eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

Challenges Strategy, Tactics of Terrorists Hackers to Cyber Security and Data Privacy

Dr. Munna Lal Yadav[1]
[1]Head of Department, Defence and Strategic Studies, R.K. P.G. College, Amethi, Dr. Ram Manohar Lohia Avadh University Ayodhya.

Received: 25 November 2025 Accepted & Reviewed: 28 November 2025, Published: 30 November 2025

Abstract

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. 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, but a brief review suggests that while many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable. 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 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.

KeyWords:- Cyber Terrorism- Why Computer Attacks are Successful, Vulnerabilities Persist, Possible Effects of Cyber Attack, Capabilities for Cyber Attack, Terrorist-Sponsoring Nations, Possible Links Between Hackers and Terrorists, National Strategy to Secure Cyberspace, Terrorist Tactics.

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

Introduction

Terrorist groups today frequently use the Internet to communicate, raise funds, and gather intelligence on future targets. Although there is no published evidence that computers and the Internet have been used directly, or targeted in a terrorist attack, malicious attack programs currently available through the Internet can allow anyone to locate and attack networked computers that have security vulnerabilities and possibly disrupt other computers without the same vulnerabilities. Terrorists could also use these same malicious programs, together with techniques used by computer hackers, to possibly launch a widespread cyber attack against computers and information systems that support the U.S. critical infrastructure.

Some security experts believe that past discussions about cyber terrorism may have over-inflated the perceived risk to the critical infrastructure.[1] However, other observers believe that security threats are continuously evolving along with changes in technology. They believe that terrorist groups are recruiting new, younger members more knowledgeable about computer technology, and that someday a terrorist group may attempt to use computers as a weapon.

Definition of Cyber Terrorism

It is first important to note that no single definition of the term "terrorism" has yet gained universal acceptance. Additionally, no single definition for the term "cyber terrorism" has been universally accepted. Also, labeling a computer attack as "cyber terrorism" is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred.

There are some emerging concepts, however, that may be combined to help build a working definition for cyber terrorism. Under 22 USC, section 2656, terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The term "international terrorism" means terrorism involving citizens or the territory of more than one country. The term

"terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism.[2]

The National Infrastructure Protection Center (NIPC), now within DHS, defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and or destruction, and creating terror for the purpose of coercing a government to change its policies."[3]

By combining the above concepts, "cyber terrorism" may also be defined as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies. The definition may be extended by noting that DOD operations for information warfare also include physical attacks on computer facilities and transmission lines.[4]

Finally, other security experts reportedly believe that a computer attack may be defined as cyber terrorism if the effects are sufficiently destructive or disruptive to generate fear potentially comparable to that from a physical act of terrorism. Under this "severity of effects" view, computer attacks that are perhaps limited in scope, but that lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence portions of the economy may also qualify as cyber terrorism.[5]

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

Why Computer Attacks are Successful

Networked computers with exposed vulnerabilities may be disrupted or taken over by an attacker. Computer hackers opportunistically scan the Internet looking for computer systems that do not have necessary or current software security patches installed, or that have improper computer configurations leaving them vulnerable to potential security exploits. Even computers with up-to-date software security patches installed may still be vulnerable to a type of attack known as a "zero-day exploit". This may occur if a computer hacker discovers a new vulnerability and launches a malicious attack program onto the Internet before a security patch can be created by the software vendor and made available to provide protection to software users. Should a terrorist group attempt to launch a coordinated attack against computers that manage the U.S. critical infrastructure, they may copy some of the tactics now commonly used by computer hacker groups to find computers with vulnerabilities and then systematically exploit those vulnerabilities.

Why Computer Vulnerabilities Persist

Vulnerabilities provide the entry points for a computer attack. Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate training in computer security and poor quality in software products.[6] Sometimes this delay may occur if an organization does not actively enforce its own security policy or if the security function is under-staffed or sometimes the security patch itself may disrupt the computer when installed, forcing the systems administrator to take additional time to adjust the computer configuration to accept the new patch. To avoid potential disruption of computer systems, sometimes a security patch is tested for compatibility on an isolated network before it is distributed for installation on other computers. As a result of delays such as these, the computer security patches that are actually installed and protecting computer systems in many organizations, at any point in time, may lag considerably behind the current cyber threat situation. Whenever delays for installing important security patches are allowed to persist in private organizations, in government agencies, or among home PC users, some computer vulnerabilities may remain open to possible attack for long periods of time.

Many security experts also emphasize that if systems administrators received proper training to adhere to strict rules for maintenance, such as installing published security patches in a timely manner or keeping their computer configurations secure, then computer security would greatly improve for the U.S. critical infrastructure.[7]

Commercial software vendors are often criticized for consistently releasing products with errors that create vulnerabilities.[8] Government observers have reportedly stated that approximately 80 percent of successful intrusions into federal computer systems can be attributed to software errors or poor software quality.[9] There is currently no regulatory mechanism or legal liability if a software manufacturer sells a product that has design defects. Often the licensing agreement that accompanies the software product includes a disclaimer protecting the software vendor from all liability.

Possible Effects of Cyber Attack

A cyber attack has the potential to create economic damage that is far out of proportion to the cost of initiating the attack.[10] Security experts disagree about the damage that might result from a cyber attack[11] and some have reportedly stated that U.S. infrastructure systems are resilient and could possibly recover easily from a cyber terrorism attack, thus avoiding any severe or catastrophic effects.

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

Tighter physical security measures now widely in place may actually encourage terrorists in the future to explore cyber terror as a form of attack that offers lower risk of detection to the attackers, with effects that could possibly cascade to disrupt other information systems throughout the critical infrastructure.[12] A successful cyber attack that targets vulnerable computers, causing them to malfunction, can result in corrupted flows of information that may disable other downstream businesses that have secure computer systems previously protected against the same cyber threat. Cyber attacks that secretly corrupt secure credit card transaction data at retail Internet sites, could possibly cause that corrupted data to spread into banking systems and could erode public confidence in the financial sector or in other computer systems used for global commerce. Also, some Security experts reportedly have stated that because technology continuously evolves it is incorrect to think that future cyber attacks will always resemble the past annoyances we have experienced from Internet hackers.

However, other security observers disagree, stating that terrorist organizations might be reluctant to use the Internet itself to launch an attack. Some observers believe that terrorists will avoid launching a cyber attack because it would involve less immediate drama and have a lower psychological impact than a traditional physical bombing attack. These observers believe that unless a computer attack can be made to result in actual physical damage or bloodshed, it will never be considered as serious as a nuclear, biological, or chemical terrorist attack. Unless a cyber terror event can be designed to attract as much media attention as a physical terror event, the Internet may be better utilized by terrorist organizations as a tool for surveillance and espionage, rather than for cyber terrorism.[13]

Supervisory Control And Data Acquisition (SCADA) systems are computer systems relied upon by most critical infrastructure organizations to automatically monitor and adjust switching, manufacturing, and other process control activities, based on feedback data gathered by sensors. Some experts believe that these systems may be vulnerable to cyber attack and that their importance for controlling the critical infrastructure may make them an attractive target for cyber terrorists. SCADA systems once used only proprietary [14] computer software and their operation was confined largely to isolated networks. However, an increasing number of industrial control systems now operate using Commercial- Off-The-Shelf (COTS) software, and more are being linked via the Internet directly into their corporate headquarters office systems.[15] Some observers believe that SCADA systems are inadequately protected against a cyber attack, and remain vulnerable because many of the organizations that operate them have not paid proper attention to computer security needs.[16]

However, other observers disagree, suggesting that the critical infrastructure and SCADA systems are more robust and resilient than early theorists of cyber terror have stated and that the infrastructure would likely recover rapidly from a cyber terrorism attack. They cite, 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 always affect national security. System failure is a routine occurrence at the regional level, where service may often be denied to customers for hours or days. Highly skilled engineers and technical experts who understand the systems would, as always, work tirelessly to restore functions as quickly as possible. Cyber terrorists would need to attack multiple targets simultaneously for long periods of time, perhaps in coordination with more traditional physical terrorist attacks, to gradually create terror, achieve strategic goals, or to have any noticeable effects on national security.[17]

Capabilities for Cyber Attack

Stealth and pre-operational surveillance are important characteristics known to precede a computer attack launched by hackers. Launching a coordinated or widespread attack against critical infrastructure computers

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

may call for significant resources to develop the required set of technically sophisticated hacker tools and to also conduct the necessary pre-operational surveillance. It has been estimated that advanced structured cyber attacks against multiple systems and networks, including target surveillance and creation and testing of new hacker tools, may require 2 to 4 years of preparation, while a complex coordinated cyber attack causing mass disruption against integrated, heterogeneous systems may require 6 to 10 years or preparation.[18]

Terrorist-Sponsoring Nations

The U.S. Department of State lists seven designated state sponsors of terrorism in 2002: Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan.48 These countries are identified as sponsors for funding, weapons and other materials for planning and conducting operations by terrorist groups. Elements in Iran are believed by some observers to have close links with Al Qaeda and North Korea has continued to sell weapons and high-technology items to other countries designated as state sponsors of terrorism. However, it should be pointed out that a study of trends in Internet attacks determined that countries on the Department of State list generated less than one percent of all reported cyber attacks directed against selected businesses in 2002.[19]

News sources have reported that, other than a few Web site defacements, there was no evidence that a computer attack was launched by Iraq or by terrorist organizations against United States military forces during Gulf War II.[20] The security research organization, C4I.org, reported that prior to the March 2003 deployment of U.S. troops, traffic increased from Web surfers in Iraq using search terms such as, “Computer warfare,” “NASA computer network,” and “airborne computer.” Experts interpreted the increased Web traffic as an indication that Iraq’s government was increasingly relying on the Internet for intelligence gathering.[21]

News sources have reported recent statements made by Major General Song Young-geun, head of the Defense Security Command of South Korea, claiming that North Korea may currently be training more than 100 new computer hackers per year.[22] Pentagon and State Department officials reportedly are unable to confirm the claims made by South Korea, and defense experts reportedly believe that North Korea is incapable of seriously disrupting U.S. military computer systems. Also, Department of State officials have reportedly said that North Korea is not known to have sponsored any terrorist acts since 1987. However, computer programmers from the Pyongyang Informatics Center in North Korea have done contract work to develop software for local governments and businesses in Japan and South Korea and other security experts reportedly believe that North Korea may have also developed a considerable capability for cyber warfare, partly in response to South Korea’s admitted build up of 177 computer training centers and its expanding defense budget targeted at projects to prepare for information warfare.[23]

Possible Links Between Hackers and Terrorists

Hacker groups are numerous and have differing levels of technical skill .Membership in highly-skilled hacker groups may be exclusive and limited only to individuals who develop and share their own closely-guarded set of sophisticated hacker tools. These exclusive hacker groups are more likely to not seek attention because secrecy allows them to be more effective.

Some hacker groups may be globally dispersed, with political interests that are supra-national or based on religion or other socio-political ideologies. Other groups may be motivated by profit or linked to organized crime, and may be willing to sell their computer skills to a sponsor, such as a nation state or a terrorist group, regardless of the political interests involved. For instance, it has been reported that the Indian separatist group, Harkat-ul-Ansar, attempted to purchase military software from hackers in late 1998. In March 2000, it was reported that the Aum Shinrikyo cult organization had contracted to write software for up to 80 Japanese

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

companies and 10 government agencies, including Japan's Metropolitan police department; however, there were no reported computer attacks related to these contracts.[24]

Linkages between hackers, terrorists, and terrorist-sponsoring nations may be difficult to confirm, but cyber terror activity may possibly be detected through careful monitoring of network chat areas where hackers sometimes meet anonymously to exchange information. The Defense Advanced Research Projects Agency (DARPA) has conducted research and development for systems, such as the former Terrorism Information Awareness Program [25] that are intended to help investigators discover covert linkages among people, places, things and events related to possible terrorist activity.

National Strategy to Secure Cyberspace

Another potential issue is whether the National Strategy to Secure Cyberspace should rely on voluntary action on the part of private firms, home users, universities, and government agencies to keep their networks secure or whether there may be a need for possible regulation to ensure best security practices. Some security experts believe that public response has been slow to improve computer security despite warnings about possible cyber terrorism, partly because there are no regulations currently imposed by the National Strategy to Secure Cyberspace.[26] Others in the technology industry, however, believe that regulation would interfere with innovation and possibly harm U.S. competitiveness.

Terrorist Tactics

Similarities may exist in characteristics of some tactics used to prepare for and execute a cyber crime or cyber espionage computer attack and tactics used to prepare for and execute some recent physical terrorist operations.

(1) Network meetings in cyberspace
(2) Extensive pre-operative surveillance
(3) Exploits of soft and vulnerable targets
(4) Swarming methods may all be characteristics of tactics used by some terrorist groups as well as by computer hackers. Knowing these similarities may be helpful to investigators as they explore different methods to detect planning, and help prevent a possible cyber attack by terrorist groups.

The organizational structures of many terrorist groups are not well understood and are usually intended to conceal the interconnections and relationships.[27] A network organization structure (as opposed to a hierarchical structure) favors smaller units, giving the group the ability to attack and quickly overwhelm defenders, and then just as quickly disperse or disappear. Terrorist groups using a network structure to plan and execute an attack can place government hierarchies at a disadvantage because a terrorist attack often blurs the traditional lines of authority between agencies such as police, the military, and other responders.

Conclusion

Terrorist groups are described by DHS as opportunistic, choosing to exploit soft vulnerabilities that are left exposed. Similarly, an increasingly popular trend for computer hackers engaged in computer crime or computer espionage is to use a malicious program called a worm, that pro-actively spreads copies of itself through the Internet, rapidly finding as many computers as possible with the same non-patched vulnerability, and then automatically installing itself to quietly await further instructions from the attacker.

At an appropriate time, the attacker may choose to send a command through the Internet to activate these thousands of infected computers, instructing them to either stop working properly, or reveal unauthorized information (such as passwords or credit card numbers) or attack and overwhelm a targeted organization and

block access to many services on the Internet. A worm can quietly corrupt data on infected computers, transmit that corrupted data to other downstream computers, and even interfere with network response for computers that have installed the right security to protect against infection.

Similarly, computer hackers are often composed of small groups or individuals who meet anonymously in network chat rooms to exchange information about computer vulnerabilities, and plan ways to exploit them for cyber crime or cyber espionage. By meeting only in cyberspace, hackers can quickly disappear whenever government authorities try to locate them. Hackers have also designed recent computer exploits that launch anonymously from thousands of infected computers to produce waves of disruption that quickly overwhelm a single targeted organization or multiple organizations such as a list of banking institutions.

References

01-Drew Clark: The critical infrastructure is viewed by some more resilient than previously thought to the effect of a

computer attack. 03 June-2003, Computer Security Officials Discount Chances of Digital Pearl Harbor.

02 -The U.S Government has employed this definitions of terrorism for statistical and analytical purposes sins 1983. U.S.

Department of State, 2002, patterns of global terrorism-2003.

03- Scott Berinato: Ron Dick, 2002 Direct of NIPC, 15 March-2002, The Truth About Cyber terrorism, CIO.

04-Clay Wilson: DOD information warfare operations include the use of directed energy weapons that can deliver high-

energy electromagnetic pulses to destroy computer circuits-14 march-2003-Information Warfare and Cyber war.

05-Dorothy Denning, Nov-2001, is Cyber War Next, Social Science Research Council.

06-The SANS Institute , in cooperation's with the National Infrastructure Protection Centre, Publish an annual list of the

10 most commonly exploited vulnerabilities for Windows systems and for Unix system-15 April-2003.

07-Robert Lemos: According to security group attrition org, failure to keep software patches up to date resulted in 99%

of 5823 Web site defacements in 2003.

08-Jai Kumar Vijayan: 15 September 2003 Attack new Windows Flaws Expected Soon, Computer World, Vol.37 P.01

09-Johathan Krim: 24 Sep, 2003, Security Report Puts Blame on Microsoft, Washingtonpost.com.

10-Hurricane Andrew: The most expensive natural disaster in U.S History, March-2003

11-James Lewis: Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats.

12-Terrorims an Introductions, CFR 4 April-2003

13-James Lewis:2002, December, Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats.

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 11, November 2025

14-Proprietary systems are unique, customs built software products intended for installation on a few computers and

their uniqueness makes them a less attractive target for hackers. they are less attractive because finding a security

vulnerability takes time (See Appendix a) and a hacker may usually not consider it worth their while to invest

preoperative surveillance and research needed to attack a proprietary system on a single computer.

15-Kevin Poulsen: 19 Aug-2003 Slammer Worm Crashed Ohio Nuke Plant Networks, Security Focus

16-Sharon Gaudin: 19 July 2002, Security Experts: U.S. Companies Unprepared for Cyber Terror.

17-Scott Nance: 7 April-2003 Debunking Fears: Exercise Finds- Digital Pearl Harbor Risk Small, Defense Weak.

18-Dorothy Denning: 2002, Levels of Cyber terror Capability: Terrorist and the Internet, Presentations.

19-U.S. Department of State, April-2003, 2002 Patterns of Global Terrorism Report.

20 -Kim Zetter, May-2003, Faux Cyber war, Computer Security, Vol.6 No-05, P-22

21-Brian Mc Williams: 22 May 2003- Iraq's Crash Course in Cyber war, Wired News

22-Miami Herald: 16 May-2003-North Korea May be Training Hackers

23-Brian Mc Williams: 2 June- 2003- North Korea's School for Hackers, Wired News.com

24- Dorothy Denning: Cyber Terrorism: 24 August-2000

25-Report to Congress Regarding the Terrorism Information Awareness Program, Executive Summary, 20 May 2003 P-1

26-Gary H. Anthes and Thomas Hoffman: 12 May-2003, Tarnished Image, Computerworld, Vol. 37 No. 19 P-37

27-Report to Congress Regarding the Terrorism Information's Awareness Program, Executive Summary, 20 May2003p-3