 1999. There is continuing work on the part of the cyber security industry and cyber security engineers to program an early warning system to stem the damage caused by cyber attacks. See: Information Assurance and Advisory Council, "Early Warning & Threat Assessment Methodologies For Information Assurance," March 2001, <http://www.iaac.org.uk/Publications/esrc.htm>

[527] For example see: George Cybenko, Guofei Jiang, and Dennis McGrath, "Infrastructure web: Distributed monitoring and managing critical infrastructures," Institute for Security Technology Studies, Proc. of SPIE

According to the National Research Council, cyber attacks that are sustained over time proceed gradually and incrementally require fewer resources; if such attacks are undetected, the cumulative effects could attain dangerous proportions. This suggests that direct, bold assaults may be less effective than more calibrated, subtle methods of attack. In the long run, a slow, gradual process of reconnaissance and infection will be more insidious because it fails to disturb any of the stakeholders involved.[528] Increased awareness in this possibility and formulation of detection methods would reduce the possibilities of such an attack occurring.

5. A Partnership Between Government and the Private Sector

As outlined in the conclusion to the *National Strategy to Secure Cyberspace*, a partnership between government and the private sector regarding cyber security is critical for several reasons. According to the *National Strategy* "this unique partnership and process was and will continue to be necessary because the majority of the country's cyber resources are controlled by entities outside of government."[529] Anthony Cordesman thoughtfully points out that "there is no practical way that the federal government will ever develop the technical skills, and overcome its lack of specialized competence in ways that enable it to defend the vast majority of physical nodes in America's critical infrastructure or critical e-commerce, computer, and information systems. In fact at least 90% of the burden of day-to-day defense must fall on the private user or corporation."[530] The private sector's profit incentive and the government's lack of technical expertise stands in the way of either one of these organizations "going-it-alone" on the issue of cyber security. A long-lasting and functional partnership between government and the information technology industry, facilitated by the Department of Homeland Security, will help make cyber space more secure.

conference on Enabling Technologies for Law Enforcement and Security, Boston, Nov, 2000. <http://www.ists.dartmouth.edu/lib_published_s.php>

[528] These tactics are discussed at some length in Wayne Michael Hall, *Stray Voltage: War in the Information Age* (2002)

[529] Conclusion, *National Strategy to Secure Cyberspace*, 2003, p. 53

[530] Anthony H. Cordesman, "Homeland Defense: Information Warfare," Center for Strategic and International Studies, December 2000, p. 186

APPENDIX A: MORE CRITICAL VULNERABILITIES

This section examines the main types of cyber warfare targets more carefully. Much of the discussion presented below derives from previous work published by Dartmouth College's Institute for Security Technology Studies.

CORE INTERNET INFRASTRUCTURE

1. Routers

Internet traffic is passes through several routers that are grouped into management domains called "Autonomous Systems," each with its own number. The Autonomous Systems pass routing information to each other using the Border Gateway Protocol (BGP). Routers interconnect logical networks by forwarding information to other networks based upon IP addresses. They ensure that packets get from source to destination.

A study published in 2001 noted that a lack of diversity in router operating systems leaves open the possibility of attacks. A particular weakness involves the Border Gateway Protocol. This protocol, which governs decisions on where to send traffic on the Internet, is vulnerable to information poisoning that could affect routing tables. In a worst case, large volumes of information headed for global destinations would be lost.

2. Domain Name Service (DNS) Servers

Root DNS servers act as a type of telephone directory, matching names of a site into a numerical address. In October 2002, all 13 of the Internet's root DNS servers—three of which lie outside the U.S.—were victims of a distributed denial of service (DDoS) attack. According to media accounts, the attack was an attempt to clog root DNS servers with useless traffic. [531]

Many experts contend that the failure of the October 2002 attack to cause permanent damage is a tribute to the resiliency of the Internet. Most of the information contained in the root servers is cached in redundant and hierarchical fashion across the multiple secondary DNS servers.[532]

[531] "Net's Vulnerability Exposed," *Computerworld,* October 28, 2002. In DDoS attacks, hackers typically break into and take control of thousands of poorly-protected networked computers and exploit these so-called "zombie" machines to send useless data to target servers or networks.

[532] "The Internet Root's Alright, Says ICANN," *VNU Business Publications Newswire*, November 22, 2001. The Bind operating software that runs on the root name servers is not known to have any security related vulnerabilities, according to Lars-Johan Liman, operations manager of a European root server in Sweden.

LOCAL NETWORKS

Background

The past half-decade has witnessed several malicious Distributed Denial of Service (DDoS) virus attacks which—despite the widespread use of defensive firewalls—have either prevented authorized access to a system resource or delayed system operations.[533]

The Melissa Macro Virus demonstrated that attackers can affect one's computer from the Internet even if a fire wall is in place. First observed in March 1999, Melissa was a malicious Trojan that infected over 100,000 hosts in four days. It started with executable software.[534]

The Love Bug virus reportedly crippled millions of computers world wide in 2000 by clogging the e-mail systems of many businesses with unwanted messages. Originating in the Philippines, it first emerged in Asia and "spread to Europe and the United States overnight." According to press reports, the virus not only destroyed data on infected machines but attempted to activate another program from a Philippine website that stole passwords from victims' computers.[535]

In June 2001, a computer security company identified a vulnerability in a web server program that could lead to a buffer overflow exploit. In July 2001 the Code Red Worm was released, targeting the White House. It has been estimated that over 200,000 computers participated in the attack.

Code Red worms search for systems running Microsoft Internet Information Server (IIS) that have not patched the unchecked buffer vulnerability in idq.dll or removed the ISAPI script mappings. The worm exploited the vulnerability to inject itself.

Although these exploits proved to be annoyances, albeit costly ones, they did not cause irreparable systemic damage or adversely affect U.S. national security. Attacking unencrypted U.S. defense networks (DoD logistics, for example), on the other hand, could compromise significant military logistics operations or force costly reconfigurations or "work arounds" with potential security implications.[536]

The foregoing examples demonstrate that firewalls are insufficient protection and are often thwarted by the actions of internal users (who unwittingly allow malicious code to enter a system

[533] The terms virus and worm are often used interchangeably to describe malicious computer programs. A virus is software malicious logic that propagates by infecting another program. A virus cannot propagate by itself; it requires that its host program be run to make the virus active. A worm is a computer program that can run independently and can propagate a complete version of itself onto other hosts on a network.

[534] The virus was activated by users opening a Microsoft Word document. The virus replicated by locating Microsoft Outlook address books and sending itself to the first 50 entries in each book. *SANS Security Essentials*, SANS.org, 2002, p. 313 and p. 496

[535] "Love Bug Virus Evidence Reportedly Pointing to Manila Suspect," DPA, May 7, 2000

[536] In 1997, according to prosecutors, two Swedes hacked into the NASA computer system. Allegedly, the two individuals planted viruses and made changes in various databases that caused multi-million dollar damages. See "Swedish Men Charged with NASA Hacking," *Nordic Business Report*, August 23, 1999

or network) In addition, attackers often use scanners to search for open shares and services on a system; such scanners often use packet crafting and source address spoofing to circumvent firewalls.

Worms Coupled with a Denial of Service Payload

The SQL Slammer worm, which first appeared in January 2003, exploited a vulnerability in the Resolution Service of SQL Server 2000 and Microsoft Desktop Engine 2000. The vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow. The worm is a self-propagating code, i.e., if a packet is sent to a vulnerable machine the victim machine will become infected and also begin to scan for new hosts.[537]

A recent research paper by a South African computer security firm described in detail a hypothetical attack combining malicious computer code joined with a destructive payload. The essence of the scenario is that a publicly available search engine, a few selected e-mail addresses, and an off the shelf computer code could cripple an entire internal network.[538] This scenario was adumbrated in a 2001 analysis that pointed out that a worm similar to Code Red "could do much more serious damage with only minor design modifications [to include a destructive payload]…If maximum destruction is a hostile adversary's goal, worms are a cost effective way to significantly disrupt the Unites States' national information infrastructure." [539]

Creating a worm to target a specific country[540]

SensePost, a South African computer security firm, has identified several vulnerabilities to a potential worm that permitted a full host compromise. Among the vulnerabilities are:

Microsoft IIS (5) Unicode/ 2x decode
Microsoft IIS (4) MSADC
Microsoft IIS (5) printer extensions
Microsoft IIS (5) WebDAV
Microsoft SQL with blank SA configured
Blank local administrator passwords on Microsoft Windows hosts.

According to SensePost, a worm based on the above-mentioned vulnerabilities, combined with a Denial of Service payload, could completely disable a large internal network.

In delivering the payload, the key is to find e-mail addresses to target. The author wrote scripts that use Google to search for public references to e-mail addresses on the WWW. The scripts allow the author to search for e-mails from a given country and, in particular, seek individuals

[537] CERT Advisory CA-2003-04 MS-SQL Server Worm, January 27, 2003 <http://www.cert.org/advisories/CA-2003-04.html>
[538] See "How an e-mail virus could cripple a nation," CNET/ZDNet Reviews, August 11, 2003.
[539] Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, September 22, 2001, p. 16 <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>
[540] Source: Derived from "Putting the Tea Back into Cyber Terrorism," SensePost Research, BlackHat Briefings, Las Vegas, July 2003

employed by telecommunications and financial firms, energy utilities, government departments, armed services, or hospitals in that country.

According to the SensePost document, running the scripts demonstrates that there are many e-mail addresses available, especially on bulletin boards. If a malicious user could infect one government node with a worm (even the desktop computer of a low ranking official), he could infect the government system as well.

PHYSICAL INFRASTRUCTURE ATTACKS: THE VULNERABILITIES OF SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS (SCADA)

"Process control" information systems associated with critical infrastructures (such as banking, electricity, water, oil and gas) are considered likely targets for cyber attackers. Supervisory Control and Data Acquisition systems rely on embedded "process control" programs. Individual SCADA systems may be unique, but the knowledge associated with Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) are accessible to most computer programmers.

Over the past decade, an evolution in data communications and process control has introduced potential systemic vulnerabilities. The data connections from DCS and PLC systems to the plant network are vital to production, yet can be an invitation to compromise if "problems on the business network can be passed on to the process network" through a utility's Ethernet and TCP/IP networking.[541]

According to some experts, hackers are learning about PLC's and DCS's. Recently, an individual hacked into a PLC in a semiconductor manufacturing plant, shutting down a reverse osmosis system. Reportedly, several brands of controllers can be compromised by tools in the "average teenage script kiddy tool kit."[542]

SCADA Systems

Supervisory control and data acquisition (SCADA) programs are used in control of administrative systems from nuclear power plants to traffic control systems to gas pipelines. What is most troubling about SCADA is its user-friendliness and its potency in total control of most applications. While most SCADA operators are probably not trained IT professionals, the ease of use and the GUI interfaces that SCADA employs make it extremely easy to access and to use. The main exploits of SCADA systems will come from worms and viruses that make their way into the system and Trojan horses which offer remote access to SCADA servers. Another

[541] Eric Byres, "Protect that Network: Designing Secure Networks for Industrial Control," <http://extranet.arcweb.com/cybersecurity//Shared%20Documents/IEEE%2099%20-%20Process%20LAN%20Protection.pdf>

[542] Eric Byres, "The Myth of Obscurity," *InTech*, September 1, 2002 <http://public.arcweb.com/cybersecurity/Shared%20Documents/Intech%20Sep02%20-%20Myth%20of%20Security.pdf>

exploit comes from a terrorist-hacker being physically at the terminal, versed in the operation of the SCADA system from using online user manuals.[543] The plethora of information about SCADA packages includes free .pdf documentation of user interfaces, user logon creations, alarm systems, etc as well as online tutorials, paid training sessions at the company sites, and other methods of learning the ins-and-outs of SCADA software and hardware packages.

[543] A quick search of the Internet revealed online user manuals for: Nortech Industries, SCADA system for GSM telephones, <http://www.nortechonline.co.uk/documents/PD4%20USER%20MANUAL.pdf>, D-Log Phoenix Electrical Systems, SCADA for electrical and sewage systems, <http://www.phoenix-electrical.co.uk/DLOG%20User%20Manual.htm>, Telemetric.net, SCADA for oil and gas transport or management of electrical systems <http://www.telemetric.net/info/documentation.htm>, DRMCC, SCADA for oil and gas power plants, <http://www.dynamicratings.com/pdf/drmcct2_download/T2-002T2UserManual.pdf>, Data Flow Systems, Hyper SCADA System package, <http://www.scadaserver.com/index.html>

APPENDIX B: TERMINOLOGY ISSUES

"Cyber" refers to the virtual world in which attacks take place, although the wall between the virtual world and the so-called real world is rapidly crumbling. Actions in the virtual world (sending e-mail, electronic commerce in the retail or in business-to-business, and electronic controls and software that control physical devices such as train switches, air-traffic control devices, and waterway regulation) have physical impacts on the real world. The "warfare" part of the term is derived from the various characteristics of cyber warfare that resemble conventional warfare. War is usually defined as the organized use of violent force by groups to forward a political goal. This academically sanitized definition is sometimes qualified by the requirements that combat and actual deaths need be involved to define some phenomenon as warfare, but here the term warfare is used as an illustrative analogy. Cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations.

Figure 1: Differences in terminology

National security experts, military analysts, academia, and terrorism researchers have each come up with terms describing the cyber attack phenomena. Depending upon the stated mission or the scope of each group, the terms serve to clarify the exact nature of the phenomena they are attempting to describe. Although in the short term these terms clarify, the plethora of terminology used to identify essentially the same phenomenon serves only to confuse the reader. The primary differences lie in the kinds of actions and kinds of actors that are at the heart of each specific definition.

The term *information operations* is preferred by national security and military experts to describe the strategies employed in the military arena in order to defeat the enemy using electronic and other high-tech means. It is also meant to be the term used during times of peace. Not all of the actions within information operations would be considered cyber warfare. According to the operational definition of information operations that is used by the Joint Chiefs of Staff, information operations encompasses all of the "actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO."[544] Here the primary nuance, information operations, as well as information warfare, is focused on the control of information (interpretation of observed phenomena) and the ability to disrupt its acquisition and dissemination. Information operations also encompasses the capturing of signals intelligence and deployment of planes carrying leaflets in an attempt to influence an adversary using propaganda, known as psychological operations.

The term *information warfare* is preferred in the military as well as in the academic study of the implications of the innovations in the Information Age upon warfare. Information warfare is "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems."[545] Information warfare seeks to deny the enemy the acquisition of information and improve upon one's own information resources. As can be expected, the usage of this term by military experts is during wartime. Military experts also use the term information warfare specifically with respect to the military's attempt to lift the fog of war by integrating units with a wireless network in order to

[544] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, October 9, 1998 <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>

[545] Information warfare, when it appears in quotations and in referenced studies and publications in this study is defined as: "Those actions intended to protect , exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary." John Alger, National Defense University, cited by Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p. 10

maintain better battlefield control and sight.[546] Information warfare largely stays in the cyber realm, where data is electronic and can be accessed remotely, but information warfare can expand beyond bits and bytes. The Department of Defense's definition of information warfare is "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."[547]

Cyber terrorism, the subject of Dan Verton's recent book, *Black Ice*, is nearly identical a phenomena to cyber warfare. According to Professor Dorothy Denning, "cyberterrorism refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide."[548] The primary difference between cyber terrorism and cyber warfare lies in the condition of the actor, whether or not the actor is state, non-state, or sub-state.

There are two roots to the confusion involving the usage of the term information warfare and other similarly vague terms. During the early-1990's, military analysts and general staffs around the world recognized that warfare was changing due primarily to the integration of computing capability into conventional warfare. This is warfare in the Information Age, or high-tech warfare.[549] These innovations in and of themselves do not constitute cyber warfare,

[546] Gunilla Ivefors, MDA Group, Linköping University, "Information Warfare," 1996 <http://www.ida.liu.se/~guniv/Infowar/> and Daintry Duffy, "Information is a Weapon," *DarwinMag*, November 2001, <http://www.darwinmag.com/read/110101/weapon_content.html>

[547] Department of Defense, "Appendix A: Missions and Activities," Special Operations Force Posture, 2000 <http://www.defenselink.mil/pubs/sof/a.pdf>

[548] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Georgetown University, December 10, 1999 <http://www.nautilus.org/info-policy/workshop/papers/denning.html> and Dorothy E. Denning, "Is Cyber Terror Next?," November 1, 2001 <http://www.ssrc.org/sept11/essays/denning.htm>

[549] The usage of precision-guided bombs, night vision devices, and the ability of commanders to view battles in real-time from a rear-area (command), the employment of systems such as Force XXI Battle Command, Brigade and Below (FBCB2) along with the global positioning system (GPS), the on-demand supply-system (control and coordination) and the ability for even the infantry rifleman at incredible distances to speak directly with a commanding officer (communications) are several examples of the revolutions that have taken place as a result of militaries adopting the innovations of the Information Age. See Close Combat Tactical Trainer, "Learn About FBCB2 in CCTT," <http://www.peostri.army.mil/PM-CATT/CCTT/CITT/io/ie/io_10.htm>. For more discussion of military use of network technologies see Timothy Lenoir, Chart 1: Large DOD development Programs in Modeling and Simulation, "Programming Theaters of War" in Robert Latham, *Bombs and Bandwidth*, (New York, New Press, 2003) pp. 182-183. Some experts have argued that there a revolution in military affairs has not occurred due to the integration of information technologies with the projection of military power. The reality may be that the speed of current technological innovation has caused a fundamental change in the time it takes to achieve a revolution in military affairs, and that not one single technological innovation has defined the evolution in warfare that has taken place in the past two decades. See Chris Hables Gray, "Perpetual Revolution in Military Affairs, International Security, and Information," in Robert Latham, *Bombs and Bandwidth*, (New York, New Press, 2003) pp. 199-212

however the disruption of such capabilities would be considered cyber warfare.[550] The second root of confusion regards the idea of knowledge as a biased and manipulable resource; a post-modernist view of the epistemological consequences of data integrity in the Information Age. Control of information in times of warfare, masterfully thought-out and espoused by the Chinese philosopher Sun Tzu shapes the missions of the modern intelligence community. Information control and control of media access, the main mission of psychological operations, are also integrated in the information warfare term.

[550] For example, the U.S. Army's Future Combat System (FCS) Land Warrior concept turns the infantry rifleman into a self-contained and self-sustaining fighting unit. The FCS Land Warrior system envisions self-monitoring health-systems for soldiers, which in turn are connected to medical systems monitored by combat medics and lifesavers. The FCS Land Warrior system integrates the soldier into the overall intelligence system, pipelining information to the soldier as well as giving the soldier the ability to send real-time information to other soldiers and to intelligence personnel. Another example would be the global positioning system's integration into military activities. As quickly as the capabilities and battlefield improvements conferred by GPS technologies was adopted by the U.S. military, it is not hard to imagine how vital systems considered high-tech today may become an application considered standard in the future. The disruption of GPS technology would put today's military's at a severe disadvantage: this disruption is an example of cyber warfare.
See Program Executive Office Soldier, "Land Warrior Interactive," 2004, <https://peosoldier.army.mil/default.asp?section=multi>