Computational Red Teaming and Cyber Challenges

Prof. Hussein A. Abbass
FACS, AFAIM, SMIEEE

Defence and Security Applications Research Centre
University of New South Wales
Australian Defence Force Academy
Canberra
Content

- Computational Red Teaming
- Cyber Challenges
  - Cyber Crime
  - Cyber Terrorism
  - Cyber ....
Part 1
Computational Red Teaming
Creating a secure system is **Innovation**

Finding vulnerabilities in a secure system is **Creativity**
Playing the Devil: Red Teaming [Mason, 1969]

Create a team of people charged with defeating our forces and strategies, perhaps by adopting strategies toward which our adversaries would be more inclined for strategic, cultural, economic, and military reasons.
• Red Teaming
  - Discover vulnerabilities in blue by playing “devil’s advocate”
  - Reveal systematic loopholes in decision making processes on strategic, tactical and operational level
  - The art of ethical attacks
  - The practice of viewing a problem from an adversary or competitor’s perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary’s preferences and strategies or by simply acting as a devil’s advocate. Red teeming may be more or less structured, and a wide range of approaches exists [Source: Red Team Journal]
Military Adaptation of Red Teaming

Kevin Benson

November 14, 2007

Operations supporting the Global War on Terrorism and analysis of future complex operational environments confirm that the Army requires a capability, a "red team," within its units to aid the commander and staff to identify and quickly adapt to new and unanticipated challenges and opportunities. Historically the military, government and industry have employed some form of Red Teaming; however, there has been no formal education or training program nor common red teaming doctrine, methodologies, or framework.

US Army Training and Doctrine Command (TRADOC) established the University of Foreign Military and Cultural Studies (UFMCS) at Fort Leavenworth, Kansas to provide the educational and training foundation to support the fielding of an Army-wide red team capability. The curriculum is designed to enable Red Teams to support decision making during planning and operations. Red teams identify potential weaknesses, vulnerabilities and unseen opportunities. Red teams also anticipate and account for the perceptions of partners, adversaries and others in our planning, and conduct independent and unbiased critical reviews and analysis of such items as concepts and experiments.

Red teams provide commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of the operational environment. They do this from the perspectives of our partners, adversaries, and others. Red Teaming is a function executed by trained and educated officers, senior non-commissioned officers, and civilians to enhance staff planning and improve decision making in today’s dynamic and uncertain environment.

In 2008, UFMCS projects to reach full operational capability to meet the education and training requirements to fill requirements for the Army's operating force. In the near term the Army and TRADOC will continue to institutionalize the concept of Red Teaming by adding Red Teams to existing force structure, adding the concept to doctrine, refining techniques and procedures, and continuing formal UFMCS conducted education and training programs at Fort Leavenworth and at unit locations.

UFMCS recommended teams of trained personnel be added to every echelon of command from the Brigade Combat Team through Army headquarters. Based on this recommendation, the Army approved the addition of a Red Team to division and corps headquarters. Beginning in 2008, we anticipate that two officers assigned to the brigade combat team headquarters will receive Red Team education and training at UFMCS. UFMCS will continue to develop and refine best practices, techniques and procedures sharing these using an established reachback capability. This reachback capability provides access to subject matter experts, databases, and serves as a means to exchange lessons learned.
Computational Red Teaming (CRT)

- A set of computational models to support the red teaming exercise
- Red teaming in Silico
- A framework for assessing system-level vulnerabilities by adopting computational intelligence techniques
The History of CRT

Computational Red Teaming: From Environment Change to Defence and ... File Format: PDF/Adobe Acrobat - View
In this presentation, I will present computational red teaming - a framework for ...
computational red teaming in a variety of contexts ranging from ...
www.griffith.edu.au/__data/assets/pdf_file/0007/june15_seminar.pdf - Similar

Griffith University IIIS Seminar: Computational Red Teaming...
11 Jun 2009 ... In this presentation, I will present computational red teaming - a framework for assessing system-level vulnerabilities by adopting ...
www3.griffith.edu.au/03/events/view.php?eventID=9634 - Cached - Similar

Automated red teaming
Automated red teaming: a proposed framework for military application. Full text, Pdf (360 KB).
Source, Genetic And Evolutionary Computation Conference ...
portal.acm.org/citation.cfm?id=1277345 - Similar
by CS Choo - 2007 - Cited by 4 - Related articles - All 5 versions

Characterizing Warfare in Red Team ing
Characterization can be defined in terms of maximizing damage in the red team while minimizing damage in ...
explore.ieee.org/iel5/3477/33735/01605376.pdf - Similar
by A Yang - 2006 - Cited by 7 - Related articles
Characterizing Warfare in Red Teaming
Ang Yang, Hussein A. Abbass, Senior Member, IEEE, and Ruhul Sarker, Member, IEEE

Automated red teaming: a proposed framework for military application
Full text

Source
Genetic And Evolutionary Computation Conference archive
Proceedings of the 9th annual conference on Genetic and evolutionary computation table of contents
London, England
SESSION: Real-world applications: papers table of contents
Pages: 1936 - 1942
Year of Publication: 2007
ISBN: 978-1-4244-0874-4

Authors
Chwee Song Choo DSO National Laboratories, Singapore, Singapore
Ching Lian Chua DSO National Laboratories, Singapore, Singapore
Su-Han Victor Tay Defence Science and Technology Agency, Singapore, Singapore

Sponsors
SIGEVO: ACM Special Interest Group on Genetic and Evolutionary Computation
ACM: Association for Computing Machinery

Publisher
ACM New York, NY, USA
Research Aims

• Establishing Red Teaming as a Science
  – Structuring the process
  – Generalising the lessons

• Identifying the Building Blocks for a CRT system

• Undertaking **fundamental research** to reach an effective CRT system by filling the gap in our knowledge base
The CRT Framework

<table>
<thead>
<tr>
<th></th>
<th>Blue</th>
<th>Red</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immune System</td>
<td>Self</td>
<td>Non-self</td>
<td>Body</td>
</tr>
<tr>
<td>Market strategy</td>
<td>Us</td>
<td>Competitors</td>
<td>The market</td>
</tr>
<tr>
<td>Defence Planning</td>
<td>Our planning</td>
<td>Our enemy planning</td>
<td>The international environment</td>
</tr>
<tr>
<td>Future technology</td>
<td>The technology</td>
<td>Other technologies</td>
<td>The market</td>
</tr>
<tr>
<td>An algorithm</td>
<td>The algorithm</td>
<td>Problem instances</td>
<td>????????????</td>
</tr>
</tbody>
</table>
# The CRT Framework

## Bringing the environment within

<table>
<thead>
<tr>
<th></th>
<th>Blue</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immune System</td>
<td>Self</td>
<td>Non-self and Body</td>
</tr>
<tr>
<td>Market strategy</td>
<td>Us</td>
<td>Competitors and the market</td>
</tr>
<tr>
<td>Defence Planning</td>
<td>Our planning</td>
<td>Our enemy planning and the international environment</td>
</tr>
<tr>
<td>Future technology</td>
<td>The technology</td>
<td>Other technologies and the associated market</td>
</tr>
<tr>
<td>An algorithm</td>
<td>The algorithm</td>
<td>Problem instances</td>
</tr>
</tbody>
</table>
Red in CRT is any entity that affects Blue’s decision
# The CRT Framework

<table>
<thead>
<tr>
<th>Blue</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>Fixed</td>
</tr>
<tr>
<td>Vary</td>
<td>Fixed</td>
</tr>
<tr>
<td>Fixed</td>
<td>Vary</td>
</tr>
<tr>
<td>Vary</td>
<td>Vary</td>
</tr>
</tbody>
</table>
The Computational Challenge

- It looks like everything we do but doing it reveals that it is nothing like anything we did!
- Search is done on a different topological structure
- Every assumption in the modelling is a source of vulnerability!
- Combinatorial explosion of possibilities
- Detecting dynamics is different from modelling dynamics
- Human encoded noise violates the key assumption in almost all models that are robust against noise!
- The mind-shift from predicting failure and optimization to understanding vulnerabilities
The CRT Framework

Blue
- Measures of Performance
- Intelligence
- Decision Making and Planning
- Reflection

Red
- Measures of Performance
- Intelligence
- Decision Making and Planning
- Reflection

Synthesized Simulation Environments

Scenario Generation
Part 2
Cyber Challenges
The commander must work in a medium which his eyes cannot see, which his best deductive powers cannot always fathom; and which, because of constant changes, he can rarely be familiar.

Carl von Clausewitz
Military Strategist
1780-1831
Cyber Warfare
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.

US Department of Defense (DOD)
Cyber warfare is the sub-set of information warfare that involves actions taken within the cyber world. The cyber world is any virtual-reality contained within a collection of computers and networks. There are many cyber worlds, but the one most relevant to cyber-warfare is the Internet and related networks that share media with the Internet.
Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.

Dr. Ivan Goldberg
Director of the Institute for the Advanced Study of Information Warfare (IASIW).
Principles of Cyber Warfare

- Cyber Warfare (CW) must have real world effects to be meaningful
- An adversary can hide in cyber-world by taking active steps such as using normal activity to carryout an attack
- Cyber-world is unpredictable, inconsistent and unreliable
- Sub-parts of cyber-world are controlled by attackers and defenders. The uncontrolled spaces are vulnerable
- There are no spatio-temporal limitations in carrying out the attacks
Cyber Crime
Statute and treaty law both refer to cybercrime. In Australia, cybercrime has a narrow statutory meaning as used in the Cybercrime Act 2001 (Cwlth), which details offences against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe’s Convention on Cybercrime (EST no. 185), cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences and copyright offences. This wide definition of cybercrime overlaps in part with general offence categories that need not be ICT dependent, such as white-collar crime and economic crime as described by Grabosky and Sutton (1989).
Cyber Crime

February 21, 2000

Cyber crime is becoming one of the Net's growth businesses. The recent spate of attacks that gummed up Web sites for hours--known as "denial of service"--is only one type. Today, criminals are doing everything from stealing intellectual property and committing fraud to unleashing viruses and committing acts of cyber terrorism in which political groups or unfriendly governments nab crucial information. Indeed, the tactic used to create mayhem in the past few days is actually one of the more innocuous ones. Cyber thieves have at their fingertips a dozen dangerous tools, from scans that ferret out weaknesses in Web site software programs to sniffers that snatch passwords. All told, the FBI estimates computer losses at up to $10 billion a year.
Cyber Crime

- Cyber crimes can be categorised in different ways
  - Type of criminals
    - professionals, juvenile, Insiders, Intruders ...
  - Intent or motive of crime
    - mere bragging, fame, financial gain, revenge ...
  - Type of target (victim)
    - individuals, organisations, hardware, software, industry ...
- By no means exhaustive, some of the cyber crime are highlighted in the following slides
Cyber Crime – Intrusions

• Generally refers to illegitimate breaking-in to the computing resources

• Most prevalent cyber crime and a major source nuisance for security managers

• Sophistication of intrusions depends on individual skill level

NEWS RELEASE

For Immediate Distribution

February 11, 2008

Thomas P. O’Brien
United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
(213) 894-6947
thom.mrozek@usdoj.gov
www.usdoj.gov/usa/cno

YOUNG ‘BOTHERDER’ PLEADS GUILTY TO INFECTING MILITARY COMPUTERS AND FRAUDULENTLY INSTALLING ADWARE

A well-known juvenile member of the “botnet underground” pleaded guilty this afternoon to delinquency charges related to his use of “botnets” – armies of compromised computers – to surreptitiously install adware on computers, including military computers.
Cyber Crime – Intrusions

- Botnets
- Trojan Horses
- Worms
- Viruses
- Spyware
- Malware
- Hacking
Major Cybercrime Busts Take Place In Romania

Major bank fraud ring broken up; alleged NASA hacker faces charges

Mar 13, 2009 | 04:13 PM

By Tim Wilson

DarkReading

The Romanian police had a busy Wednesday, breaking up a major bank fraud ring and arresting another individual who is accused of breaking into major U.S. government and university servers.

According to news reports, the Romanian police, working along with the FBI, arrested 20 individuals who allegedly built cloned bank sites and then drained the accounts of users who were lured into logging in to them.

The cloned sites, which were deployed in Italy and Spain, looked and operated like the actual bank Websites, but they asked users questions that ultimately led to the divulging of personal bank details, according to Stefan Negriu, chief of the Romanian Police’s organized crime division. Once obtained, the hackers allegedly used that information to access the real bank Websites and transfer or withdraw cash.

Nearly 100 police officers from special troops entered suspects’ houses in major cities across Romania, the reports said. Investigators said the ring stole at least 350,000 euros.

In a separate case, police also arrested a Romanian resident accused of hacking into several U.S. government servers -- including NASA’s -- and multiple university servers. The hacker had set up several servers in the United States, which he controlled from Romania and used to carry out the hacks, according to reports.

The hacks on NASA alone cost the space agency some $5 million, according to news reports. The accused attacker, Victor Faur, has previously been accused of breaking into computers at the U.S. Navy and Department of Energy between 2005 and 2009.
Cyber Crime – Identity Theft

Stolen: Google's employee records

By Brendan Chase, ZDNet.com.au
July 03, 2008

Google has confirmed that personal data of US employees hired prior to 2006 have been stolen in a recent burglary.

Records kept at Colt Express Outsourcing Services, an external company Google and other companies use to handle human resources functions, were stolen in a burglary on 26 May. An undisclosed number of employees' details and those of dependents such as names, addresses, and social security numbers were on the stolen computers. It is understood that Colt did not employ encryption to protect the information.

It's still unclear how many more of Colt Express' clients were affected by the breach. CNET Networks (publisher of ZDNet.com.au and Builder AU) was another company affected by the burglary with around 6,500 employee's details stolen.

Although there is no evidence of misuse of the data to date, the information obtained could be used by ID thieves to create fake accounts and identities.

It's only come to light now that Google was one of the companies affected. Google itself was not burglarised, nor was any of its internal systems compromised.

Danny Torpe, former chief scientist at Borland and engineer at Google who now works for Microsoft, was informed of the theft on 1 July.

I've just received a letter from Google that personal data of Google employees hired prior to 31 December, 2005 may have been stolen in the 26 May burglary of Colt Express Outsourcing Services. No credit card numbers were in the stolen data, just names, addresses, SSNs(Social Security Numbers) — all the info needed for a thief to open new

Internet 100%
Phishers get more wily as cybercrime grows

By Diane Bartz

WASHINGTON (Reuters) - Phishing scams have grown up from the unsophisticated swindles of the past in which fake Nigerian princes e-mailed victims, who would get a big windfall if they just provide their bank account number.

Even as authorities try to stamp out that con and other e-mail and online scams, scammers are getting more wily and finding new loopholes to exploit.

The vast majority of e-mail is spam and an unknown percentage of that is meant to defraud. The scale of electronic fraud means that the criminals can make huge profits even if only a small percentage of people are duped.

Phishing commonly refers to hoax e-mails purportedly from banks or other trustworthy sources that seek to trick recipients into revealing bank or credit card account numbers and passwords.

The U.S. government scored a big victory in November when the web hosting company McColo Corp. was taken offline. Estimates vary, but the Washington Post said that 75 percent of spam worldwide had been sent through that single company.
Cyber Crime Cell arrest one for extortion over web

Express News Service Posted online: Monday, Oct 13, 2008 at 0257 hrs

Chandigarh, October 12: Cyber Crime Investigation Cell of the Chandigarh Police today arrested one Puja Negi, for involvement in an “extortion through the Web” racket.

Police said one of the accused, posing as Shelly, met and chatted with complainant Manjit Singh (name changed) of Chandigarh online on October 1 this year. During the conversation, the complainant disclosed personal information, which the accused later used to blackmail the victim over the phone, saying she would disclose their relationship to his parents if he did not fulfill her demands.

"The complainant parted with valuables like his mobile phone, a Play Station 3, a webcam, a wrist watch, sunglasses and recharge coupons worth Rs 4,500. Another of the accused collected the items from the complainant.

Police said the accused demanded another mobile phone and more recharge coupons from the victim and asked him to wait with the items near Airtel Mobile Buzz, Zulu in Sector 17-E. The victim then reported the matter to the Cyber Crime Investigation Cell, who arrested the accused from the designated spot. The girl, is a resident of Sector 39, Chandigarh."
Man Sentenced for Internet Harassment

South Carolina Man Sentenced In First Federal Prosecution Of Internet Harassment

From Federal Bureau of Investigations, for About.com

James Robert Murphy, 38, of Columbia, South Carolina, was sentenced to 5 years of probation, 500 hours of community service, and more than $12,000 in restitution today for two counts of Use of a Telecommunications Device (the internet) with Intent to Annoy, Abuse, Threaten or Harass.

Murphy was indicted in April 2004, for sending harassing emails to Seattle resident Joelle Ligon and to other employees of the City of Seattle. He pleaded guilty to two counts in June 2004. In sentencing Murphy, U.S. District Court Judge Thomas Zilly told Murphy he “…did not demonstrate the type of remorse he should under the circumstances.”

In his plea agreement, Murphy admitted he had a sporadic romantic relationship with Ligon from 1984-1990. In May of 2002, Murphy began sending dozens of uninvited and harassing emails and facsimile (fax) messages to Ligon and her co-workers. Murphy hid his identity with special email programs and created the “Anti Joelle Fan Club” (AJFC) and repeatedly sent threatening emails from this alleged group.

Murphy disseminated false information about Ligon’s background to her co-workers. The harassment escalated over time, with Murphy sending pornographic material and making it appear that Ligon was sending the pornographic material to her co-workers at the City of Seattle. Even after Ligon was able to identify the person harassing her and get a court order barring contact, Murphy violated the order by sending an email denying he was the harasser.

No Remorse From Murphy

In court, Murphy told the Judge what he did was “stupid, hurtful and just plain wrong. I was going through a bad patch in my life. I want to take my lumps and get on with life.”

In sentencing Murphy Judge Zilly noted that he was surprised that Murphy “made no effort to indicate your remorse to the victim, to indicate you were sorry.” The Judge noted that he had received a letter from Joelle Ligon unlike any he had ever received from a crime victim.

In it Ligon asked the Judge to impose “an effective and compassionate sentence.” Judge Zilly decided to impose 500 hours of community service instead of the 160 hours requested by the government. He ordered Murphy to pay $12,297.23 to the City of Seattle to compensate the City for 160 hours of work time lost by employees dealing with the harassment.

Task Force Targets Cyber Crime
In China, $700 puts a spammer in business
The country is home to server hosting providers that also sell ‘bullet-proof domains’ for cybercriminals

Robert McMillan (DG News Service) 11/05/2009 04:18:00
Tags: spam, cybercrime, China

It's a great deal, if you're a spammer.
You pay US$700 to use a server in China that lets you send all the spam you like. It's called bulletproof hosting, and to the people who fight spam and cybercrime it's becoming a big problem.
Cybercriminals use these services not just to host servers, but also to register Internet domain names that they use for spam and online attacks.
In a three-month period this year, researchers at the University of Alabama at Birmingham traced more than 22,300 domains, all used to send online pharmaceutical spam, to just six bulletproof computers hosted in China, said Gary Warner, director of research in computer forensics at the university.
The Waledac Trojan, which uses clever social-engineering techniques to spread itself, has been using bulletproof domain names to keep itself alive, Warner said.
Under the Spam Act 2003 it is illegal to send, or cause to be sent, unsolicited commercial electronic messages. The Act covers email, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing.

ACMA is responsible for enforcing the Spam Act and actively works to fight spam in Australia.
## Spam Statistics 2006 (TopTenREVIEWS.com)

<table>
<thead>
<tr>
<th>Category</th>
<th>Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email considered Spam</td>
<td>40% of all email</td>
</tr>
<tr>
<td>Daily Spam emails sent</td>
<td>12.4 billion</td>
</tr>
<tr>
<td>Daily Spam received per person</td>
<td>6</td>
</tr>
<tr>
<td>Annual Spam received per person</td>
<td>2,200</td>
</tr>
<tr>
<td>Spam cost to all non-corp Internet users</td>
<td>$255 million</td>
</tr>
<tr>
<td>Spam cost to all U.S. Corporations in 2002</td>
<td>$8.9 billion</td>
</tr>
<tr>
<td>States with Anti-Spam Laws</td>
<td>26</td>
</tr>
<tr>
<td>Email address changes due to Spam</td>
<td>16%</td>
</tr>
<tr>
<td>Estimated Spam increase by 2007</td>
<td>63%</td>
</tr>
<tr>
<td>Annual Spam in 1,000 employee company</td>
<td>2.1 million</td>
</tr>
<tr>
<td>Users who reply to Spam email</td>
<td>28%</td>
</tr>
<tr>
<td>Users who purchased from Spam email</td>
<td>8%</td>
</tr>
<tr>
<td>Corporate email that is considered Spam</td>
<td>15-20%</td>
</tr>
<tr>
<td>Wasted corporate time per Spam email</td>
<td>4-5 seconds</td>
</tr>
</tbody>
</table>

The University of New South Wales at the Australian Defence Force Academy
## Types of Spam (TopTenREVIEWS.com)

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products</td>
<td>25%</td>
</tr>
<tr>
<td>Financial</td>
<td>20%</td>
</tr>
<tr>
<td>Adult</td>
<td>19%</td>
</tr>
<tr>
<td>Scams</td>
<td>9%</td>
</tr>
<tr>
<td>Health</td>
<td>7%</td>
</tr>
<tr>
<td>Internet</td>
<td>7%</td>
</tr>
<tr>
<td>Leisure</td>
<td>6%</td>
</tr>
<tr>
<td>Spiritual</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>
## Cyber Crime – Spamming

### Most Annoying (TopTenREVIEWS.com)

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pornography</td>
<td>91%</td>
</tr>
<tr>
<td>Mortgage and Loans</td>
<td>78%</td>
</tr>
<tr>
<td>Investments</td>
<td>68%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>61%</td>
</tr>
<tr>
<td>Software</td>
<td>41%</td>
</tr>
<tr>
<td>Internet</td>
<td>7%</td>
</tr>
<tr>
<td>Leisure</td>
<td>6%</td>
</tr>
<tr>
<td>Spiritual</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>
Cyber Terrorism
an action or threat of action where:
(a) the action falls within subsection (2) and does not fall within subsection (2A); and
(b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and
(c) the action is done or the threat is made with the intention of:
   (i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or
   (ii) intimidating the public or a section of the public.

(2) Action falls within this subsection if it:
(a) causes serious harm that is physical harm to a person; or
(b) causes serious damage to property; or
(c) causes a person’s death; or
(d) endangers a person’s life, other than the life of the person taking the action; or
(e) creates a serious risk to the health or safety of the public or a section of the public; or
(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:
   (i) an information system; or
   (ii) a telecommunications system; or
   (iii) a financial system; or
   (iv) a system used for the delivery of essential government services; or
   (v) a system used for, or by, an essential public utility; or
   (vi) a system used for, or by, a transport system.

(2A) Action falls within this subsection if it:
(a) is advocacy, protest, dissent or industrial action; and
(b) is not intended: (i) to cause serious harm that is physical harm to a person; …
Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack 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 cyberterrorism, 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, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Dorothy Denning
Cyber Terrorism

A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Cyberterrorism: An evolving concept, 2001
Garrison, L and Grand, M.
US National Infrastructure Protection Center
Cyber Terrorism

• While an information system can be attacked in any number of ways (eg, conventional methods involving bombing, arson, etc), for an act to be classed as cyberterrorism, the attacker must use information systems or other electronic means to launch the attack (Kathryn Kerr, AusCERT, 2003)

• The actions that do not cause severe harm, loss, fear, do not fall under cyber terrorism
Cyber Terrorism

• The actions that do not cause severe harm, loss, fear, do not fall under cyber terrorism (AusCERT)
  – Secure/encrypted communications between terrorist groups
  – Electronic communications (Web, email) use to solicit support or propagate terrorism
  – Occasional cyber attacks or scanning activities carried out by terrorist groups that do not cause harm
Website Defacement

• Steps involved in website defacement process
  – Identify and exploit a vulnerability in the web server to get unauthorised access
  – Replace the contents of webpage (usually homepage) with some derogatory remarks and cracker’s ID/claimed affiliation details
  – Publicise defacement
  – Potentially achieve desired objectives
Website Defacement

# id:uname -a
uid=0(root) gid=1(other)
SunOS labourweb 5.8 Generic_108528-13 sun4u sparc SUNW,Ultra-4

Software failure. Press left mouse button to continue.
Guru Meditation #00000069.0000BABE

m'kay, woot woot you say.
where r all my server?
is in /www/htdocs/font.unhacked

UK Labour Party website defaced
Website Defacement

White House website attacked

Chinese hackers are suspected of attacking the White House website.

By BBC News Online's Kevin Anderson in Washington

President George W Bush appears to be the latest victim in an online assault by Chinese hackers, as the White House website was unavailable for several hours early Friday.

The hackers' attack was similar to ones that took CNN and Yahoo offline last year.

The White House confirmed that for two hours and 15 minutes their website was down.

A White House spokesman said "there was no security breach, and the attack is under review".
Website Defacement

• Is website defacement cyber terrorism?
  – Usually done to get publicity and instigate fear and appreciation of attacker’s skills among general public and/or victim
  – May not work (terrorise) if does not get enough attention
  – Harm is usually low and short lived
Denial Of Service (DOS)

- Purpose is to make a service unavailable to legitimate users by
  - Chocking the network bandwidth and overburden the computing resources with large volume of unsolicited traffic
  - Causing the computing resource providing the service to crash
  - Hijacking the connections and re-routing them to unintended resources
  - Physically destroying the resources
- Distributed Denial of Service (DDOS) an upgraded version that involves control of multiple attack resources
Denial Of Service (DOS)
Denial Of Service (DOS)

Coordinated Russia vs Georgia cyber attack in progress

August 11th, 2008

In the wake of the Russian-Georgian conflict, a week of speculation around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia’s Internet infrastructure. The attacks have already managed to compromise several government websites, with continuing DDOS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S. with Georgia’s Ministry of Foreign Affairs undertaking a desperate step in order to disseminate real-time information by moving to a blogspot account.

Who’s behind it? The infamous Russian Business Network, or literally every Russian supporting Russia’s actions? How coordinated and planned is the cyber attack? And do we actually have a relatively decent example of cyber warfare combining PSYOPs (psychological operations) and self-mobilization of the local Internet users by spreading “For our motherland, brothers!” or “Your country is calling you!” hacktivist messages across web forums. Let’s find out, in-depth.

The attacks originally starting to take place several weeks before the actual “intervention” with Georgia President’s website coming under DDOS attack from Russian hackers in July, followed by active discussions across the Russian web on whether or not DDOS attacks and web site defacements should in fact be taking place, which would inevitably come as a handy tool to be used against Russian from Western or Pro-Western journalists. The peak of DDOS attack and the actual defacements started taking place as of Friday;

Sponsored Links

- DSD Tech Security jobs
- Heart Disease worries?
  Complete our Free Heart Health Profiler. It only takes a few mins!
  cholesteroltest.com.au

Recent Entries

- IE users beware: Zero-day attacks hit Microsoft Video ActiveX Control
- EyeWonder malware incident affects popular web sites
- Manchester City Council pays $2.4m in Conflker clean up costs
- Michael Jackson’s death themed malware campaigns spreading
- Secunia: Average insecure program per

www.unsw.adfa.edu.au
• Is cyber terrorism a fact or a fallacy?
  – The biggest and most fundamental problem facing a potential cyber terrorist is that often they can’t rise above the normal online “noise floor”. (Joe St Sauver, Security Programs Manager, Internet2, 2008).
  – Cyber attack as a tool for terrorism has limitations (Kathryn Kerr, AusCERT 2003)
    • Terrorist are most likely uncertain about the impact of cyber attack on critical IS resources such as SCADA
    • Recovery from cyber attack is quicker
    • Attackers could well be able to cover their true identity – Plausible denial
  – Vulnerability of critical information systems to cyber attack
Cyber Espionage or Surveillance
Cyber espionage seen as growing threat to business, government

SANS Institute ranks it No. 3 on cyber menace list
By Ellen Messmer, Network World, 01/17/2008

Cyber espionage is getting renewed attention as fresh evidence emerges of online break-ins at U.S. research labs and targeted phishing against corporations and government agencies here and abroad.

It's no wonder that research firm SANS Institute has ranked cyber espionage No. 3 on its "Top Ten Cyber Menaces for 2008," just behind Web site attacks exploiting browser vulnerabilities and botnets such as the infamous Storm.

"Economic espionage will be increasingly common as nation-states use cyber theft of data to gain economic advantage in multinational deals," SANS Institute claims. "The attack of choice involves targeted spear phishing with attachments, using well-researched social engineering methods to make the victim believe that an attachment comes from a trusted source."

Alan Paller, director of research at SANS Institute, adds that people should be aware that an "extraordinary treasure chest of information has been stolen," and "the same people doing the military espionage are engaged in economic espionage using the same or very similar techniques to steal information from organizations that are working on business ventures in the attackers' country." He offered no estimate as to how much cyber espionage is costing organizations.

Top 10 cyber security menaces for 2008
The SANS Institute has drawn up its list of looming security dangers facing organizations and their information-technology defenders.
1. Increasingly sophisticated Web site attacks that exploit browser vulnerabilities.
2. Increasing sophistication and effectiveness in botnets.
3. Cyber espionage efforts by well-resourced organizations looking to extract large amounts of data, particularly using targeted phishing.
Cyber Espionage

- Cyber espionage is far less riskier than the physical espionage through hard paper documents
- Advanced computing resources such as high network bandwidth have facilitated in the access and retrieval of crucial information
  - “insiders” can take advantage
- Motives behind cyber espionage
  - Obtain competitive edge
  - Obtain personal gains (financial, political or otherwise)
  - Advance a country’s economy
The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)

By Nathan Thornburgh/Washington

It was another routine night for Shawn Carpenter. After a long day analyzing computer-network security for Sandia National Laboratories, where much of the U.S. nuclear arsenal is designed, Carpenter, 36, retreated to his ranch house in the hills overlooking Albuquerque, N.M., for a quick dinner and an early bedtime. He set his alarm for 2 a.m. Waking in the dark, he took a thermos of coffee and a pack of Nicorette gum to the cluster of computer terminals in his home office. As he had almost every night for the previous four months, he worked at his secret volunteer job until dawn, not as Shawn Carpenter, mid-level analyst, but as Spiderman—the apt nickname his military-intelligence handlers gave him—tirelessly pursuing a group of suspected Chinese cyberspies all over the world. Inside the machines, on a mission he believed the U.S. government supported, he clung unseen to the walls of their chat rooms and servers, secretly recording every move the snoopers made, passing the information to the Army and later to the FBI.

The hackers he was stalking, part of a cyberspy network that federal investigators code-named Titan Rain, first caught Carpenter’s eye a year earlier when he helped investigate a network break-in at Lockheed Martin in September 2003. A strikingly similar attack hit Sandia several months later, but it wasn’t until Carpenter compared notes with a counterpart in Army cyberintelligence that he suspected the scope of the threat. Methodical and voracious, these hackers wanted all the files they could find, and they were getting them by penetrating secure computer networks at the country’s most sensitive military bases, defense contractors and aerospace companies.

Carpenter had never seen hackers work so quickly, with such a sense of purpose. They would commandeer a hidden section of a hard drive, zip up...
Couples turn to online espionage

Fidelity check includes email, SMS and browsing history

Iain Thomson, vnunet.com 08 Apr 2008

Research undertaken at Oxford University suggests that an increasing number of people are spying on their partners online.

One in five couples admitted to reading a partner's emails or text messages, and 13 per cent examined their partner's internet browsing history. More than 2,400 individuals were questioned in the research.

Six per cent of the couples had met online, of which over a third had met at an internet dating site and 19 per cent in a chat room.

Online daters choose more diverse partners, according to the research, as 36 per cent of the 'online' couples had different levels of education compared with 21 per cent of 'offline' couples.

Bill Dutton, director of the Oxford Internet Institute, said: "This study is a dramatic illustration of the potential for the internet to reconfigure social relationships."

The survey also found strong evidence to suggest that couples believe 'online' relationships to be just as important as 'offline' ones.

Around 85 per cent of respondents disapproved of a partner 'flirting' online with someone else.

This rises to 89 per cent for 'communicating relationship troubles to others', 94 per cent for 'having cyber-sex' and 97 per cent for 'falling in love', raising interesting questions about the three per cent who are fine with this.
Other Weapons Used in Cyber War
Unfortunately, in the US, there is nothing but confusion over cyberwarfare. In contrast to failed US efforts, both China and Russia have adopted the OSW approach to cyberwarfare.

Engage, co-opt, and protect cybercriminals. Essentially, use this influence to deter domestic commercial attacks and encourage an external focus. This keeps the skills sharp and the powder dry.

Seed the movement. Once the decision to launch a cyberattack is made, start it off right. Purchase botnets covertly from criminal networks to launch attacks, feed 'patriotic' blogs to incite attacks and list targets, etc.

Get out of the way. Don't interfere. Don't prosecute participants. Take notes.

John Robb
OPEN SOURCE WARFARE: Cyberwar, 15 August 2008
On October 21, 2002, all thirteen DNS root name servers were targeted simultaneously through a coordinated DDoS (distributed denial of service) attack which lasted for approx one hour.

Attack volume was approximately 50 to 100 Mbits/sec (100 to 200 Kpkts/sec) per root name server, yielding a total attack volume was approximately 900 Mbits/sec (1.8 Mpkts/sec).

Some root name servers were unreachable from many parts of the global Internet. While all servers continued to answer all queries they received (due to successful overprovisioning of host resources), many valid queries were unable to reach some root name servers due to attack-related congestion effects, and thus went unanswered. (http://d.root-servers.org/october21.txt)

This could have been worse if the attack volume was increased many folds.
Attacks on Internet Backbone

Pakistan move knocked out YouTube
The government said it decided to block the video after senior representatives from several ministries of the Pakistani government met, according to a statement on the PTA Web site.

The authority sent the letter to Internet service providers after the meeting, Mehmood said, adding that the government would reinstate access to the video-sharing site if YouTube complied with the request.

The decision in Pakistan received mixed reactions.

"Some people are quite upset and screaming. They say they have been using YouTube regularly," said Wahid us Siraj, one of the founders of the Internet Service Providers Association of Pakistan, and chief executive officer of Micronet Broadband. "There are others who say that YouTube is full of videos that are damaging to the character of children."

Roughly 3 million to 5 million of Pakistan's 165 million people have Internet access, according to Siraj's association.

The recent reprinting in European newspapers of the controversial cartoon of the Prophet Mohammed that sparked worldwide protests two years ago has inflamed emotions further. Watch Pakistanis denounce the drawing.

The 3-year-old YouTube has exploded in popularity by letting ordinary people post their own videos online and watch videos that others have posted. The Web site's growth also has spawned efforts around the world to regulate it.

Authorities in Brazil, China, Iran, Morocco, Myanmar, Syria and Thailand have blocked access to YouTube in the last few years, according to Reporters Without Borders, a press advocacy organization.

The countries acted after concluding that YouTube videos were subversive (China), immoral (Iran), embarrassing to well-known figures (Brazil) or critical of a country's king (Thailand), the group said.

This time incidental it could be deliberate
Targeted Physical Attacks
Targeted Physical Attacks

• Software based attacks might be easier and quicker to recover, physical damages are not!
• The impact of cyber attacks are much lower than the physical attacks. For example, a sophisticated DDOS attack might result in an outage of few hours, destroying few backbone exchanges could result in days of work to recover (hurricane Katrina)
Cyberwar: Israel And Hamas Attack Each Other's Media

Eric Krangel | Jan. 6, 2009, 2:26 PM | 15
Tags: Middle East, Media

Israeli tanks are pushing into the Gaza Strip, and the Israel-Hamas fight is also playing out on another front: the Internet.

Over New Year's, a Morocco-based Islamic group calling itself "Team Exit" hacked DNS servers to reroute traffic away from Israeli media outlets like ynetnews to a site containing anti-Israeli propaganda.

Not to be outdone, the Israelis in turn hacked into Gaza-based Al Aqsa TV, taking the station's sometimes luridly antisemitic programming off the air and replacing it with a crude animation of Hamas leaders being gunned down, accompanied by the Arabic text "Time is running out."

Attacking the other side's media outlets seems to be a standard feature of 21st century warfare: During the summer Russia-Georgia war, Georgian news outlets were targeted by pro-Russia hackers.

We hope American media sites hold up well during when cyberwar inevitably comes to our own servers.

See Also:
Israel Puts War Footage On YouTube

Dow
-161.27
at 8163.60

Nasdaq
-41.23
at 1746.17

Earnings Season Special

palm prè
Filled with technology you'll never have to think about.
What about SCADA Systems?

- Supervisory Control And Data Acquisition (SCADA) generally refers to industrial automation systems
- Other related systems include Distributed Control Systems (DCS)
- Almost all large to medium scale industries including production and utility industries use some sort of automation
- Originally these control systems were isolated from outside world
- Current generation control systems are increasingly leveraging public switched networks
- This makes them vulnerable to cyber attacks which if successful can potentially have large impacts.
What about SCADA Systems?

Attack code released for SCADA software vulnerability
Dan Kaplan  September 08 2008

Updated on Monday, Sept. 8 at 5:16 p.m. EST

Security researcher Kevin Finisterre has created an exploit that takes advantage of a serious vulnerability reported earlier this summer in industrial process control software.

The bug in CitectSCADA, which was patched in early June after being discovered by Core Security Technologies, is a traditional stack-overflow vulnerability that grants an attacker access over supervisory control and data acquisition (SCADA) software that controls industrial processes, including chemical plants, assembly lines and power grids.

"I honestly feel that the flaw has the potential to be very critical," Finisterre, who works for security firm Netragard, said in an email Monday to SCMagazineUS.com. "That is the main reason for my secondary disclosure. I don't think this bug got the proper exposure the first time around."

He said Citect, whose U.S. headquarters is in Georgia, downplayed the severity of the flaw.

But Kurt Lovell, vice president of Citect Americas, told SCMagazineUS.com on Monday that the company advises its customers to take the vulnerability seriously.

"With respect to our install base, [Finisterre is] making it significantly easier for someone who wanted to do harm to try to do harm," Lovell said. "I am not particularly concerned because we have already worked aggressively with our install base to make sure they're protected."
What about SCADA Systems?

NEWS

Hackers Step Up SCADA Attacks

November 1st, 2004
Written by Wes Iversen

In the past, if your industrial control system suffered an electronic attack, the odds favored an inside job. But if your company is still operating under that assumption, Eric Byres has got news for you.

“This was a shock for me,” says Byres, a research faculty member at the British Columbia Institute of Technology (BCIT, www.tc.bcit.ca/gait), which maintains a database of cyber security incidents that directly affect industrial control systems and processes. “All of the sudden, our threat sources have changed. It’s no longer coming from the inside. It’s coming from the outside.”


Historically, more than two thirds of cyber security incidents affecting Supervisory Control and Data Acquisition (SCADA) systems have resulted either from accidents, acts by disgruntled employees or other inappropriate employee activity. Byres told the ISA audience. “This is something I’ve seen reported over and over again, and that I always agreed with, that 70 percent of our problem is internal, and that 30 percent is external.” The assumption, he said, was that if industrial companies dealt effectively with their inside cyber security issues, that most of their SCADA security problems would go away.

But when Byres recently began examining data compiled over the past several years at BCIT, he discovered a changing scenario. Compared to the period from 1982 through 2000, when 31 percent of reported control system security incidents came from outside of...
One-Third of Gas and Electric Utility IT Execs Fear SCADA Attack
(February 2006)
A Trusted Network Technologies survey of 50 US gas and electric utility information technology (IT) executives found that 33 percent believe SCADA (supervisory control and data acquisition) or distribution systems will suffer an attack within the next two years. Twenty-one percent of the respondents indicated their own systems had experienced outside threats.


Source:
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=22 #sID201
Information Warfare
Information Operations
Electronic Warfare
Strategic Cyberwar
Information Warfare
For military planners, the control of information is critical to military success, and communications networks and computers are of vital operational importance. The use of technology to both control and disrupt the flow of information has been generally referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and Information Operations (IO). Currently, IO activities are grouped by the Department of Defense (DOD) into five core capabilities:

1. Psychological Operations,
2. Military Deception
3. Operational Security
4. Computer Network Operations, and
5. Electronic Warfare.
Current U.S. military doctrine for IO now places increased emphasis on Psychological Operations, Computer Network Operations, and Electronic Warfare, which includes use of non-kinetic **electromagnetic pulse (EMP) weapons**, and **nonlethal weapons for crowd control**. However, as high technology is increasingly incorporated into military functions, the boundaries between all five IO core capabilities are becoming blurred.

DOD has noted that military functions involving the electromagnetic spectrum take place in what is now called the cyber domain, similar to air, land, and sea. This cyber domain is the **responsibility of the new Air Force Cyber Command** and includes **cyberwarfare, electronic warfare**, and protection of U.S. critical infrastructure networks that support telecommunications systems, utilities, and transportation.
Psychological Operations (PSYOP)

- Planned propagation of desired information to influence behaviour and belief systems of adversary (individual, groups, countries)
- Counter competitor’s information dissemination by proactive and rapid development of new products based on the knowledge of adversary’s decision making processes
- PSYOPs are not intended to target host audience but information can leak in through the global media.
Israel steps up "psy-ops" in Lebanon

From mass targeting of mobile phones with voice and text messages to old-fashioned radio broadcasts warning of imminent attacks, Israel is deploying a range of old and new technologies in Lebanon as part of the psychological operations ("psyops") campaign supplementing its military attacks.

According to US and UK media outlets, Israel has reactivated a radio station to broadcast messages urging residents of southern Lebanon to evacuate the region.

Some reports have named the station as the Voice of the South.

The South Lebanon Army, a Christian militia backed by Israel, operated a radio station called Voice of the South from Kfar Kila in southern Lebanon in the 1980s and 1990s.

The station closed down in May 2000 when Israeli forces withdrew from southern Lebanon.

Cash for tips-offs

The Israeli newspaper Maariv on Sunday reported the...
• Computer Network Attack (CAN) – Attack and disrupt enemy computer networks through
  – Network applications
  – High voltage surge (Electronic warfare)

• Computer Network Defense (CND) – Defend own military information systems
  – Monitor, detect and respond to unauthorized computer activity

• Computer Network Exploitation – Exploit enemy computer networks through intelligence collection
  – Discover vulnerabilities
  – Gain unauthorized access

• Lacks in legal and policy issues analysis

• Network interdependencies is a big obstacle in carrying out the attacks
Hackers Attack Via Chinese Web Sites
U.S. Agencies' Networks Are Among Targets

The number of attempted intrusions from all sources identified by the Pentagon last year totaled about 79,000 [...] Concern about computer attacks from China comes amid heightened U.S. worry generally about Chinese military activities. [...] and the Pentagon's latest annual report on Chinese military power, released last month, described the ongoing modernization of Beijing's armed forces. The report contained a separate section on development of computer attack systems by China's military. It said the People's Liberation Army (PLA) sees computer network operations as "critical to seize the initiative" in establishing "electromagnetic dominance" early in a conflict to increase effectiveness in battle. [...] "The PLA has increased the role of CNO [computer network operations] in its military exercises," the report added. [...]
Electronic Warfare

• Domination of the Electromagnetic Spectrum – Exercising maximum control of entire electromagnetic spectrum including the capability of disrupting communication systems, sensors and weapon systems
  – Space control e.g. disrupting Global Positioning Satellites
  – Communication control e.g. radio and TV broadcast systems
  – Surveillance control e.g. misguiding radar systems and UAVs

• Electromagnetic Non-Kinetic Weapons – Send high energy short pulses to permanently damage adversary’s computer system, e.g.,
  – High Power Microwave (HPM) beams to destroy incoming missile control circuitry
  – Active Denial System (ADS) project beams to induce an intolerable burning sensation to repel an adversary while minimizing fatalities.
Crowd control weapons, to be used by US troops on Iraq rioters

By Tony Freinberg and Sean Rayment, Defence Correspondent

http://www.telegraph.co.uk/news/main.jhtml;sessionid=10OG3HIV4NW0VQF

(Filed: 19/09/2004) Microwave weapons that cause pain without lasting injury are to be issued to American troops in Iraq for the first time as concern mounts over the growing number of civilians killed in fighting.

The non-lethal weapons, which use high-powered electromagnetic beams, will be fitted to vehicles already in Iraq, which will allow the system to be introduced as early as next year.

Using technology similar to that found in a conventional microwave oven, the beam rapidly heats water molecules in the skin to cause intolerable pain and a burning sensation. The invisible beam penetrates the skin to a depth of less than a millimetre. As soon as the target moves out of the beam’s path, the pain disappears.

Because there are no after-effects, the United States Department of Defence believes that the weapons will be particularly useful in urban conflict. The beam could be used to scatter large crowds in which insurgents operate at close quarters to both troops and civilians.

"The skin gets extremely hot, and people can’t stand the pain, so they have to move - and move in the way we want them to,” said Col. Wade Hall of the Office of Force Transformation, a body formed in November 2001 to promote rapid improvement across all of the American armed services.

Rich Garcia, a spokesman for the Air Force Research Laboratory in New Mexico, where the systems were developed, took part in testing the weapon and was subjected to the microwave beam which has a range of one kilometre. "It just feels like your skin is on fire,” he said. "(But) when you get out of the path of the beam, or shut off the beam, everything goes back to normal. There's no residual pain.”

A heated battle on a crowded Baghdad street last week that left 16 Iraqis dead, highlighted once again the pressing need to reduce the number of civilian casualties, and at the same time prevent further damage to relations between American troops and the Iraqi population. American commanders later admitted using seven helicopter-launched rockets and 30 high-calibre machine gun rounds in last Sunday's incident.

The armoured vehicles will be named Sheriffs once they have been modified to carry the microwave weapons, known as the Active Denial System (ADS). Col Hall said that US army and US marine corps units should receive four to six ADS equipped Sheriffs by September 2005.

The project was initiated only three months ago but US military chiefs intend to rush the Sheriffs into the front line, believing that they can be of immediate assistance.

In another development, the Sheriffs will be fitted with Gunslinger, a rapid-fire gun currently under development that will detect enemy snipers and automatically fire back at them.
Concluding Remarks

• Cyber warfare has many dimensions, the two very obvious domain are military and civilian domains
• But the boundaries between military and civilian domains are becoming blur as governments and organisations has started realising the significance of cyberspace as an effective tool for warfare
• It is a never ending process, the key to success is how to always remain one step ahead of the opponent
Conclusion

Cyber warfare is coming
It will hit very hard!