Information Security
Education & Awareness
Project Phase - II

Cyber Terrorism,

- The ethical dimension of cyber crimes & psychology

Ch A S Murty, Associate Director,
Centre for Development of Advanced Computing (C-DAC)

Disclaimer

- This presentation is for educational and research purpose only
- Do not attempt to violate the law with anything we discussed here
- Neither the author of this material / references nor anyone else affiliated anyway, is liable for your actions

Cyberspace

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

-- A Definition of Cyberspace

Defining Cyber

Cyberspace is the connected Internet Ecosystem

- Trends Exposing critical infrastructure to increased risk:
  - Interconnectedness of Sectors
  - Proliferation of exposure points
  - Concentration of Assets

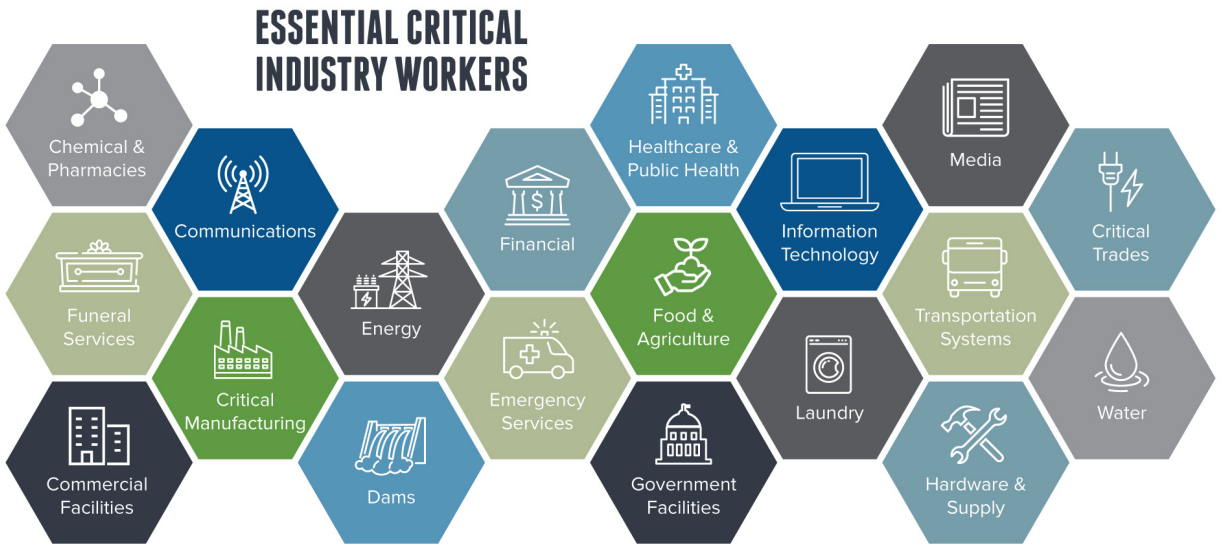
- Cyber Intrusions and Attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy

- Cyber Security is protecting our cyber space (critical infrastructure) from attack, damage, misuse and economic espionage

- Food & Technology
- Commercial Facilities
- Dams
- Energy
- Postal and Shipping
- Banking and Finance
- IT & Communication
- Defense Industrial Base
- National Monuments
- Transportation
- Chemical
- Critical Manufacturing
- Healthcare & Public Health
- Nuclear Reactors
- Water etc.,

Critical Information Infrastructures

- Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy.
- Most commonly associated with the term are facilities for:
  - Amateurs hack systems, professionals hack people. — Bruce Schneier
  - Don’t assume that you’re not a target. Draw up battle plans.
  - Learn from the mistakes of others



Cyber Challenges

- Cyberspace has **inherent vulnerabilities** that cannot be removed
- **Innumerable entry points** to Internet.
- **Assigning attribution:** Internet technology makes it relatively easy to misdirect attribution to other parties
- Computer Network Defense **techniques, tactics and practices** largely protect individual systems and networks rather than critical operations (missions)
- Attack technology **outpacing** defense technology
- Nation states, non-state actors, and individuals are at a peer level, all capable of waging attacks

Cyber Crime: Goal, Profile, Targets

Goals	Profile	Target and Motive
Money	State-Sponsored	Corporate
Power	Non-State	Defacement, Takeover / control
Control	Insiders	Financial , Extortion, Revenge
Publicity	Hactivists	Information / Data Theft
Revenge	Organized Gangs	Reputation Damage
Crackers	Criminals	Individual/Personal -
Learning	Hobbyists,	Yours and Family – entire life
Strategic	Learners and	Stalking, Blackmail, Scams
Espionage	Enthusiasts	Governmental / Military Secrets, Weapon Control
		Political, Religious, National unrest

CYBER ESPIONAGE -METHODS OF SPREADING

- Exploitation of vulnerabilities commonly software products, such as: Java ,Adobe Reader, Microsoft Office, Internet Explorer, Adobe Flash and more

- Social engineering techniques – including spear-phishing campaigns

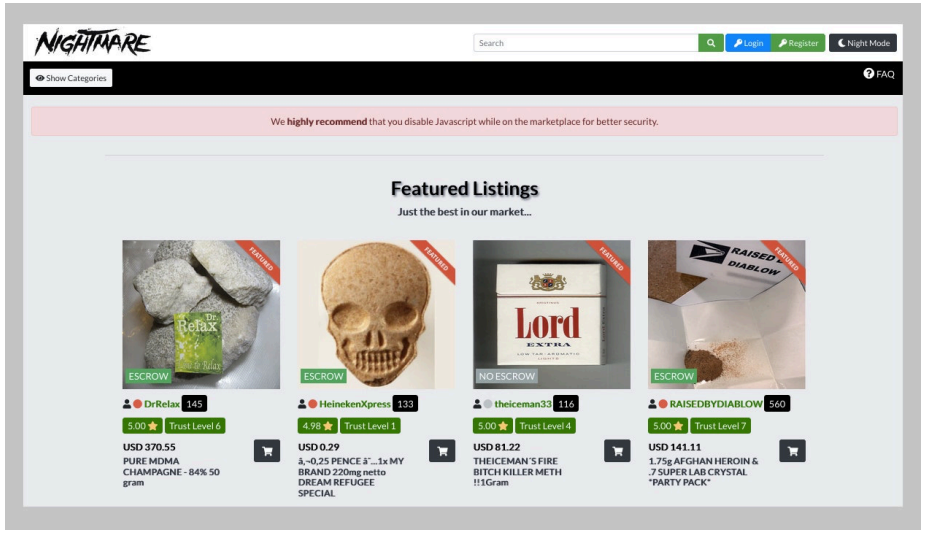
- Drive-by downloads , Droppers

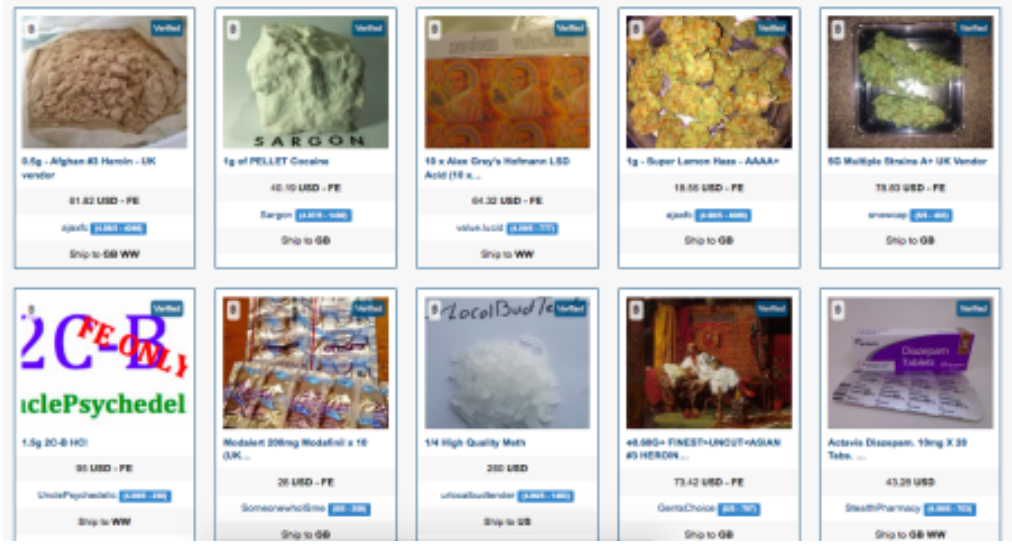
- The act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers

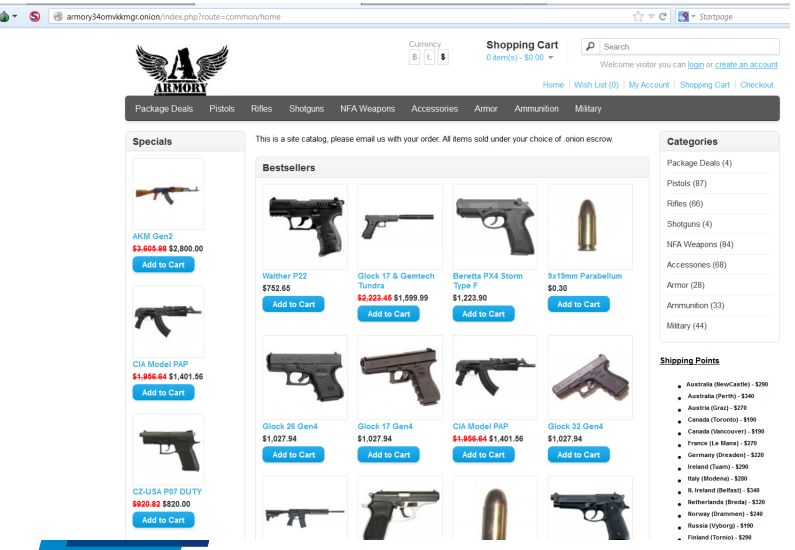
- You don’t control all of your critical business systems. Understand your vulnerabilities in the distributed, outsourced world


DARKWEBNEWS
The Ultimate Dark Web Resource
SURFACE WEB
BBC
DEEP WEB
PROPUBLICA
DARK WEB
Silk Road
Alphabay Market


DIAGRAM 1
DARK WEB SERVICES
PORNOGRAPHY
PHARMACEUTICALS
WEAPONS
BLOGS
FINANCIAL FRAUD SITES
DRUGS
FAKE DOCUMENTATION SERVICES
CARDING SITES


NIGHTMARE
Search
Login
Register
Night Mode
Show Categories
FAQ
We highly recommend that you disable Javascript while on the marketplace for better security.
Featured Listings
Just the best in our market...
ESCROW
DrRelax 145
5.00 Trust Level 6
USD 370.55
PURE MDMA CHAMPAGNE - 84% 50 gram
HeinekenXpress 133
4.98 Trust Level 1
USD 0.29
DREAM REFUGEE SPECIAL
NO ESCROW
theiceman33 116
5.00 Trust Level 4
USD 81.22
THEICEMAN`S FIRE BITCH KILLER METH !!1Gram
RAISEDBYDIABLOW 560
5.00 Trust Level 7
USD 141.11
1.75g AFGHAN HEROIN & .7 SUPER LAB CRYSTAL "PARTY PACK"


SARGON


armory34omvkkmgr.onion/index.php?route=common/home
ARMORY
Shopping Cart
Package Deals
Pistols
Rifles
Shotguns
NFA Weapons
Accessories
Armor
Ammunition
Military
Specials
Bestsellers
Categories
Shipping Points


BlackMarket Reloaded
Home
Your Account
Your Purchases
Forum
Categories
Drugs (2664)
Services (971)
Data (549)
Weapons (301)
Collectables (48)
Metals/Stones (43)
Other (338)
Software (113)
Movies (14)
Tobacco (178)
Counterfeits (124)
Ak-47, decent condition
Price
Ship from
USA, Philadelphia
Ship to
Worldwide
Stock
Created in
Last update
Your balance isn't enough to buy this item!
Please deposit the needed funds before.


BMG

Underground Cyber Market

- The Internet is where everyone has access to and where it's easy to find things because they're indexed by search engines.
- The Deep Web is the part of the Internet that isn't necessarily malicious, but is just too obscure to be indexed due to the sheer size of the web. Approx. 96 % of the internet is beyond search engines such as Google and Bing
- The Dark Web is the part of the non-indexed part of the Internet (the Deep Web) that is used by those who don't want to be found for whatever reason. This could be for seedy, illegal purposes or it could be a matter of privacy. C3 : Cyber-crime , Cyber-war , Cyber-terrorism
- Silk Road provided a platform for drug dealers around the world to sell narcotics through the Internet
  - 950,000+ registered user • Taken down Sep 2013
  - Dark market facilitated the buying & selling of stolen financial information
  - Had 2500+ members
  - Taken down in 2010 Sites like Silk Road and DarkMarket operate in the Deep Web / Dark Web offering illegal services

Cyber War

A Lot of Folks Have Substantial Misconceptions About This "Cyber War" Thing

- ❑ Cyber war is NOT about only “inadvertent” nuclear war
- ❑ Cyber war is NOT about only cyber intrusions –
- ❑ Cyber war is NOT about only defacing web sites –
- ❑ Cyber war is NOT about only DDoS attacks –
- ❑ Cyber war is NOT about only malware –
- ❑ Cyber war is NOT about only cyber-enabling regular terrorism –
- ❑ Cyber war is NOT about “high tech” war that isn't computer or network focused, nor is it about “non-technical" military information operations

- ❑ That’s all “bad stuff,” and it might be “cyber espionage,” or “cyber terrorism,” or “high tech war" or "nuclear war" or "regular war" but it’s not cyber war.

However since a lot of the impressions we have about cyber war are formed around those misconceptions, we need to start by looking at those areas

www.isea.gov.in

Data Breaches

www.cdac.in

Adobe (2013) -
150 million records

My Fitness Pal
Date: February 2018
Impact: 150 million user accounts

Adult Friend Finder (2016) –
412.2 million accounts

Equifax
Date: July 29, 2017
Impact: 147.9 million consumers

Yahoo
Date: 2013-14
Impact: 3 billion user accounts

CANVA
May 2019
Impact: 137 million user accounts

Dubsmash
Date: December 2018
Impact: 162 million user accounts

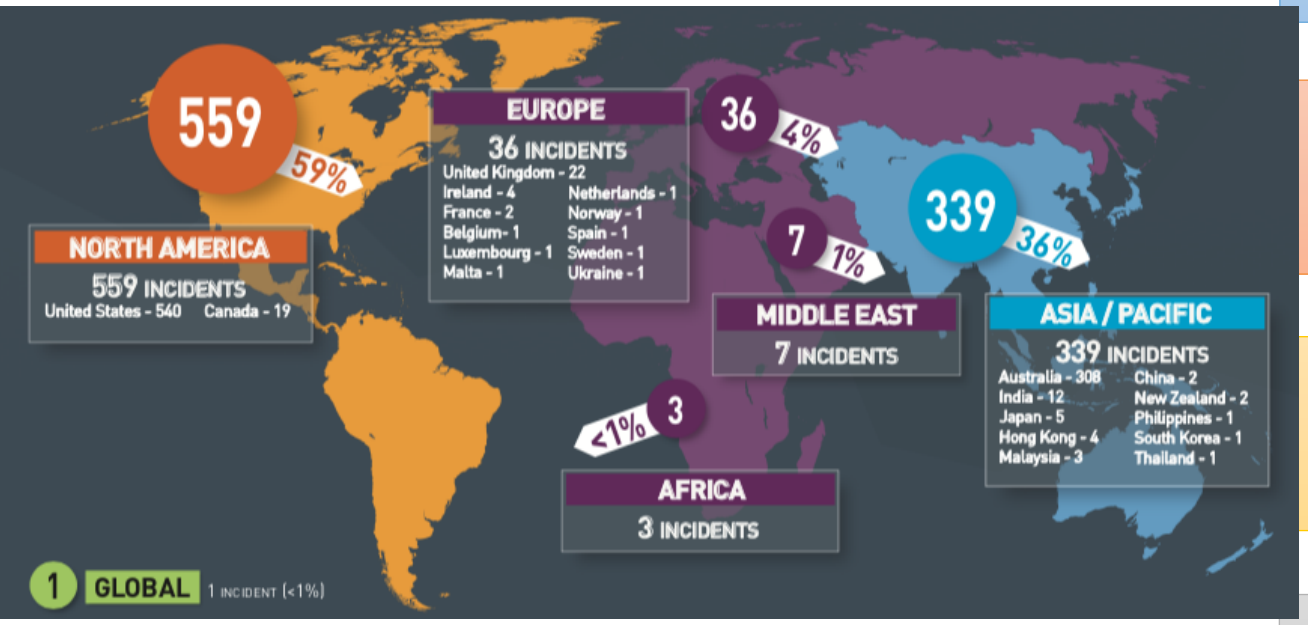
Marriott International
Date: 2014-18
Impact: 500 million customers

eBay
Date: May 2014
Impact: 145 million users

Heartland Payment Systems
Date: March 2008
Impact: 134 million credit cards exposed

Zynga
Date: September 2019
Impact: 218 million user accounts

LinkedIn
Date: 2012 (and 2016)
Impact: 165 million user accounts



Hackers steal healthcare records of 6.8 million Indian citizens

Date: August 2019

Impact: 68 lakh patient and doctor records

Local search provider JustDial exposes data of 10 crore users

Date: April 2019

Impact: personal data of 10 crore users released

SBI data breach leaks account details of millions of customers

Date: January 2019

Impact: three million text messages sent to customers divulged

Unacademy learns lesson about security

Date: May 2020

Impact: 22 million user accounts

Organized Cyber Crime

- Cyber organized criminals have engaged in a variety of cybercrimes including
  - fraud,
  - hacking,
  - malware creation and distribution,
  - DDoS attacks,
  - blackmail, and
  - intellectual property crime
    - the sale of counterfeit or
    - falsified trademarked products

- These types of cybercrimes cause
  - financial,
  - psychological,
  - economic, and even physical harm (especially counterfeit electronics and automobile parts, as well as falsified medical products, defined by the World Health Organization as "deliberately/ fraudulently misrepresent their identity, composition or source," see WHO, 2017), and
  - have been used to fund other forms of serious crime, such as terrorism

- Albanese, 2018; Europol, 2018; Broadhurst et al., 2018; Maras, 2016

- Organized criminal groups have also profited and/or otherwise benefited from illicit products and services offered online. For example, the creator of the Butterfly Bot advertised this malware online as capable of taking control of Windows and Linux computers

Five Types of Terrorism

You will need to be familiar with the five types of terrorism.

- **State-Sponsored terrorism**, which consists of terrorist acts on a state or government by a state or government.
- **Dissent terrorism**, which are terrorist groups which have rebelled against their government.
- **Terrorists and the Left and Right**, which are groups rooted in political ideology.
- **Religious terrorism**, which are terrorist groups which are extremely religiously motivated and
- **Criminal Terrorism**, which are terrorists acts used to aid in crime and criminal profit.

Cyber Terrorism: An Introduction

Cyber-crime, Info war, Net war, cyber terrorism, Cyber harassment, Virtual warfare, digital terrorism, cyber tactics, Computer Warfare, cyber attack, and cyber-break-ins is used to describe what some military and political strategists describe as the **"new terrorism"** of our times.

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner."

Ban Ki-moon,
The eighth Secretary-General of the United Nations

Cyber Terrorism: An Introduction

- Cyber terrorism is the convergence of cyberspace and terrorism.
- It refers to **unlawful attacks** and threats of attacks against computers, networks and the information stored therein when done **to intimidate** or **coerce a government** or **its people in furtherance** of political or social objectives.
- Further, to qualify as cyber terrorism, an **attack should result in violence** against persons or property, or **at least cause enough harm to generate fear**.
    - Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact.
    - Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyber terrorism Vs. Hacktivism

It is important to distinguish between cyberterrorism and “hacktivism,” a term coined by scholars to describe the marriage of hacking with political activism.

“Hacking” is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software.

Unlike hacktivists, hackers tend not to have political agendas.

Hacktivists have four main weapons at their disposal:

- Virtual blockades;
- e-mail attacks;
- Hacking and computer break-ins; and
- Computer Viruses and Worms.

Is Cyberterrorism is an attractive option?

it is cheaper than traditional terrorist methods

Cyber terrorism is more anonymous than traditional terrorist methods

The variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth

Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists

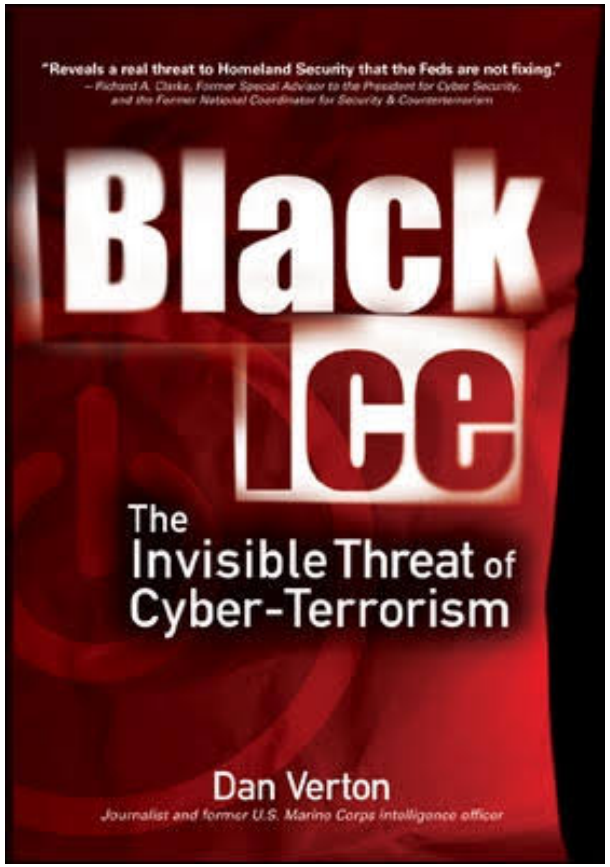
Cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods

The hackers managed to gain access to dozens of critical Pentagon computer systems

Black Ice: The Invisible Threat of Cyber-Terror, a book published in 2003

The 1997 exercise code-named "Eligible Receiver," conducted by the National Security Agency (NSA).

- The exercise began when NSA officials instructed a "Red Team" of thirty-five hackers to attempt to hack into and disrupt U.S. national security systems
- They were told to **play the part of hackers** hired by the **North Korean intelligence service**, and their primary target was to be the U.S. Pacific Command in Hawaii.
- They were allowed to penetrate any Pentagon network but were prohibited from breaking any U.S. laws
- They could only use hacking software that could be downloaded freely from the Internet



Once they entered the systems, they could easily create user accounts, delete existing accounts, reformat hard drives, scramble stored data, or shut systems down. They broke the network defenses with relative ease and did so without being traced or identified by the authorities.

In March 2000, Japan's Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult,

the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6,000 more.

- At the time of the discovery, the cult had received classified tracking data on 115 vehicles.
- Further, the cult had developed software for at least 80 Japanese firms and 10 government agencies. They had worked as subcontractors to other firms, making it almost impossible for the organizations to know who was developing the software.
- As subcontractors, the cult could have installed Trojan horses to launch or facilitate cyber terrorist attacks at a later date.

32°C M/SUNNY
TOKYO (5 p.m.)
MARKETS 106.14 ¥/$ (4 p.m.)

the japan times

NEWS | OPINION | LIFE | COMMUNITY

NATIONAL | ASIA PACIFIC | BUSINESS | WORLD | REFERENCE | COLUMNS

NATIONAL

Agencies examine software supplied by Aum-linked firms

SHARE Mar 2, 2000

Government agencies and major companies opted to double check various computer systems Wednesday after it was discovered that some of the the software may have been developed by a firm controlled by Aum Shinrikyo.

A Ground Self-Defense Force communications system was not put into scheduled operation Wednesday after it was revealed that the firewall of the software in question was made penetrable in its development stage.

Member firms of the Nippon Telegraph and Telephone Corp. group have announced that they will stop using computer-system software allegedly developed by firms linked to the Aum Shinrikyo cult if the reports are confirmed, NTT said Wednesday.

"Should we find such software . . . as a result of checks, we will replace it," NTT President Junichiro Miyazu told a news conference.

Four NTT group companies reportedly placed a total of 10 orders for computer systems with software development companies linked to the cult.

As a general rule, NTT "follows a policy of allowing developers to supply, as long as we find they conform to our technological specifications and are cheap," Miyazu said.

Black Out Day

- It was first cyber war at “New York” city on 14th,August, 2003
  - Real incidents that horribly suffered New York for 3 days
  - The hacker attacks on power lines
  - Before 3 days some one some where realize the virus named as “ BLASTER” and it a self active
  - 100 power plants are shut down × By the incident effects on whole traffic ,air line power ,water system & nuclear reactor too
  - New York government struggled 3 months to find the accused

That was Russian government is totally responsibility to this act

Cyber Terrorism

www.isea.gov.in

www.cdac.in

- 9/11 Twin Towers Attack

- Al-Qaeda laptop was found in Afghanistan.
- Hits on web sites that contained “Sabotage Handbook”.
  - Al-Qaeda actively researched publicly available information concerning critical infrastructures posted on web sites.

Ahmedabad Bomb Blast(26-07-2008)

- A mail with id alarbi_gujrat@ yahoo.com was being sent by a group of Terrorists.
- Person named Kenneth Haywood’s unsecured WIFI router in his house was being misused by terrorists.
- 3 more mails were sent after the blast with the same misuse of unsecured WIFI routers.

- 26/11 Mumbai Attack

- Terrorists communicated with handlers in Pakistan through Callphone using VoIP (Voice over Internet Protocol).

- The accused communicated to terrorists with an email id Kharak_telco@yahoo.com which was accessed from 10 different IP addresses

Cyber Space Role

Since the late 1980s, the Internet has proven to be a highly dynamic means of communication, reaching an ever-growing audience worldwide

Internet technology makes it easy for an individual to communicate with relative anonymity, quickly and effectively across borders, to an almost limitless audience

The development of increasingly sophisticated technologies has created a network with a truly global reach, and relatively low barriers to entry.

The benefits of Internet technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognized as a fundamental

It must also be recognized,

However, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism.

The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism.

Cyber Terrorism in India ???

ECIL(Electronic Corporation of India Limited) which was invented electro voting system in India , controlling parliament security system , Nuclear plants ,Defense etc.

- ECIL CYBER website was hacked by Phrozenmyst
- Not only ECIL and also ISRO ,BARC
- The hacker Phrozenmyst was stolen sensitive data from ECIL and pasted on PAGEBIN website
- Due to they are making some illegal tenders and he tweet on his tweeter account
- rom 2010 to Pakistan and china attacking the India by cyber
- Recently Pakistan is made a successfully attack on India by an fake currency at elections time

Cyber Attacks on India are Increasing with Rapid Growth of 200%+ /Year.

- Hack Your Life ultimately ~ Hack your nation
- CYBERCRIME - When a Cyber-attack is use to Steal Money HACTIVISM When one uses Cyber-attack to promote Political Agendas
- CYBER ESPIONAGE - When Cyber-attack is used to steal Specific Information
- CYBER WARFARE When Cyber-attack is used to form terrorism against Govt. ,Nation

Means by which Cyber Space is utilized for terrorist purposes

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- ***Propaganda*** (including recruitment, radicalization and incitement to terrorism);
- ***Financing;***
- ***Training;***
- ***Planning*** (including through secret communication and open-source information);
- ***Execution;*** and
- ***Cyberattacks***.

- **Propaganda generally takes the form of multimedia communications providing**
  - **ideological or Practical instruction,**
  - **Explanations,**
  - **justifications or**
  - **Promotion of Terrorist Activities.**
- These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers.
- intended and likely to incite acts of violence against individuals or specific groups of individuals
- **The promotion of violence is a common theme in terrorism-related propaganda.**

Means by which Cyber Space is utilized for terrorist purposes

The Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- ***Propaganda*** (including recruitment, radicalization and incitement to terrorism);
- ***Financing;***
- ***Training;***
- ***Planning*** (including through secret communication and open-source information);
- ***Execution;*** and
- ***Cyberattacks***.

Terrorist organizations and supporters may also use the Internet to finance acts of terrorism.

Direct Solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations.

Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud.

the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. 1400 credit cards – 1.6 million pounds of illicit funds

Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purpose

Established shell corporations, disguised as philanthropic undertakings, to solicit online donations

Means by which Cyber Space is utilized for terrorist purposes

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- ***Propaganda*** (including recruitment, radicalization and incitement to terrorism);
- ***Financing;***
- ***Training;***
- ***Planning*** (including through secret communication and open-source information);
- ***Execution;*** and
- ***Cyberattacks***.

In recent years, terrorist organizations have increasingly turned to the Internet as an alternative training ground for terrorists.

Growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice

Inspire is an online magazine allegedly published by Al-Qaida in the Arabian Peninsula with the stated objective of enabling Muslims to train for jihad at home

The fall 2010 edition included practical instructional material on how to adapt a four-wheel-drive vehicle to carry out an attack on members of the public

Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications

Means by which Cyber Space is utilized for terrorist purposes

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- ***Propaganda*** (including recruitment, radicalization and incitement to terrorism);
- ***Financing;***
- ***Training;***
- ***Planning*** (including through secret communication and open-source information);
- ***Execution;*** and
- ***Cyberattacks***.

criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology

from France, Public Prosecutor v. Hicheur,15 illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications

Steps may also be taken via the Internet to identify a potential target of an attack and the most effective means of achieving the terrorist purpose

Preparatory secret communication

A simple online e-mail account may be used by terrorists for electronic, or virtual, "dead dropping" of communications

Encryption tools and anonymzing software are readily available

Organizations and individuals often publish extensive amounts of information on the Internet.

individuals also publish, voluntarily or inadvertently, an unprecedented amount of sensitive information on the Internet

Means by which Cyber Space is utilized for terrorist purposes

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- ***Propaganda*** (including recruitment, radicalization and incitement to terrorism);
- ***Financing;***
- ***Training;***
- ***Planning*** (including through secret communication and open-source information);
- ***Execution;*** and
- ***Cyberattacks***.

explicit threats of violence, including in relation to the use of weapons, may be disseminated via the Internet to induce anxiety, fear or panic in a population or subset of the population

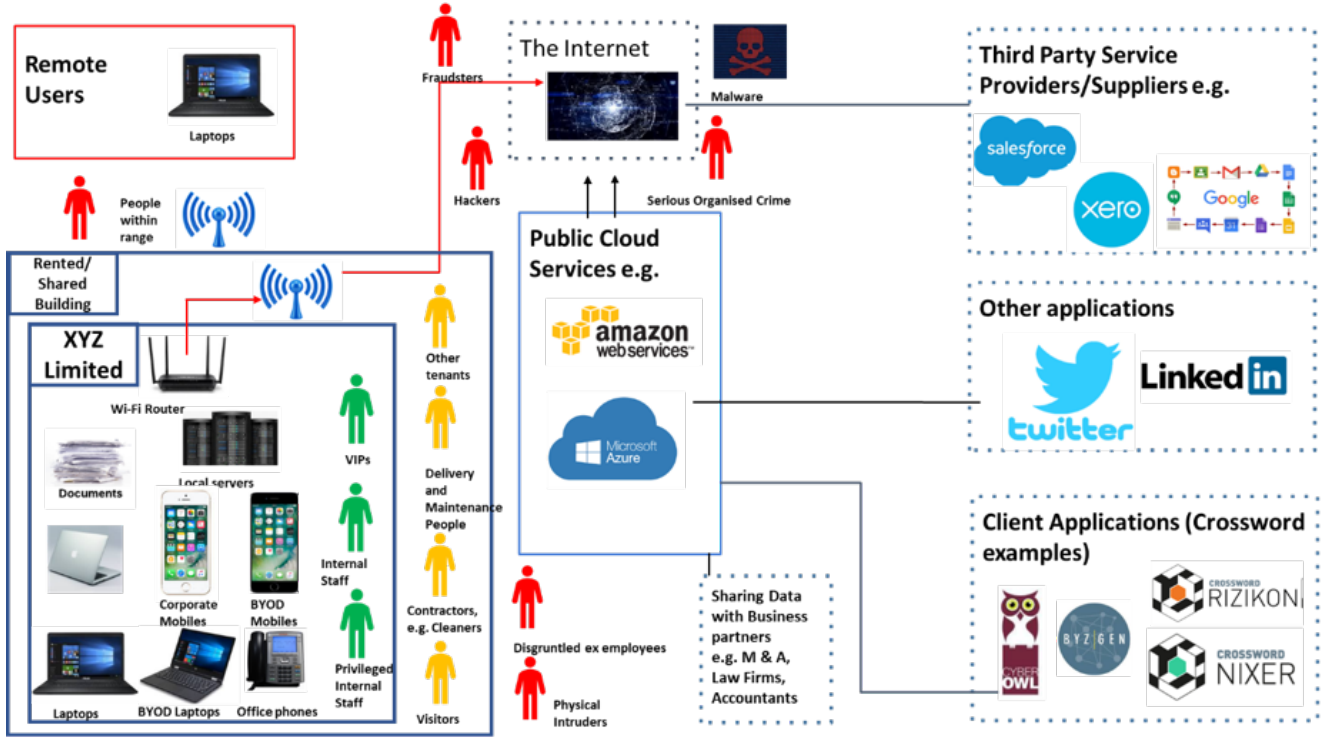
Internet communications may also be used as a means to communicate with potential victims or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the attacks of 11 September 2001 in the United States

The use of the Internet in furtherance of the execution of acts of terrorism may, inter alia, offer logistical advantages, reduce the likelihood of detection or obscure the identity of responsible parties

Terrorists may purchase individual components or services required to perpetrate violent acts of terrorism by means of electronic commerce

How does Cyber Terrorism affect you and your future?

- Air traffic control towers or our airlines infrastructure could be hacked into.
- Banking systems could be violated and all of our money could be stolen.
- Bombs and other explosives could be set off by remote.
- Hospitals could lose all of their information.
- Learn Government secrets and plans
- The tampering of our water systems.



Cyber security countermeasures to combat cyber terrorism
L. Mackinnon, L. Bacon, +3 authors D. Frangiskatos

Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes
Michael L. Gross, Daphna Canetti, Dana R. Vashdi

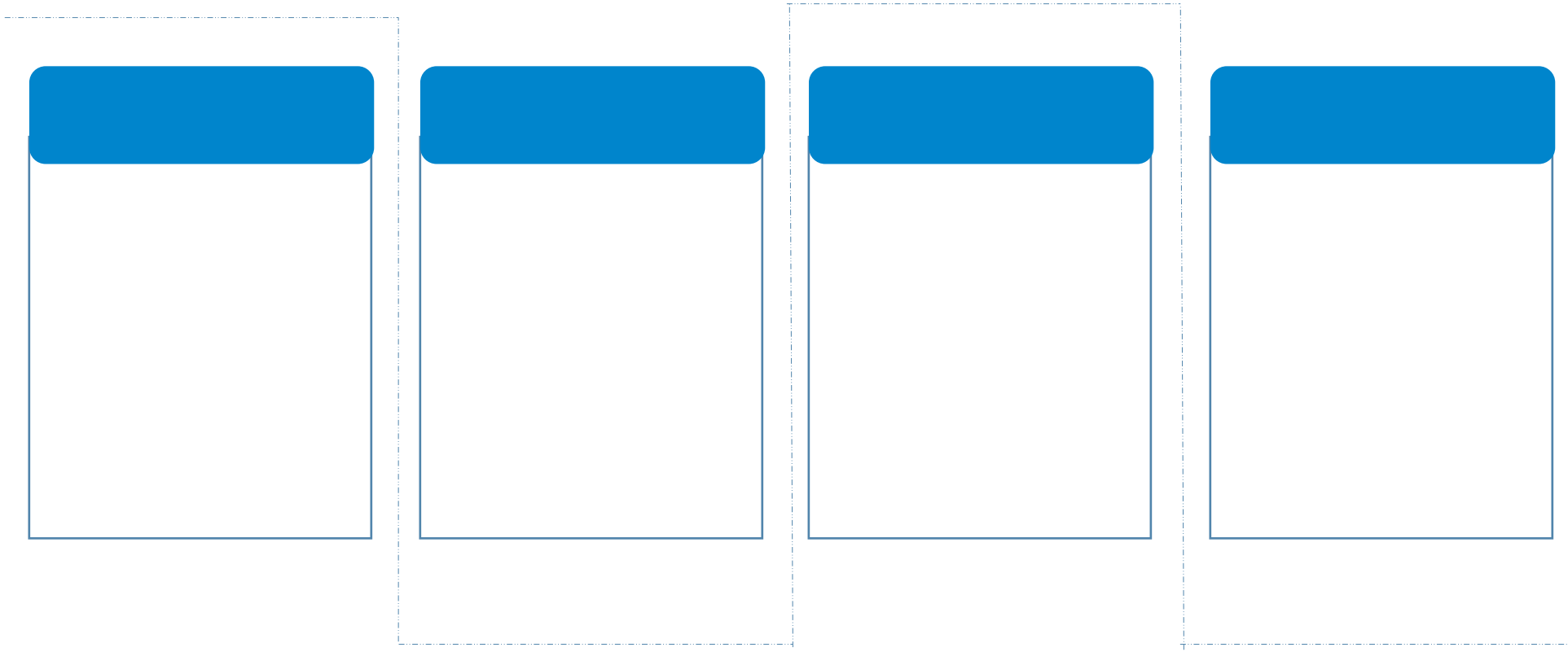
Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes (March 2016) - Michael L GrossDaphna CanettiDana Vashdi

What do we need to do??

- Maintain high alert & vigilance.
- Update OS and applications regularly.
- Enforce strong passwords.
- “Lock down" systems.
- Keep anti-virus software installed and up-to- date.
- Employ intrusion detection systems and firewalls.
- Prevention & Protection:
  - Be cautious about opening email attachments.
  - Complete Software Updates
  - Create difficult passwords
  - Download updated anti-virus software
  - Uninstall unused applications or services

References

- https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
- https://www.cisa.gov/cyber-storm-vi
- https://www.usip.org/sites/default/files/sr119.pdf
- https://www.slideshare.net/Deepakniit14/c3-11-sep
- https://www.slideshare.net/tejesh002/cyber-terrorism-36520078



www.isea.gov.in

www.
InfoSec
awareness.in

www.isea.gov.in

www.InfoSec awareness.in