Center for Strategic & International Studies
Washington, DC

Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:

James A. Lewis
Center for Strategic and International Studies
December 2002

Cyber-warfare conjures up images of information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations. This a frightening scenario, but how likely is it to occur? What would the effects of a cyber attack be on a potential opponent?

Cyber attacks, network security and information pose complex problems that reach into new areas for national security and public policy. This paper looks at one set of issues – those related to cyber-terrorism and cyber attacks on critical infrastructure and their implications for national security. Cyber-terrorism is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." The premise of cyber terrorism is that as nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created – "a massive electronic Achilles' heel." A hostile nation or group could exploit these vulnerabilities to penetrate a poorly secured computer network and disrupt or even shut down critical functions.

Much of the literature on cyber-terrorism assumes that the vulnerability of computer networks and the vulnerability of critical infrastructures are the same, and that these vulnerabilities put national security at a significant risk. Given the newness of computer network technology and the rapidity with which it spread into economic activity, these assumptions are not surprising. A closer look at the relationships between computer networks and critical infrastructures, their vulnerability to attack, and the effect on national security, suggests that the assumption of vulnerability is wrong. A full reassessment is outside the scope of this paper, but a brief review suggests that while many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable.

A reassessment of the cyber threat has four elements. First, we need to put cyber-warfare and cyber-terrorism in the historical context of attacks against infrastructure. Strategies that emphasize attacks on critical civil infrastructures have discussed for more than eighty years. Second, we need to examine cyber attacks against a backdrop of routine infrastructure failures. There is extensive data on power outages, flight delays and communications disruptions that occur normally and the consequences of these routine failures can be used to gage the effect cyber-warfare and cyber-terrorism. Third, we need to measure the dependence of infrastructure on computer networks and the redundancy

already present in these systems. Finally, for the case of cyber-terrorism, we must consider the use of cyber-weapons in the context of the political goals and motivations of terrorists, and whether cyber-weapons are likely to achieve these goals.

A preliminary review of these factors suggests that computer network vulnerabilities are an increasingly serious business problem but that their threat to national security is overstated. Modern industrial societies are more robust than they appear at first glance. Critical infrastructures, especially in large market economies, are more distributed, diverse, redundant and self-healing than a cursory assessment may suggest, rendering them less vulnerable to attack. In all cases, cyber attacks are less effective and less disruptive than physical attacks. Their only advantage is that they are cheaper and easier to carry out than a physical attack.

Infrastructure as Target

Cyber-terrorism is not the first time a new technology has been seized upon as creating a strategic vulnerability. While the match between theories of cyber-warfare and air power is not precise, a comparison of the two is useful. In reaction to the First World War, European strategists like Douhet and Trenchard argued that aerial bombing attacks against critical infrastructure well behind the front lines would disrupt and cripple an enemies' capacity to wage war. Their theories were put to the test by the U.S. Army and Royal Air Forces during World War II in strategic bombing campaigns aimed at destroying electrical power, transportation and manufacturing facilities. Much of the first tranche of literature on cyber attacks resembles in many ways (and owes an unspoken debt to) the early literature on strategic bombing.

A key document for understanding how attacks on infrastructure affect societies is the Strategic Bombing Survey conducted by the United State during and after World War II. During the war, Britain and America launched thousands of heavy bombers that dropped millions of tons of high explosives on Germany, seeking to cripple its infrastructure, destroy its industrial base and break the will of the population to continue the war. Early theorists of air warfare had predicted that such an onslaught would paralyze or cripple the target. What the survey found, however, is that industrial societies are impressively resilient. Industrial production actually increased for two years under the bombing and it was not until ground forces occupied Germany that resistance ceased:

> As the air offensive gained in tempo, the Germans were unable to prevent the decline and eventual collapse of their economy. Nevertheless, the recuperative and defensive powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations. Germany resorted to almost every means an ingenious people could devise to avoid the attacks upon her economy and to minimize their effects….
>
> The mental reaction of the German people to air attack is significant. Under ruthless Nazi control, they showed surprising resistance to the terror and

> hardships of repeated air attack, to the destruction of their homes and belongings, and to the conditions under which they were reduced to live. Their morale, their belief in ultimate victory or satisfactory compromise, and their confidence in their leaders declined, but they continued to work efficiently as long as the physical means of production remained….[1]

The U.S. found similar results from aerial bombardment during the Vietnam War. Counter-intuitively, the effect of aerial attack was often to harden and increase popular support for continued resistance. The advent of nuclear weapons (and perhaps large precision-guided munitions) gave air power the ability to disrupt civil infrastructures needed to achieve the visions of Douhet, Trenchard or Mitchell, but cyber attacks do not pose the same level of lethality.

One of the Strategic Bombing Survey's conclusions was that "The German experience showed that, whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary." However, cyber attacks are likely to be single attacks. Once a hacker has gained access and the damage done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line. Cyber attackers would continually need to exploit new vulnerabilities and new tactics to ensure sustained disruption. Cyber attacks also seldom if ever produce physical damage that requires time-consuming repairs.

'Routine' Failure versus Cyber Attack

Critical infrastructure protection creates a new set of problems for national security. Different actors are involved. The focus is on civilian and commercial systems and services. Military force is less important. The scope of these new problems depends on how we define national security and how we set thresholds for acceptable damage. From a legal or public safety perspective, no country will accept even a single attack on infrastructure or interruption of services. If the goal is to prevent cyber-attacks from costing a single day of electric power or water service, we have set a very high standard for security. However, from a strategic military perspective, attacks that do not degrade national capabilities are not significant. From this perspective, if a cyber-attack does not cause damage that rises above the threshold of the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security.

It is particularly important to consider that in the larger context of economic activity, water system failures, power outages, air traffic disruptions and other cyber-terror scenarios are routine events that do not affect national security. On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine occurrence at the system or regional level, with service denied to customers for hours or days. Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect. For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers, terrorist groups or nation states

(particularly for nation states, where the risk of discovery of what would be universally seen as an act of war far outweigh the limited advantages gained from cyber attacks on infrastructure).

Weapons of Mass Annoyance

A detailed examination of some of the scenarios for attacks on critical infrastructures helps place cyber-attacks more accurately in a strategic or national security context. For example, dams used for water storage and for power generation are often cited as a likely target for cyber attack. The Washington Post recently wrote that unnamed "U.S. analysts" believe that "by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and property."[2]

In the United States, the water supply infrastructure would be an elusive target for cyber attack. There are 54,064 separate water systems in the U.S. Of these, 3,769 water systems serve eighty one percent of the population and 353 systems served forty-four percent of the population. However, the uneven spread of diverse network technologies complicates the terrorists' task. Many of these water supply systems in the U.S., even in large cities, continue to rely on technologies not easily disrupted by network attacks. There have been cases in the U.S. when a community's water supply has been knocked out for days at a time (usually as a result of flooding), but these have produced neither terror nor paralysis. A cyber terrorist or cyber warrior would need to carry out a sustained attack that would simultaneously disrupt several hundred of these systems to gain any strategic benefit.

Assuming that a terrorist could find a vulnerability in a water supply system that would allow him to shut down one city's water for a brief period, this vulnerability could be exploited to increase the damage of a physical attack (by denying fire fighters access to water). In general, a cyber attack that alone might pass unnoticed in the normal clutter of daily life could have useful multiplier effects if undertaken simultaneously with a physical attack. This sort of simultaneous combination of physical and cyber attacks might be the only way in which cyber weapons could be attractive to terrorists. The American Waterworks Association assessment of the terrorist threat to water supplies placed "physical destruction of the system's components to disrupt the supply of water" as the most likely source of infrastructure attack.[3]

Comparing aerial and cyber attacks on hydroelectric dams helps provide a measure for cyber-threats. Early in World War II, the Royal Air Force mounted a daring attack on dams in the Ruhr, a chief source of electrical power for German industry. The raid was a success, the dams breached by bombs and, for a period of time, the electrical supply in the region was disrupted.[4] A comparable cyber attack occurred when a young hacker reportedly gained access to the computer controls for a dam in the U.S. Southwest, but did not disrupt service or cause physical damage.[5] In neither attack was the damage or the reduction in electrical power paralyzing. Of the two, the cyber attack was less

effective in that it caused no physical damage and could be classed more as an annoyance than a threat. The aerial attack resulted in physical damage that needed to be repaired. The only advantage of a cyber attack is that it is less expensive - a teen-ager and a desktop computer rather than valuable aircrews and expensive aircraft.

Many analyses have cyber-terrorists shutting down the electrical power system. One of the better cyber security surveys found that power companies are a primary target for cyber attacks and that seventy percent of these companies had "suffered a severe attack" in the first six months of 2002.[6] The U.S. electrical power grid is a desirable target, but it is a network of multiple, redundant systems that are used to routine system failure and disruption. The national electrical grid is a highly interconnected system of over 3,000 public and private utilities and cooperatives. These 3,000 electrical power providers use a variety of different information technologies to operate their controls for power generation and transmission. A hacker or even a large group of hackers would need to find vulnerabilities in multiple systems to significantly disrupt the power supply and even then, an attack might only disrupt service for a few hours.

The North American Electric Reliability Council, an industry group formed after the 1965 New York blackout, has been working with the Federal government since the 1980s to improve the security of the electrical system and to develop rapid responses to large outages. In Congressional testimony, NERC officials have said that in the last few years, neither viruses nor Distributed Denial of Service attacks against the U.S. electrical system have interrupted service.[7] While industry sources can paint an over-optimistic picture at times, it remains true that falling trees have caused many electric system disruptions while cyber attacks have caused none. A risk assessment by the Information Assurance Task Force of the National Security Telecommunications Advisory Committee concluded "Physical destruction is still the greatest threat facing the electric power infrastructure. Compared to this, electronic intrusion represents an emerging, but still relatively minor, threat."[8]

The U.S. has already run a large-scale experiment on the effects of disrupting electrical power supplies, thanks to California's experience with 'deregulation' last year. California's efforts to de-regulate the electrical power market resulted in months of blackouts and rolling brownouts across the state. Deregulation was a more powerful 'attack' on the electrical infrastructure than anything a cyber-terrorist could mount. There was clearly economic cost to the California regulatory event, but it was not crippling nor did it strike terror into the hearts of Americans. Similarly, power outages across the country in 1999 affected millions of people and cost electrical power customers millions of dollars in lost business and productivity. These outages were the result of increased electricity use prompted by sustained high summer temperatures. In contrast to California's State government or hot weather, the number of blackouts in U.S. caused by hackers or cyber-terrorists remains zero.

Interference with national air traffic systems to disrupt flights, shut down air transport and endanger passenger and crews is another frequently cited cyber-threat.[9] We are not yet at a stage where computer networks operate aircraft remotely, so it is not possible for

a cyber-attacker to take over an aircraft. Aircraft still carry pilots who are trained to operate the plane in an emergency. Similarly, the Federal Aviation Authority does not depend solely on computer networks to manage air traffic, nor are its communications dependent on the Internet. The high level of human involvement in the control and decision making process for air traffic reduces the risk of any cyber attack. In a normal month storms, electrical failures and programming glitches all ensure a consistently high level of disruption in air traffic. Pilots and air traffic controllers are accustomed to unexpected disruptions and have adapted their practices to minimize the effect. Airlines and travelers are also accustomed to and expect a high degree of disruption in the system. In the United States, it is normal for 15,000 to 20,000 flights to be delayed or cancelled every month. A cyber attack that degraded the air traffic system would create delays and annoyance, but it would not pose a risk to national security.

The FAA has 90 major computer systems and nine different communications networks. These networks rely on elderly equipment and use proprietary software that make them difficult for outsiders to hack. This may explain why the few reported attacks have not affected air traffic. In one reported incident, a young hacker interrupting local phone service in a New England, cutting off a regional airport's control tower and the ability to turn on runway lights. Although the interruption lasted six hours, there were no accidents at the airport. In other cases, FAA headquarters computer networks have been penetrated, allowing hackers to make public unpublished information on airport passenger screening activities, and in another case, a hacker was able to enter an FAA mail server. None of these cases resulted in any disruption to flight.[10] Ironically, modernization could actually increase FAA vulnerability if greater attention is not given to security.

A recent attack on the Internet illustrates the nature of vulnerabilities from cyber attack. For a one-hour period in October 2002, unknown parties launched a Distributed Denial of Service attack on the thirteen 'root servers' that form the basis of the domain names system that governs Internet addresses. Eight of the thirteen servers were force off-line because of the attacks. The attack itself was invisible and without effect on Internet users. The attack on the DNS system did not noticeably degrade Internet performance. Most DNS data needed for the daily operation o f the Internet is stored locally and updated daily. Very few requests require assistance from the root servers. Additionally, the presence of thirteen servers (of which five were not affected by the attack) gives a degree of redundancy that suggests that if there are vulnerabilities to the Internet, the DNS servers are not one of them. In contrast to the DNS attack, shortly after it occurred thousands of Internet customers in the western United States experienced serious delays when their service provider had routing problems due to programming errors. Unlike the attack, this DNS failure actually disrupted service, but it had no effect on national security.

While the Internet may have a few points of failure that offer the possibility for system-wide disruption, it was designed to be a robust, distributed communications network capable of continuing operations after a strategic nuclear exchange. Packet switching and Internet protocols were developed to allow communications to be maintained even when

some nodes in the network were eliminated and the Internet itself was designed to automatically route around damage to allow for continued communications. Additionally, computer networks rely on a backbone of high capacity telecommunications systems that are relatively secure from cyber-attack. The introduction of new communications technologies also enhances survivability. Wireless and satellite communications also provide some redundancy for landline systems. Most industrial countries now have access to three or four different modes of communications, making the system considerably more robust than it was a decade ago. Increased use of ultra wideband and mesh radio networks will also increase redundancy and survivability against cyber attack in communications networks.

The 911 emergency response system, a specialized communications network that relies on local telephone service, is also a favorite target for theorists of cyber-terrorism, but like other infrastructures, it is a robust target. The U.S. for example, does not use a single 911 system in but instead has several thousand local systems using different technologies and procedures. No 911 system in a major city has been hacked. It might be possible to send a flood of email messages instructing people to call 911 for important information and thus overload the system (this was the technique used in the 1997 U.S. cyber exercise "Eligible Receiver"). This sort of technique usually works only once - but made in conjunction with a bombing or other physical attack they could act as a 'force multiplier' for a terrorist event.

Manufacturing and economic activity are increasingly dependent on computer networks, and cyber crime and industrial espionage are new dangers for economic activity. However, the evidence is mixed as to the vulnerability of manufacturing to cyber attack. A virus in 2000 infected 1,000 computers at Ford Motor Company. Ford received 140,000 contaminated e-mail messages in three hours before it shut down its network. E-mail service was disrupted for almost a week within the company. Yet, Ford reported, "the rogue program appears to have caused only limited permanent damage. None of its 114 factories stopped, according to the automaker. Computerized engineering blueprints and other technical data were unaffected. Ford was still able to post information for dealers and auto parts suppliers on Web sites that it uses for that purpose."[11] Companies now report that the defensive measures they have taken meant that viruses that were exceptionally damaging when they first appeared are now only "nuisances."[12]

Cyber attacks are often presented as a threat to military forces and the Internet has major implications for espionage and warfare. Information warfare covers a range of activities of which cyber attacks may be the least important. While information operations and information superiority have become critical elements in successful military operations, no nation has placed its military forces in a position where they are dependent on computer networks that are vulnerable to outside attack. This greatly limits the effectiveness of cyber weapons (code sent over computer networks). The many reports of military computer networks being hacked usually do not explain whether these networks are used for critical military functions. It is indicative, however, that despite regular reports of tens of thousands of network attacks every year on the Department of Defense, there has been no degradation of U.S. military capabilities.

For example, while there were many attack against U.S. military computer networks during operations in Kosovo, these attacks did not result in sorties being cancelled or in a single casualty. Similarly, a foreign power that used cyber-weapons to try to prevent a carrier battle group from leaving the U.S. would be unlikely to succeed. A recent attack by a British hacker neither compromised classified information nor disrupted military operations. A Rand study conducted for the U.S. Air Force on military operations and information vulnerabilities noted "while most of the current topical interests has focused on the newer, trendier threats to information systems, particularly computer hacking and associated disruption and manipulation…our analysis showed that some of the "old-fashioned" threats pose a greater danger…."[13]

Hacking and Terror

Much of the early work on the 'cyber threat' depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other's websites. No critical infrastructures have been shut down by cyber attacks.

Terrorists seek to make a political statement and to inflict psychological and physical damage on their targets. If terrorism is an act of violence to achieve political objects, how useful will terrorists find an economic weapon whose effects are gradual and cumulative? One of Al Qaeda's training manuals, "Military Studies in the Jihad Against the Tyrants" notes that explosives are the preferred weapon of terrorist because "explosives strike the enemy with sheer terror and fright." Explosions are dramatic, strike fear into the hearts of opponents and do lasting damage. Cyber attacks would not have the same dramatic and political effect that terrorists seek. A cyber attack, which might not even be noticed by its victims, or attributed to routine delays or outages, will not be their preferred weapon. If terrorism is an act of violence to create shock and achieve political objects, how useful will terrorists find an economic tool whose effects are at best gradual and cumulative?

An analysis of the risk of cyber terrorism is also complicated by the tendency to initially attribute cyber events to military or terrorist efforts when their actual source is civilian recreational hackers. When DOD computer networks were penetrated in an attack that occurred in the late 1990s, the U.S. was quick to suspect potential opponents, particularly Iraq or China, as the culprit. U.S. officials debated the merits of an active defense and whether this was an act of war, justifying a counter-attack. As tension mounted, the U.S. discovered that far from being a hostile power, the source of the attack was two high school students in southern California. It is difficult, especially in the early stages of an

incident, to determine if the attacker is a, terrorist, group, foreign state, criminals, or a teenager in California. However, a quick survey of incidents over the last four years suggests that criminals and bored teenagers are the most likely sources of attack. To this day, the vast majority of hacking incidents result from the actions of recreational hackers.

While the press has reported that government officials are concerned over Al Qaeda plans to use the Internet to wage cyber-terrorism, these stories often recycle the same hypothetical scenarios previously attributed to foreign governments' cyber-warfare efforts. The risk remains hypothetical but the antagonist has changed from hostile states to groups like Al Qaeda. The only new element attributed to Al Qaeda is that the group might use cyber attacks to disrupt emergency services in order to reinforce and multiply the effect of a physical attack. If cyber-attacks were feasible, the greatest risk they might pose to national security is as corollaries to more traditional modes of attacks.

Espionage opportunities created by a greater reliance on internet-accessible computer networks will create greater risk for national security than cyber attacks. Terrorist groups are likely to use the Internet to collect information on potential targets, and intelligence services can not only benefit from information openly available on the web but,[14] more importantly, can benefit from the ability to clandestinely penetrate computer networks and collect information that is not publicly available. This is very different from hacking, in that in the event of a successful penetration of a hostile network, a terrorist group or an intelligence service will want to be as unobtrusive as possible. A sophisticated opponent might hack into a system and sit there, collecting intelligence and working to remain unnoticed. It will not disrupt essential services or leave embarrassing messages on websites, but remain quietly in the background collecting information. Collection techniques for the Internet differ significantly from earlier signals and communications intercept techniques, and while different kinds of data will be collected, the overall effect may be to make some espionage activities much more rewarding. This topic, the implications for espionage of the greater use of computer networks and Internet protocols, deserves further study.

Cyber Crime and the Economy

Cyber attacks do pose a very real risk in their potential for crime and for imposing economic costs far out of proportion to the price of launching the attack. Hurricane Andrew, the most expensive natural disaster in U.S. history, caused $25 billion dollars in damage and the average annual cost from tornadoes, hurricanes, and flood damage in the U.S. is estimated to be $11 billion. In contrast, the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. Putting aside for the moment the question of how the estimates of the Love Bug's cost were calculated (these figures are probably over-estimates), the ability of a single university student in the Philippines to produce this level of damage using inexpensive equipment shows the potential risk from cyber crime to the global economy.[15]

The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third party

liability. Opportunity cost (lost sales, lower productivity, etc) make up a large proportion of the reported cost of cyber attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. For example, if a Distributed Denial of Service attack prevents customers from reaching one online bookseller, they may instead go to another to purchase their books. The aggregate national sale of books could remain the same although the first bookseller's market share would decline. A small number of customers may choose not to bother going to another site if their first choice is unavailable, but some of these lost sales may well be recouped by later return to the sight by the customer. Businesses face greater damage from financial fraud and theft of intellectual property over the Internet, crimes that continue to grow in number.[16]

Emphasizing the transnational nature of cyber security issues, the last few years have seen the emergence of highly sophisticated criminal gangs capable of exploiting vulnerabilities in business networks. Their aim is not terror, but fraud or the collection of economically valuable information. Theft of proprietary information remains the source of the most serious losses, according to surveys of large corporations and computer crime.[17] These crimes must be differentiated from the denial of service attacks and the launching of viruses. Denial of services or viruses, while potentially damaging to business operations, do not pose the same level of risk.

Cyber crime is a serious and growing threat, but the risk to a nation-state in deploying cyber-weapons against a potential opponent's economy are probably too great for any country to contemplate these measures. For example, writers in some of China's military journals speculated that cyber attacks could disable American financial markets. The dilemma for this kind of attack is that China is as dependent on the same financial markets as the United States, and could suffer even more from disruption. With other critical infrastructures, the amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery for a nation state could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda. Cyber attacks could potentially be a useful tool (albeit not a fatal or determinative tool) for non-state actors who reject the global market economy.

Conclusion

The Internet is a new thing, and new things can appear more frightening than they really are. Much of the early analysis of cyber-threats and cyber security appears to have "The Sky is Falling" as its theme. The sky is not falling, and cyber weapons seem to be of limited value in attacking national power or intimidating citizens. The examples presented in this paper suggest that nations are more robust and resilient than the early theories of cyber terror assumed. To understand the vulnerability of critical infrastructures to cyber attack, we would need for each target infrastructure a much more detailed assessment of redundancy, normal rates of failure and response, the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. This initial assessment suggests that infrastructures in large industrial countries are resistant to cyber attack.[18]

Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber-terrorism and cyber-warfare give them credit for, and cyber attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring service than early analysts realized. Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cyber crime may be not be fully appreciated by many observers.

This is not a static situation, and the vulnerability of critical infrastructure to cyber attack could change if three things occur. Vulnerability could increase as societies move to a ubiquitous computing environment[19] when more daily activities have become automated and rely on remote computer networks. The second is that vulnerability could increase as more industrial and infrastructure applications, especially those used for SCADA (Supervisory Control and Data Acquisition), move from relying on dedicated, proprietary networks to using the Internet and Internet protocols for their operations. This move to greater reliance on networks seems guaranteed given the cost advantage of Internet communications protocols (Transmission Control Protocol/Internet Protocol), but it also creates new avenues of access. These changes will lead to increased vulnerabilities if countries do not balance the move to become more networked and more dependent on Internet protocols with efforts to improve network security, make law enforcement more effective, and ensure that critical infrastructures are robust and resilient.

From a broader security perspective, nations now face a range of amorphous threats to their safety that are difficult for the traditional tools of national security to reach. The lines between domestic and foreign, private and public, or police and military are blurring, and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.

Notes

[1] U.S. Strategic Bombing Survey, Summary Report (European War), 1945. http://www.anesi.com/ussbs02.htm

[2] Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002

[3] DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5, pp. 78–85, http://www.awwa.org/Communications/journal/Archives/J501es3.htm, see also Scott Berinato, "Debunking the Threat to Water Utilities," CIO Magazine, March 15, 2002, http://www.cio.com/archive/031502/truth_sidebar2.html

[4] The Germans quickly repaired the damage and production in the Ruhr actually increased after the attack. There were a number of civilian casualties, but most of these were Soviet prisoners of war who were trapped in their prison camp and unable to escape the initial flood. Cyber attacks that open floodgates would not produce the same surge of water as an explosive breach.

[5] Lemos, Robert, "Cyber Terrorism, the Real Risks," ZDNet News UK, August 27, 2002, http://news.zdnet.co.uk/story/0,,t269-s2121358,00.html

[6] Riptech Internet Security Threat Report, July 2002, http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf
[7] Testimony of Michehl R. Gent Before the Senate Government Affairs Committee, May 8, 2002, ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/mrg-testimony-SenateGovernmentalAffairs-5-08-02-(final).pdf
[8] Information Assurance Task Force of the National Security Telecommunications Advisory Committee http://www.aci.net/kalliste/electric.htm
[9] Larissa Paul, "When Cyber Hacktivism Meets Cyberterrorism," SANS Institute, February 19, 2001 "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"
[10] Sascha Segan, "Safety At Risk, " ABC News.com, September 27, 2000, http://abcnews.go.com/sections/tech/DailyNews/gao_faa000927.html, General Accounting Office, "Air Traffic Control: Weak Security Computer Practices Jeopardize Flight Safety," GAO-AIMD 98-155, http://www.gao.gov/archive/1998/ai98155.pdf
[11] Keith Bradsher, "With Its E-Mail Infected, Ford Scrambled and Caught Up," The New York Times, May 8, 2000
[12] Riptech Internet Security Threat Report, July 2002,
[13] Buchan, Glenn C., "Implications of Information Vulnerabilities for Military Operations," in Khalilzad and White, The Changing Role of Information in Warfare, Rand, 1999
[14] This is not an argument for self-censorship, as the economic and political benefits of openness and having information available to the public outweigh in almost all cases the potential costs of espionage.
[15] "Extreme Weather Sourcebook," http://sciencepolicy.colorado.edu/sourcebook/composite.html, Richard Wray, "Comptroller estimates city's overall bill at up to $95bn," The Guardian, September 5, 2002. http://www.guardian.co.uk/september11/story/0,11209,786326,00.html, To help put these losses in the context of a $10 trillion national economy, note that the U.S. spent $7 billion in 2002 on Halloween candy.
[16] See: American Society for Industrial Security and PriceWaterhouseCoopers, 10th Annual Survey "Trends in Proprietary Information Loss," http://www.pwcglobal.com/extweb/ncsurvres.nsf/0cc1191c627d157d8525650600609c03/36951f0f6e3c1f9e852567fd006348c5/$FILE/ASIS.pdf, and Computer Security Institute, "2002 Computer Crime and Security Survey," http://www.gocsi.com/press/20020407.html
[17] http://www.gocsi.com/press/20020407.html
[18] I am grateful to Antoin O Lachnain and Michael Yap for pointing out that small countries like Singapore, that do not have the same degree of redundancy, may be more vulnerable.
[19] See Computer Science and Telecommunications Board, National Research Council, Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers, National Academy Press, 2001