

ISSN: 2582 - 2942



LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- VI

AUGUST 2020

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of LexForti Legal Journal. The Editorial Team of LexForti Legal Journal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of LexForti. Though all efforts are made to ensure the accuracy and correctness of the information published, LexForti shall not be responsible for any errors caused due to oversight otherwise.



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE

OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS
INTERNATIONAL UNIVERSITY) - MARKETING
MANAGEMENT

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION
BUSINESS LAW)

EDITOR

DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL
AND ADMINISTRATIVE LAW)., NET (TWICE) AND
SET (MAH.)

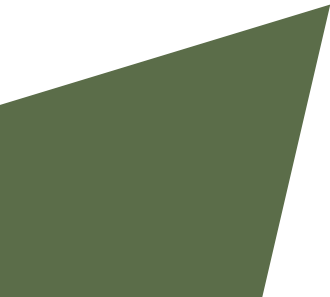
EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE

ABOUT US

LexForti is a free open access peer-reviewed journal, which gives insight upon broad and dynamic legal issues. The very objective of the LexForti is to provide open and free access to knowledge to everyone. LexForti is highly committed to helping law students to get their research articles published and an avenue to the aspiring students, teachers and scholars to make a contribution in the legal sphere. LexForti revolves around the firmament of legal issues; consisting of corporate law, family law, contract law, taxation, alternative dispute resolution, IP Laws, Criminal Laws and various other Civil issues.



Emerging form of Terrorism: Cyber Terrorism

Karun Roy & Parvati M Pai

INTRODUCTION

Terrorism is about violence. With the advent of twenty first century, the definition of terrorism has become more complex. Now the weapons of terrorism have varied from the traditional firearms to a click in the computer. Terrorism is not a new phenomenon. It has, and always will, remain a weapon of the weak. It is a low-cost, high-leverage method and tactic that enable small nations, sub national groups and even individuals to circumvent the conventional projections of national strength.

Underscoring that India was on the threshold of a digital age, former National Security Adviser M.K. Narayanan said the country needed to further strengthen its defensive and offensive capabilities to deal with the new wave of cyber warfare. The Aadhar card was in controversies for the same matter. "India is on the threshold of a digital age and the use of Aadhaar cards is becoming ubiquitous. The danger is that not only it is becoming easier to mask an identity online, but also once the malware codes come into the open market, it can be bought and repurposed by hackers anywhere in the world," Narayanan said. He was speaking at a seminar on 'Cyber-terrorism and the economy' organised by CENERS-K (Centre for Eastern and North Eastern Regional Studies.)¹

This paper is a brief attempt to look into something that has hit mankind with a high severity, that is, cyber terrorism and cyber terrorism's weapons and their effects and consequences and how to overcome or face such attacks. Cyber terrorism has become a highly increasing form of terrorism. It has acquired so much media appeal and that has made it one of the a feasible form of terrorism. It can be considered as one of the negative consequences of technological advancements.

¹http://economictimes.indiatimes.com/articleshow/67555647.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

UNDERSTANDING THE TERM TERRORISM

The term "terrorism" has been taken from the French word '*terrorisme*', which in turn is based on the Latin verb '*terrere*'. It dates back to 1795 when it was used to describe the actions of the Jacobin Club in their rule of post-Revolutionary France, the so-called "Reign of Terror".

Terrorism refers to a strategy of using violence, social threats, or coordinated attacks, with an intention to generate fear, cause disruption, and ultimately, bring about compliance with specified political, religious, or ideological demands put forward by the attackers. In 1994, in the UN General Assembly Declaration on Measures to Eliminate International Terrorism, it was stated that terrorism include criminal acts intended to provoke a state of terror in the public or a group or particular persons and that such acts are in any circumstances unjustifiable whatever the considerations to justify it be.²

CYBER TERRORISM

Cyber terrorism has been defined by the U.S. Federal Bureau of Investigation as, '*a premeditated politically motivated attack against information, a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and sub national groups*'.³ The main aim behind cyber terrorism is to cause harm and destruction. It is different from common Internet crimes like identity theft and money fraud.

In cyber terrorism, technology is used to divert or destroy systems and infrastructure, cause injury or death and undermine economies and institutions. It is otherwise referred to as cyber warfare. It is capable of even causing wars. It consists of two elements: cyberspace and terrorism. Basically, inculcating the terrorism aspects into cyber space is how cyber terrorism comes up. Cyber terrorism is becoming more dangerous because of its anonymity, the potential to cause huge harm, the psychological impact and finally the media appeal. The threat is very alarming because most of the countries depend on the computer and the internet for communications regarding critical infrastructures and defence and other confidential information thus gaining access and causing threats to the nation.

² OHCHR factsheet

³ <https://www.techopedia.com/definition/6712/cyberterrorism>

According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centres and water systems. It is a genuine danger to the quick innovation and improvement. It could be committed against an individual or against the nation as a whole. Potential targets include frameworks who and which control the country's resistances and foundation.

CYBER TERRORISM CAN BE BROADLY CATEGORIZED UNDER THREE MAJOR CATEGORIES:

- Simple: This category includes basic attacks such as hacking of an individual system.
- Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
- Complex: These are coordinated attacks that can have a large-scale impact and they make use of sophisticated tools.

With the help of the Internet, a few examples of some attacks and incidents around the world that are considered to be acts of cyber terrorism are listed:

1. Currently during the outbreak of the Covid-19, the CEO of the IT security giant Kaspersky Lab, Eugene Kaspersky in an online press conference likened the chances of cyber attacks on hospitals to acts of terror. It was stated that there has been a significant rise in both opportunistic and targeted attacks including spear-phishing campaigns with fake information about the virus. There were cases where the users were tricked to opening malicious links or attachments and downloading malwares. It constitutes as a form of cyber attack.⁴
2. The Russian government allegedly perpetrated a distributed denial-of-service attack in March 2014 that disrupted the internet in Ukraine and allowed pro-Russian rebels to take control of the Crimea.
3. In December 2016, 225,000 customers in Ukraine experienced a blackout, the result of remote intrusions at three regional electric power distribution companies. The cyber terrorists blamed for the attack were thought to be from Russia. The cyber criminals flooded phone lines with a DoS attack and also used malware to attack and destroy data on hard drives.

⁴ <http://www.infosecurity-magazine.com/news/cyberattacks-hospitals-acts-of/>

4. In 2016, the U.S. Department of Justice announced that Ardit Ferizi, a citizen of Kosovo, was convicted and sentenced to 20 years in prison "for providing material support to the Islamic State of Iraq and the Levant (ISIL), a designated foreign terrorist organization, and accessing a protected computer without authorization and obtaining information in order to provide material support to ISIL." It was considered to be a dangerous national security cyber threat.
5. Hackers affiliated with the North Korean government were thought to be responsible for the cyber-attack on Sony Pictures Entertainment prior to Sony releasing the film *The Interview*, which depicted the death of North Korean leader Kim Jong-Un. The hacking group that claimed responsibility, known as the "Guardians of Peace," expressed anger at *The Interview* and made vague threats of violence in reference to the 9/11 terrorist attacks, which led to Sony cancelling the film's theatrical release. The FBI ultimately determined that the code, encryption algorithms, data deletion methods and compromised networks were similar to those previously used by North Korean hackers. Additionally, the FBI discovered that the hackers had used several IP addresses associated with North Korea.
6. With the Middle East Conflict as a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported by the NIPC (National Infrastructure Protection Center) in October of 2000 to U.S officials. The attacks were a stream of e-mail floods. DoS attacks and Ping flooding of such sites as the Israel Foreign Ministry, Israeli Defence Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah.
7. As tensions between the neighbouring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan (which also included members of the Al Qaeda Organization) began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Centre which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy's website.

8. In 2015, cybercriminals attacked the German parliament, causing widespread disruption. The hackers infected 20,000 computers used by German politicians, support staff members and civil servants, stealing sensitive data and then demanding several million euros to clean up the damage. A group of Russian nationalists who wanted the government of Berlin to stop supporting Ukraine claimed responsibility, but members of the Russian intelligence were also thought to be involved.
9. In May 2017, major companies, government offices and hospitals around the world were hit by a ransom ware called WannaCry, which seized control of victims' computers until they paid ransom. Cyber security firm Avast identified more than 75,000 ransom ware attacks in 99 countries, making it one of the largest and most damaging cyber-attacks in history. Experts and government agencies agreed that the Lazarus Group, which was affiliated with the North Korean government, was responsible for releasing 'WannaCry'. These two attacks [WannaCry and NotPetya] affected organizations in more than 150 countries, prompted business interruption and other losses estimated at well over USD 300 million by some companies, brought reputational damage, and resulted in loss of customer data.

CYBER TERRORISM AND LAWS IN INDIA

In India there is no one law, which specifically deals with prevention of malware through aggressive defence. Thus, the analogous provisions have to be applied in a purposive manner. The protection against malware attacks can be claimed under the following categories:

(A) Protection under the Constitution of India:

(B) Protection under the Indian Penal Code (I.P.C), 1860, and

(C) Protection under the Information Technology Act (ITA), 2000:-On October 17, 2000 special laws governing Cyber Crimes became effective in India with the passage of IT Act 2000. Section 66 F lays down the punishment for cyber terrorism. It reads as follows:

66F. Punishment for cyber terrorism.—(1) Whoever,— (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by— (i) denying or cause the denial of access to any person authorised to access computer resource; or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce

any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70;

or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

(D)Special statutes for terrorism such as Unlawful Activities Prevention (Amendment) Act, 2014

EFFORTS OF COMBATING CYBER TERRORISM

Some ways to protect computer from cyber-attacks are isolation, encryption, use of firewalls to screen all communications to a system such as to screen user requests to check if they come from a previously defined domain or Internet Protocol (IP) address or to prohibit Telnet access into the system.

The Interpol, with its 178 member-countries, does a great job in fighting against cyber terrorism. They help all the member countries and training their personnel. The Council of Europe Convention on Cyber Crime(the first international treaty for fighting against computer crime) is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. This treaty has already enforced after its ratification by Lithuania on 21st of March 2004.

The Association of South East Asia Nations (ASEAN) has set plans for sharing information on computer security. They are going to create a regional cyber-crime unit by the year 2005.

In December 1998, the Department of Defence (DoD) announced that information warfare was being institutionalized as the new operational battle space (Information Operations Department, School of Information Warfare and Strategy, National Defence University). The three traditional battle-grounds were land, sea, and air. These elements are now called battle spaces to incorporate the fourth element of information warfare. In essence, cyber-space is formally recognized as spread throughout all DoD battle spaces.

Battle spaces do not exist in the emergency response world. However, we organize response units in an operations section, with response branches being EMS, fire/rescue, law enforcement, public health, and public works. These critical branches are similar to battle spaces, are dependent on information operations, and are vulnerable to information warfare. Like the DoD, civilian emergency agencies are subject to cyber-attack, and must protect this essential battlespace element.

ADAPTING TO CHANGE

As the millennium approached, we were constantly reminded that things were changing in the world, that things are different in this century, that new technologies will revolutionize the future. We witnessed miraculous changes over the last 100 years and there are no indications that this century will be any different. All of the factors influencing future global social, economic, technologic, information, and political evolution are currently in place or in development. For public safety, the concern is not the changes that are occurring, but in which forms they will manifest and whether any potential negatives are associated with them. For example, we know that information technology will have a profound positive effect on emergency services, yet we also faced the first crisis of the new millennium: the possibility of failure of the information technology platform.

The Year 2000 (Y2K) computer problem, also known as the millennium bug, was potentially catastrophic to the national infrastructure of industrial economies. However, the Y2K non-event was not an imagined threat. Cyber awareness, preparation, and an intense focus on the information infrastructure is what saved the people. The transformation to a technology-based society brought not only solutions, but also unanticipated problems.

CRITICAL INFRASTRUCTURE- WHAT?

The critical infrastructure consists of, in part, information and financial management systems, telecommunications, dispatch centres, cable television, power production, water service, and natural gas and its storage facilities, transportation, and distribution mechanisms. Protecting this infrastructure against physical and electronic attack and ensuring the availability of the infrastructure is a complex issue.

The highlights of the "2000 Computer Crime and Security Survey" conducted include the following:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches in the previous twelve months.
- Seventy percent reported a variety of serious computer security breaches other than the most common ones of computer viruses, lap-top theft, or employee "net abuse"; For example, theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks, and sabotage of data or networks.
- Seventy-four percent acknowledged financial losses due to computer breaches/cyber attacks.
- Forty-two percent were willing and /or able to quantify their financial losses.

The critical infrastructure is currently the most vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential for the use of cyber-terrorism. For economic reasons, increasing deregulation and competition created an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This, in turn, creates a tunnel of vulnerability previously unrealized in history.

The critical infrastructure of our communities is basically transparent. Almost every aspect of twenty-first-century life revolves around the efficiency of zeros and ones flowing at near light speed through microchips.

- Transportation is an example. Air, ground, and water transportation systems depend on computer traffic control. Software, data systems, and communications guide the entire air traffic control system.
- The nation's power grid is another example. The system is a complex matrix of generating systems, switching systems, and distribution systems, all computer controlled. Major blackouts and brownouts have occurred because of a software failure or the bisection of a fibre-optic cable.

- A third example is the world financial system. As reported in a Learning Channel TM documentary, 90 percent of the world's wealth is digital. Individual and business financial holdings are essentially an account number associated with a fiscal amount in a financial database.

In the previous examples, accidental electronic failures have disrupted the systems. Intentional cyber-attacks have likewise caused system disruption. An information attack can halt air traffic, gridlock a ground transportation system, cause a regional power failure, or cripple a financial system. These events cause multiple deaths and injuries. Such events maybe called cyber terrorist attacks.

THE PUBLIC SAFETY INFRASTRUCTURE

The elements of the critical infrastructure that are most important to emergency responders are the essential systems in the public safety infrastructure. The general areas of our infrastructure are communications, computer-aided dispatch (CAD) systems, geo-based information systems (GIS), e-mail, and informational databases.

The most critical system is communications. The communications dispatch system includes repeaters, consoles, enhanced trunking systems, transmitters, and receivers. All of these elements are electronic, and susceptible to data corruption. The public also has a communications system, namely, 911. All aspects of an enhanced 911 system are computer driven including electronic switching, automatic location identification, and automatic call routing. Most systems also have a database of caller medical information, hazardous materials data, location descriptions, and premise histories. There are many cases of hackers corrupting the telephone switching system for the purpose of making free toll calls. At a more serious level, 911 systems have been hacked for malicious purposes. The result has been missed calls, system outages, and confusion coupled with a diminished or absent capacity for responding to emergencies. Computer-aided dispatch systems include electronic mapping, system status software, automatic vehicle location software, and databases of call information. A failure of any of these systems results in downgrading dis-patching to a manual mode. Information operations sabotage during a terrorist incident could greatly inhibit the ability of the public safety delivery system to effectively respond. Information databases and decision systems have progressed from an oddity to a necessity in less than a decade. Some of the information now routinely used includes:

- Medical protocols
- Logistics data
- Disaster plans
- Personnel information
- Hazardous materials response guidelines
- Criminal histories
- Financial reports and spreadsheets

A loss of information in any of these systems results in significant reduction of efficiency. More importantly, an intentional manipulation of data may go unnoticed for a significant duration, and result in poor decisions being made from inaccurate data. Basically the critical infrastructure in our community is hardly visible. It is as simple as a chip or a computer disk. It has to be kept in mind that these systems are essential and must be protected.

CYBER WARFARE: INCIDENT AND RESPONSE

Terrorism, as a tool of the disenfranchised, the disenchanting, and the just plain destructive is expected to undergo fundamental changes during the next decade. Data packets may very likely replace explosives as the favoured implement of destruction. TCP/IP (computer protocol) will be preferred over the Kalashnikov (AK- 47) and modems rather than suicide bombers will deliver chaos to the world's governments, local communities, and institutional infrastructures. The advent of the cyber warrior is at hand. As just described above, it is predicted that acts of terrorism will be binary events that couple information and electronic warfare with other activities such as explosives or chemical releases. The most concerning aspect of this threat shift in the nature of terrorisms the magnitude of the destruction that can be inflicted by a single individual with a simple keystroke rather than a detonator. Disruption of the world's financial markets, chaos in the public safety system, reduction in commercial productivity, depletion of health services, and the downing of telecommunication networks will be only the beginning.

A.Scenario in the Unites State.

In USA, Lt. General Kenneth A. Minivan, while director of the U.S. National Security Agency, stated "the threat that is posed by potential cyber attacks against the U.S. Military and computer system networks is now growing beyond the computer hacker stage". He added that groups potentially hostile to the United States are developing, or attempting to develop offensive

information warfare capabilities. The Minihan warning is viewed as validating what the prestigious U.S. Defence Science Board has called "a recipe for national disaster."

The following illustration is a depiction of local, national, and global information interdependence: The Rand Corporation's report, "Strategic Information Warfare" bluntly states, "Many U.S. allies and coalition partners will be vulnerable to information warfare attacks on their core infrastructures". Transnational Infrastructure Warfare involves attacking a nation's or sub-national entity's key industries and utilities; to include telecommunications, banking and finance, transportation, water, government operations, emergency services, energy and power, and manufacturing. These industries normally have key linkages and interdependencies, which could significantly increase the impact of an attack on a single component. Threats to critical infrastructure include those from nation-states, state-sponsored sub-national groups, international and domestic terrorists, criminal elements, computer hackers, and insiders. Governments, at all levels, have an obligation to secure their information systems and prepare for continuous infrastructure threats; having the will to do so is another matter entirely. Systems security is not a "do it once and you're done" proposition. An effective security plan is similar to an effective response plan. It must evolve and develop as the threat to systems evolves and develops. The lack of geographical, spatial, and political boundaries precludes conventional preventive measures. Attribution is second to information stability and therefore the majority of effort is placed on denying unauthorized access and system manipulation. Information warfare is attractive because it is relatively cheap to wage and it offers an asymmetrical return on investment for resource poor adversaries. When information systems are under attack, the demand for information will increase while the capacity of the information infrastructure will concurrently decrease.

The law, particularly international law, is ambiguous regarding criminality in, and acts of war on, information infrastructures. This ambiguity, coupled with a lack of clearly designated responsibilities for electronic defense, hinders the development of remedies and limits response options. The vulnerability of the information systems was painfully demonstrated by the "denial of service" attacks that occurred during a three-day period in February, 2000. A new breed of hacker called a "cracker" prompted this attack.

Crackers are sophisticated computer terrorists that attempt to disrupt or totally shut down networks or systems, whereas hackers are satisfied with just breaking into a system. According to Knight Ridder, regarding the 2000 attacks, major providers such as Yahoo!, eBay, Amazon.com and CNN were shut down as a result. The real-time use of information assumes the availability of information and information technology. The operational implications of a failure of information

and information technology must be addressed in an organized, sequential manner. Redundant capability in command and control capacity must be built into the system. Emergency communications plans must consider the extended system and its processes, and prepare for the eventuality of widespread system failure.

GLOBALIZATION

Globalization is changing the context in which terrorists operate. A transnational cast of characters that cannot be controlled by governments, individually or collectively, increasingly affects even so-called domestic terrorism. Information technology has effectively removed the ability of countries to isolate themselves. Information and communication control is difficult, if not impossible to achieve because the information revolution has resulted in democratic access to technology. An important result is that free speech and civil liberty have been given an inexpensive existing government international medium with which to voice discontent with. The notional concept of a centrally controlled international terrorist network, previously investigated during the 1960s and 1970s, was deemed to be unlikely due to conflicting ideologies, motivating factors, funding, arming, and training among global practitioners. However, networks are now quite possible with the advent of public access to the Internet, the ability to transfer funds and conduct banking electronically, the international arms market, encrypted digital communication technology, and the emergence of stateless terrorism. An important result is that instant global communication between offensive action cells and their controllers is now possible. Controllers now have global reach and can run multiple independent cells from a single location with no interaction between the cells. They can also contract terrorism services utilizing the local indigenous practitioners in a given target community. The complexity of weapons acquisition, production, transportation, lethality, and delivery platform has been diminished. Information management technology has also resulted in a reduced requirement for infrastructure, security, and detection avoidance and has resulted in an asymmetry between cause and effect.

COMPUTER DATA

Data on a computer screen has a high degree of credibility. Anyone born after 1950 was raised in front of a television screen. Anyone born after 1970 was raised in front of a computer screen along

with the television. Anyone born after 2000 was raised in front of a smartphone. As a result, data on a screen has a very high degree of believability. The habit of accepting electronic data without question must change, especially during tactical operations. When data does not agree with reasonable expectations, the data must be questioned, and data corruption suspected. In other words, the data must be "in the ballpark." For example, a chemical database that indicates procedures that appear inaccurate or unsafe should be compared with a printed source or another data system. In another case, if the CAD system suddenly indicates grossly inaccurate unit status, the information should be checked and corruption suspected. Any uses of electronic data by tactical decision makers should observe the following guidelines:

1. Do not blindly trust data screens.
2. Evaluate tactical data as a reality check.
3. Check other sources when data corruption is suspected.

In a terrorism /tactical violence event, consider the possibility of a coordinated information attack. Suspect intentional data manipulation when there is a mysterious communications failure. Maintain low tech information sources (books and paper) as an alternative to vulnerable electronic information.

DATA THEFT

Data theft is a simple method of deleting or corrupting sensitive data. Recent literature is inundated with articles about sophisticated intrusion methods. Sophisticated hackers (local and international) are able to crack passwords or find a back door route through a security firewall. However, simple theft is still an easy way to use low technology for high technology data corruption. How easy is it to walk into an agency, remove disks stacked on a desk, and walk out? If the data is removed, altered, and discretely returned, great damage may result. If backup disks are removed, followed by a system attack, provisions for storing the system may be lost. There are several steps that should be taken in any public or private agency to protect vital data from simple theft:

1. Office design—no one should be able to freely enter an office area; place a door between the entry lobby and data storage areas.
2. Entry control—anyone entering an office or data storage area should encounter a receptionist/secretary or security officer before proceeding.

3. ID badges—visitors and guests should sign in and be issued a security badge; employees should wear identification badges; procedures should require that any person without a badge be questioned.
4. Information storage—stored data should be locked and never stored on a desktop or in an open area; critical backup data should be stored in a safe at an off-premise location. This is good advice for fire and severe weather protection as well as theft.
5. Electronic entry—sensitive areas should be controlled by electronic entry; systems should provide printouts of all names, dates, and times of entries.

.DATA PROTECTION STANDARDS

Emergency agencies are very familiar with standards. In the fire service there are National Fire Protection Association (NFPA) standards; in EMS there are the NHTSA EMT and paramedic training standards. Law enforcement is governed by Department of Justice standards. The Occupational Safety and Health Administration (OSHA) standards govern most of us. However, there are no present standards for data and information storage/security. During the Twentieth National Information System Security conference (Baltimore, 1997), Robert T. Marsh (keynote address) stated, "For example, we recommend the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) jointly set standards and publish best practices for information security, and then share these with federal, state, and local governments, as well as private industry." Most local government response agencies are merely end users of electronic data. They lack the sophistication of federal government agencies and private organizations regarding protection of critical data. Standards and protocols are needed in the following areas:

- Data storage procedures
- Detection of running system attacks (real time)
- System restoration (disaster recovery)
- Physical security protocols
- Training standards for information technology security specialists

In the future we may have standards and protocols on information operations that rival tactical procedures. Presently, no such standards exist. At best, there is an inadequate mix of guidelines borrowed from private industry and federal agencies.

PUBLIC INFORMATION VS. DATA PROTECTION

A major information services issue in state and local government agencies is public disclosure of information. Most state laws are very liberal in their definition of "public information." State legislation usually defines exact types of documents that are confidential; all other documents not specified as confidential are public documents. In many states, public documents, including electronic data, must be re-leased within the same business day they are requested. Only reasonable charges for copying or duplication are allowed. You may be shocked to dis-cover that the following information is public in your state:

- Names and addresses of all employees, including elected officials, managers, and emergency response personnel.
- Standard operating procedures for response agencies and special teams.
 - Locations and descriptions of emergency response units, including equipment inventories.
- Radio frequencies, codes, and dispatch procedures
- Driver's license lists, including social security numbers and pictures
- Mutual aid contracts and mutual aid procedures.
- Incident reports and after-action reports.
- Building pre-plans and building layout graphics.

Hazardous materials information is a classic example. Federal legislation passed in the 1980s referred to as "The Community Right-to-Know Act" requires that information relating to the storage of hazardous materials be available to any member of the public who seeks the information. In many locales, this information is available at the public library. The data includes storage locations of reportable quantities, layout drawings of the storage sites, transportation routes, materials safety data sheets (MSDS), and descriptions of storage containers. Right-to-know legislation directly conflicts with information security. The intentional release of industrial hazardous materials provides an effective terrorism/tactical violence weapon. Because of public records laws and right-to-know legislation, domestic and foreign enemies can use our in-formation to attack us. Changing the law is admittedly a long and often painful process, but reducing the tactical information available as public record is a worthy goal. As times change and the terrorism/tactical violence threat increases, the naive twentieth-century public records laws must be altered. Many emergency response agencies are knowingly releasing sensitive information through the Internet. Institution homepages include links to computer-aided dispatch data screens, tactical response information, and links to communications centers that include real-time audio

radio traffic. The motive is usually an attempt to generate positive public relations. Unfortunately, this type of information is very helpful to an adversary. Take another look at your organization's Internet links and homepages, and re-move information that may make your system or your people vulnerable.

INFRASTRUCTURE PROTECTION

Most of the critical infrastructure is owned and operated by private business entities or utilities. Private industry shares government's concern about infrastructure protection. The private sector has the advantage of funding, the ability to spend millions on information security problems. For many years, the private sector has conducted research and implemented procedures to protect it from local threats. The federal government has a more national objective; the government must protect the citizens of the United States and all of the country's systems from cyber intrusion or dysfunction. A sharing of information is in the interest of both parties. In January 2000, President Bill Clinton announced a \$2 billion proposal to combat cyber-terrorism. The proposal establishes the Institute for Information Infrastructure Protection. The objective of the institute is to establish a public/private partnership for infrastructure protection research. Other aspects of the president's proposal include increased funding for re-search and development, and increased computer security. Local governments have similar information concerns because of ownership of the public safety infrastructure. However, local governments do not have the funds or expertise to conduct research in the information protection arena. Local government must depend on spin-offs from the public/private partnerships at the national level.

A. Information Security Management.

In the future, the information security management will be in new position in progressive response agencies. Physical security is common place; information security will be just as important. Presently, information security is haphazard at best, and certainly not a prominent unit in public safety organizational charts. In most agencies, security is relegated to someone in the information services (IS) department, who usually has many other duties. In the ideal model, information security should pervade the organization. This means an information security department managed by a professional ISM. This department must be high in the management hierarchy and operate by professional standards and protocols. An effective ISM department should have the following goals:

1. Develop and maintain systems for real-time detection of running cyber-attacks.
2. Conduct ongoing educational awareness programs for all internal agencies.
3. Stay informed regarding national research and development efforts.
4. Maintain the standards and best practices of the information technology industry.
5. Maintain an intelligence system for crisis information about cyber threats.
6. Conduct aggressive investigations on all incidents relating to system attacks or data disruption.

CONCLUSION

Information operations, information warfare, and cyber-attacks are twenty-first-century concerns. Now, information operations have been added as a fourth battle space. Information operations are a large part of the nation's critical infrastructure, which consists of the financial systems, transportation systems, utility systems, and communications systems.

The public safety infrastructure includes components that are essential to public safety operations and includes 911 communications, computer-aided dispatch, informational databases, geo-based information systems, and electronic mail. All of these systems are based on software and electronic data systems and must be protected from intrusion and data corruption. The disruption of these systems inhibits emergency response capabilities and causes death and injury. Electronic data has a high degree of trust. Response agencies must recognize that this trusted data is decision-making material that is vulnerable. Tactical decision makers should be trained to perform reality checks on suspicious data and maintain low technology sources of backup information.. Stored data on disks and tapes should be protected from theft and /or tampering. Office design that prevents unescorted entry, and includes electronic entry control and security badge identification is one method of securing sensitive data. Presently, there are no national standards for critical data protection and security. There must be national standards, developed by public/ private partnerships that address data storage procedures, real-time detection of running system attacks, system restoration, physical security protocols, and information technology training standards. Protection of response data and tactical information often conflicts with public records laws. For example, community legislation requires that all citizens have access to information on the storage and transportation of hazardous materials. The public safety community, through the legislative process, must initiate a concentrated effort to protect information that makes the community vulnerable to attack.