日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

“Assessing the Risk of Cyber-terrorism, Cyber-war and other Cyber-threats”

by

Dr. James A. Lewis
Director,
Technology and Public Policy Program
Center for Strategic and International Studies

Assessing the Risk of Cyber-terrorism, Cyber-war and other Cyber-threats
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 and information warfare are complex problems that reach into new areas for national security and public policy. 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, nations expose new vulnerabilities that a hostile nation or group could exploit to penetrate computer networks 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. A closer look at the relationships between computer networks and critical infrastructures, their vulnerability to attack, and the effect on national security, suggests that this is wrong. While many computer networks remain vulnerable to attack, few critical infrastructures are equally vulnerable.

To reassess the risks of cyber attack, we need to first put cyber-warfare and cyber-terrorism in the historical context of attacks against infrastructure. Second, we need to examine cyber attacks against a backdrop of routine infrastructure failures. We have good data on power outages, flight delays and communications disruptions that occur 'normally' and can use the consequences of these routine failures 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.

Infrastructure as a 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. There theories were put to the test by the U.S. Army and Royal Air Forces during World War II.

A key document for understanding how attacks on infrastructure affect societies is the World War II Strategic Bombing Survey. Early theorists of air warfare had predicted that an aerial onslaught would paralyze or cripple the target nation. What the Survey found, however, is that industrial societies are impressively resilient. One of the 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." This is important as in a cyber attack, once a hacker has gained access and the damage is done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line. New vulnerabilities and new tactics would need to be exploited for a sustained cyber attack.

'Routine' Failure versus Cyber Attack

Critical infrastructure protection creates a new set of problems for national security. The focus is on civilian and commercial systems and services. The scope of these new problems depends on how we define national security and how we set thresholds for acceptable damage. From a public safety perspective, no country will accept even a single attack on infrastructure or interruption of services. However, from a strategic military perspective, attacks that do not degrade national power are not significant. Cyber-attacks do not pose a 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 can be a routine occurrence. Cyber-terrorists might have to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or have any noticeable effect. For most of the critical infrastructure, this is not a feasible attack 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

More 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. 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.

Cyber attacks are often presented as a threat to military forces and the Internet has major implications for espionage and warfare. While information operations and information dominance 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. For example, while there were many attack against U.S. military computer networks during operations in Kosovo, none of these attacks resulted in a single sortie being cancelled or in a single casualty.

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 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 do not have the dramatic political effect that terrorists seek and will not be their preferred weapon.

While there has been press reporting of concern by government officials over Al Qaeda plans to use the Internet to wage cyber-terrorism, these stories often recycle the same hypothetical scenarios previously attributed to the foreign government 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.

However, a greater reliance on internet-accessible computer networks opens new vistas for espionage activities, and terrorist groups are likely to use the Internet to collect information on potential targets. This differs considerably 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, unobtrusively collecting intelligence. It will not disrupt essential services or leave embarrassing messages on websites, but remain quietly in the background collecting information.

Cyber Attacks as an Economic Weapon

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. Cyber attacks could be a valuable economic weapon, especially for non-state actors. The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lowered productivity, and third party liability. 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.

The risk to a nation-state in deploying cyber-weapons against a potential opponent's economy are probably too great for any country to use these measures. The amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda.

Conclusion

This review suggests that computer network vulnerabilities are an increasingly serious economic problem but that their threat to national security is overstated. Modern industrial societies are more robust than they appear. Critical infrastructures, especially in large market economies, are more distributed, diverse, redundant and self-healing than an initial 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.

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 appear to have "The Sky is Falling" as its theme. The sky is not falling, but there are real problems, albeit not of national security. Redundancy, routine rates of failure and response, and the degree of human control and intervention present in any system suggests that many infrastructures are resistant to cyber attack. This is not a static situation, and the vulnerability of critical infrastructure to cyber attack could change if governments do not balance an increasing reliance on networks and Internet technologies with efforts to improve network security and ensure that critical infrastructures are robust and resilient.

(Complete version available upon request)