# CYBER WAR & PEACE II


Event Code: **Lecture**
Event Description: **Small event**

Ver. 1:
Duration: **30 min**
Unit: **1**

Topic: **Cyber warfare**

Author: ***Prof. Radomir A. Mihajlović, NYIT New York, USA***

# Topics

- Introduction
- Cyber space & Internet World
- Cyber aggression
- IW
- US response options and some activities
- UK response options and some activities
- Some incidents
- Strategic planning
- Concluding remarks

- **Disclaimer:** All opinions expressed are solely those of the author and do not necessarily represent the opinions of any other entity.

# What is Cyberspace?

- **Definition**: Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support businesses, infrastructure and services, [3].
  - Digital networks are behind the supply of electricity and water to our homes, the delivery of food and other goods to shops, and behind the businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances.

# Cyber aggression

- **Definition**: Cyber aggression is a premeditated act of use of electronic means, primarily Internet leading to the loss of comfort, loss of privacy (Personalized secrecy), financial or other material damage, loss of life or health well being, [8].

  - Minor cyber aggressions are cyberbullying and cyber harassment
  - Major cyber aggression is cyber espionage
  - The ultimate act of a cyber aggression is the cyber war, with governments as aggressor entities.

# Cyber warfare goals and strategies

- To incapacitate/disable/deny adversary's cyber space infrastructure, (Directly or indirectly present in the cyber space)

# Cyber warfare goals and strategies

- To influence all strategic operations by all electronic means targeted at:
  - Public affairs operations or PAO, (Guiding-leading public opinion, dealing with the media, etc., [6,7])
  - Civil affairs or CAO, (Enhancing legitimacy and credibility of the future or current military operations in the target territory [5], minimize insurgency, etc.)
  - Psychology operations, political warfare, propaganda or “Hearts & Minds Ops” or PSYOP, (used to emotionally enhance hostilities, fear, or unjustified comfort)
  - Computer network operations or CNO, (technical methods used in warfare, to gain information superiority and deny the enemy the same.)

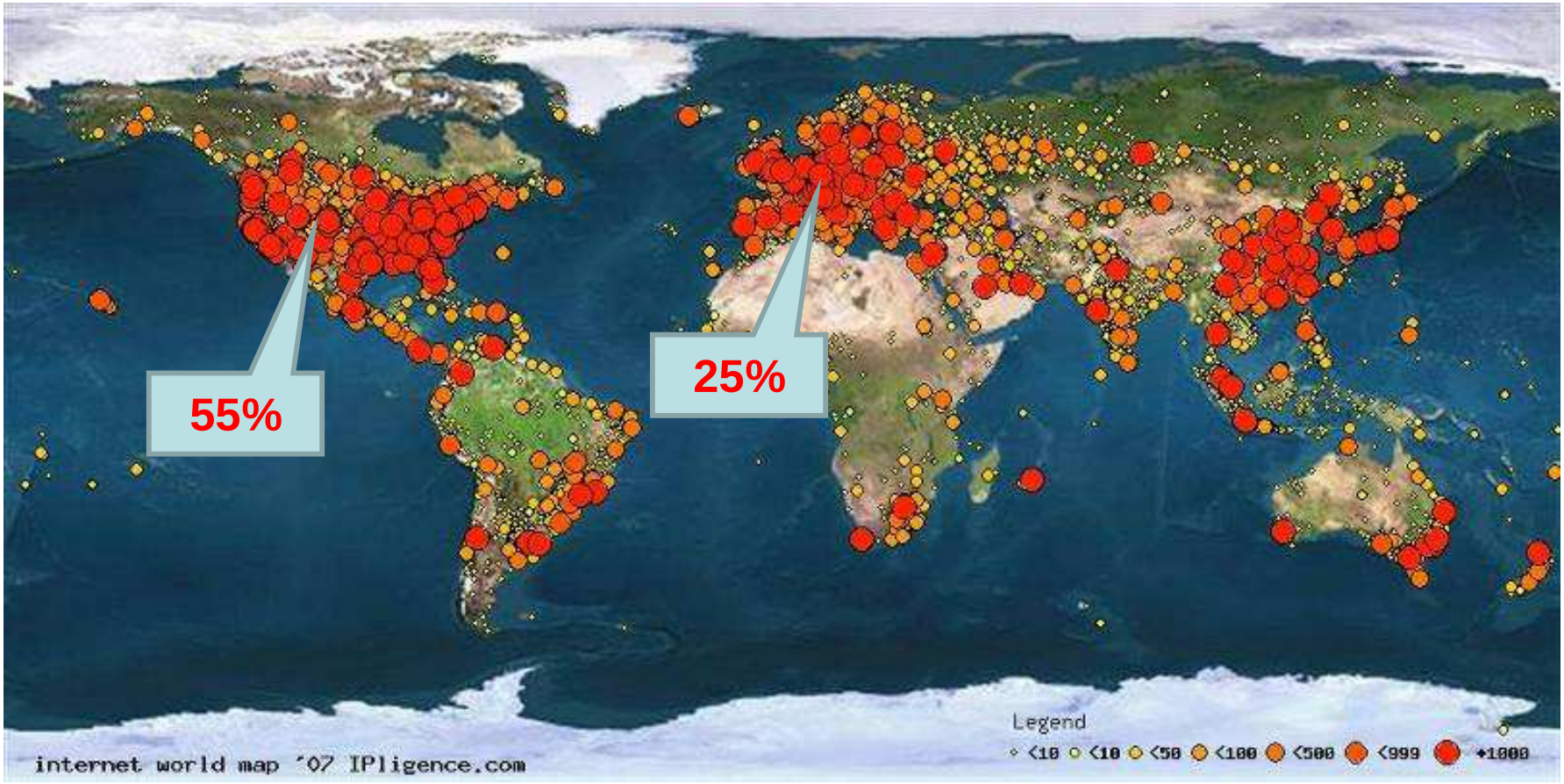
# Information warfare

- **Definition**: Information warfare or IW are all actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.

  – IW is as old as civilization.
  – IW/DIW information and disinformation warfare.
  – Soft war [4]

# Over 5 billion devices connected

- Internet connected device growth is accelerating to 22 billion (Eu. Milliard) by 2020, [1,2].



# Breakdown by geographic IP v.4 location

- Used IP address distribution may indicate where are the most likely cyber war theaters, [2].

| Geographic area | Number of addresses | Percentage |
|---|---|---|
| Africa | 40,241,664 | 1.519% |
| Antartica | 15,620 | 0.001% |
| Asia | 371,297,015 | 14.015% |
| Caribbean | 1,681,866 | 0.063% |
| Central America | 2,557,340 | 0.097% |
| Europe | 569,838,903 | 21.510% |
| Middle East | 12,011,131 | 0.453% |
| North America | 1,481,754,661 | 55.932% |
| Oceania | 76,417,711 | 2.885% |
| South America | 93,409,304 | 3.525% |

# White House memo: "International Strategy for Cyberspace"

- The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold, [9].

# The U.S. international strategy & vision for cyberspace: Norms

- These norms mentioned include:
  - Upholding Fundamental Freedoms
  - Respect for Property
  - Valuing Privacy
  - Protection from Crime
  - Right of Self-Defense
  - Global Interoperability
  - Network Stability
  - Reliable Access
  - Multi-stakeholder Governance
  - Cybersecurity Due Diligence

# US efforts planned

- To ensure the respect of all civilized norms in the cyber space, to enhance prosperity, security, and openness so all can benefit from networked technology the US will combine:
  - diplomacy,
  - defense, and
  - development

# Cyber warfare capability development strategy

- Improving cyber power and organizational effectiveness involves:
  - Legislature
  - Recruiting
  - Financing & fundraising
  - Education & Training
  - Command and control
  - Intelligence gathering

# US activities & plans

- The US Government organizes its activities across seven interdependent areas of activity, each demanding collaboration between:
  - The US government,
  - International partners, and
  - The private sector.

# US activities, plans & seven areas

- Action lines of US strategic framework.
  - Economy
  - Protecting our networks
  - Law enforcement
  - Military
  - Internet governance
  - International development
  - Internet freedom

# Economy protection

- Promoting international standards and Innovative, Open Markets:
  - Sustain a free-trade environment that encourages technological innovation on accessible, globally linked networks.
  - Protect intellectual property, including commercial trade secrets, from theft.
  - Ensure the primacy of interoperable and secure technical standards.

# Threats to energy security

- Energy security is the “provision of affordable, reliable, diverse, and ample supplies of oil and gas… and adequate infrastructure to deliver these supplies to market.”
  - Reliable energy inputs are crucial to U.S. national security.
  - A sudden removal or disruption of energy inputs could adversely impact the U.S. economy and cause severe inflation.
  - Rising fuel prices can bring windfall profits to regimes hostile to the U.S.
  - Competition over scarce energy resources also has the potential to be a major source of conflict, which could directly impact supply or result in inter-state conflict.

# Protecting our networks

- Enhancing security, reliability, and resiliency
  - Promote cyberspace cooperation, particularly on norms of behavior for states and cyber security, in a range of multilateral organizations and multinational partnerships.
  - Reduce intrusions into and disruptions of U.S. networks.
  - Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure.
  - Improve the security of the high-tech supply chain, in consultation with industry.

# Law enforcement

- To extend collaboration and the rule of law, to enhance confidence in cyberspace and pursue those who would exploit/misuse online systems:
  - Participate fully in international cybercrime policy development.
  - Harmonize/sunchronize cybercrime laws internationally by expanding accession to the Budapest Convention.
  - Focus cybercrime laws on combating illegal activities, **not restricting access** to the Internet.
  - Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.

# Problems in Thailand: Click and go to prison

- Clicking on Facebook in Thailand can potentially land you in prison, [14].
- The Thai Minister of Information and Communication Technology declared that they will begin charging Facebook users for “liking” or sharing content that could be deemed offensive to the Thai throne, the sentence for which could run anywhere between three to 15 years in prison.
  - A 61-year old retired truck driver battling mouth cancer was sentenced to 20 years in jail for sending text messages with supposed offensive content.

# Problems in Bahrain: Facebook posting troubles

- 63 Bahraini students were expelled from school for “participating in unlicensed gatherings and marches,” the evidence of which was pulled from their Facebook accounts, [14].

# Problems in Vietnam: Offensive Internet Speech

- There has been a recent wave of excessive jail sentences given to those criticizing the Chinese and Vietnamese Communist regime over the Internet.
  - October 22, 2010—Committee to Protect Journalists CPJ is concerned by Vietnamese authorities' recent crackdown against several bloggers and one print journalist, [14].

# Problems in Syria: Email tapping

- The Commerce Department is investigating whether technology produced by a California company Blue Coat Systems helped Syrian police monitor dissidents amid a bloody crackdown there. [15]

# Problems in England: Accessing extremist sites is a crime?????

- The signs, which state that the owners of the premises are actively working with the Metropolitan police, have drawn criticism due to their vagueness and questionable legality. "Downloading or accessing certain material could constitute a criminal offence" states the bright pink sign, [16].

# Form of net police in England terrifies citizens of the cyber space

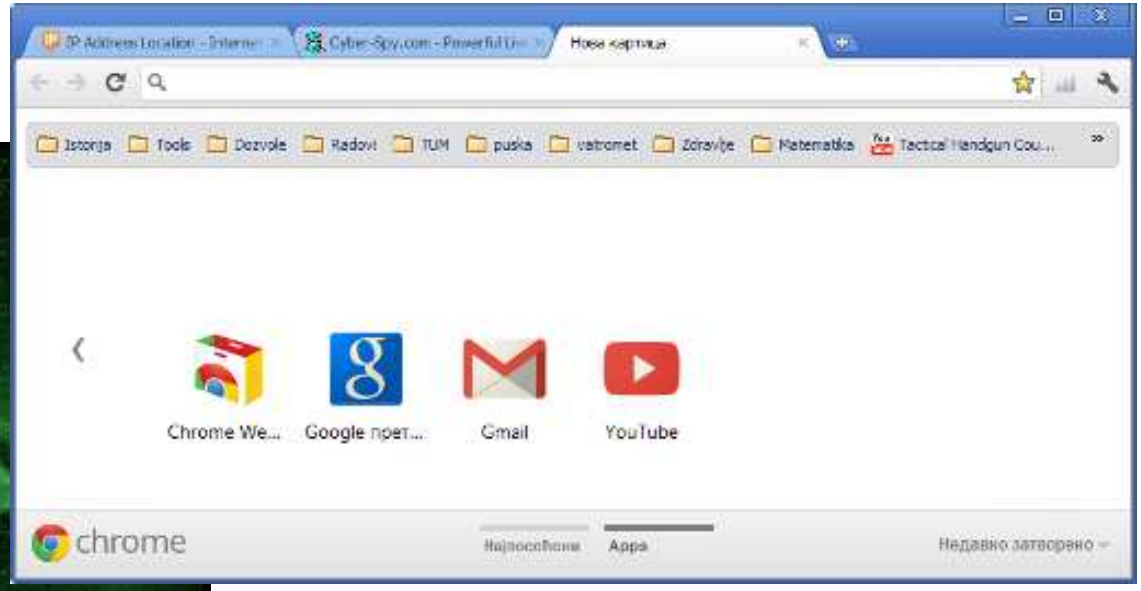
- Police signs have begun springing up in internet cafes in London warning users that they could be reported to the police and face criminal charges if they access "**extremist**", "**offensive**" or "**inappropriate**" material, [16].
- Do we have here possible violation of "rights to read!" "rights to see!" or "rights to hear!"

# Cyber threats in UK

- Some of the most sophisticated cyber threats to the UK come from other states which seek to conduct espionage with the aim of spying on or compromising UK government, military, industrial and economic assets, as well as monitoring opponents of their own regimes in UK, [3].

# What are and who are a spies?

- **Definition:** A spy is an agent employed by a state to obtain secret information, especially of a military nature, concerning its potential or actual enemies, or one employed by a company to obtain confidential information about its competitors, or one who secretly (???) keeps watch on another or others.



# Are we all spies?

- **Definition:** Spy is one who observes secretly with hostile intent, ore one who discovers by close observation, or one who investigates intensively, or one who makes a careful investigation of other people's activities.

» One who seeks or observes something secretly and closely.

» Do we like to advertise our most precious research?

# US military & cyber defense

- Preparing for 21st century security challenges with the commitment to defend citizens, allies, and interests extends to wherever they might be threatened, US military must:
  - Recognize and adapt to the military's increasing need for reliable and secure networks.
  - Build and enhance existing military alliances to confront potential threats in cyberspace.
  - Expand cyberspace cooperation with allies and partners to increase collective security

# US operational cyber warfare organizations & efforts

- STRATCOM
  - ARMY
  - AIR FORCE
  - NAVY
  - MARINES





# US operational cyber warfare organizations

- STRATCOM – USCybercom (10/31/2010. Fort Meade, Md.)
  - ARMY – ARCyber (10/1/2010, command Second Army)
  - AIR FORCE - 24th Air Force AFCYBER
  - NAVY - FLTCYBERCOM, (Tenth Fleet)
  - MARINES – MARFORCyber

# USSTRATCOM unveils new shield, mission, vision for command

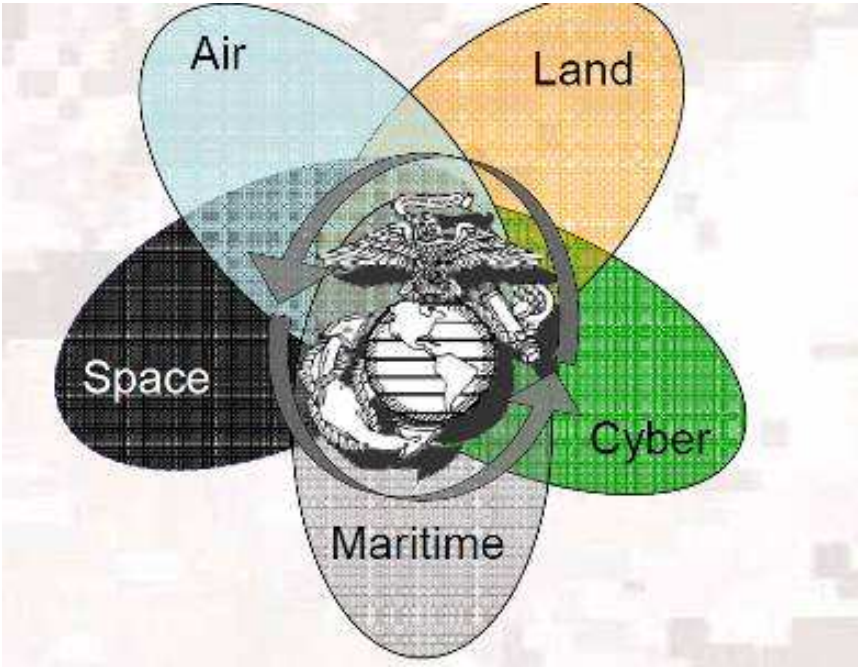
# Cyber war domain & US DoD

- A global cyber domain within the information environment consists of the interdependent network of IT infrastructures, including:
  - the Internet,
  - telecom networks,
  - computer systems,
  - embedded processors and
  - controllers.

# Cyber war domain & US DoD

- Cyberspace characteristics:
  - Domain/ Operational environment
  - Terrain (defended & exploited)
  - Weapons platform
  - Mindset; an approach for offense & defense

- The multi dimensional war theater gets one more dimension, one more domain.

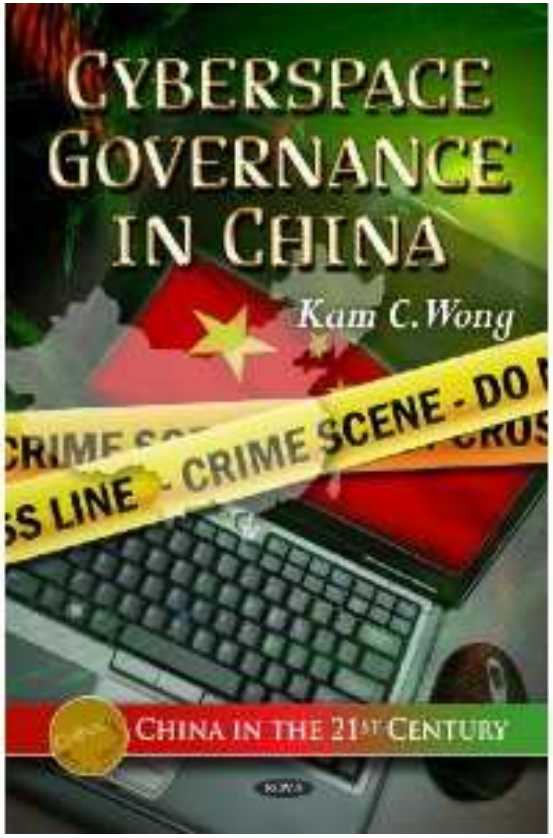


# Internet Governance

- Cyber defense has to promote effective Internet governance structures that effectively serve the needs of all Internet users:
  - Prioritize openness and innovation on the Internet.
  - Preserve global network security and stability, including the domain name system (DNS).
  - Promote and enhance multi-stakeholder venues for the discussion of Internet governance issues.

# Internet Governance

- Obama's Cyber Zar! Hired & fired?
- Chinese Cyber Zar???




# US cyber defense Internet freedom support

- Supporting fundamental freedoms and privacy help secure fundamental freedoms as well as privacy in cyberspace:
  - Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.
  - Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions.
  - Encourage international cooperation for effective commercial data privacy protections.
  - Ensure the end-to-end interoperability of an Internet accessible to all.

# US cyber defense international development support

- Building capacity, security, and prosperity to promote net technology globally, enhance the reliability of our shared nets, and build the community of responsible stakeholders in cyberspace:
  - Provide the knowledge, training, and other help to countries in need to build cyber security capacity.
  - Improve and share international cyber security best practices.
  - Enhance US states' ability to fight cybercrime – training for law enforcement, forensic specialists, jurists, and legislators.
  - Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their US Gov. counterparts

# US Omnibus Crime Control & Safe Streets, Public Law

- US cyber defense includes legislative efforts too.
- Congress finds that the high incidence of crime in the US threatens the peace, security, and general welfare of the Nation and its citizens.
- To prevent crime and to insure the greater safety of the people, legislative efforts and law' enforcement efforts must be better coordinated, intensified, and made more effective at all levels of government, [13].

# US lawmakers

- Led by the senators (D) Jay Rockefeller and (D) Joe Lieberman, US lawmakers are trying to introduce many frightening Internet control legislatures, that need long and ultra careful preliminary multi disciplinary examination and wide open discussion.

The only democrat in a staunchly republican family.

The only democrat that did not receive endorsement of his party in the state he represents???

# Example: FISA + Section 206 are too general

- Section 206 amended the Foreign Intelligence Surveillance Act (FISA) so that a wiretap order issued by the secret FISA court no longer has to specify what type of communications and which person the order applies to.

# Example: FISA + Section 206 & John Doe wiretaps

- Too general:
  - This allows "roving" surveillance, using a single wiretap order to listen in on any device or media (phone line or monitor any Internet account of the suspect or other people who are not suspects but are using devices, lines or media.
  - The FISA court can issue "**John Doe**" wiretaps that don\'t even specify the surveillance target's name

# Cyber threats in UK

- ‘Patriotic’ hackers can act upon states’ behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension.
- In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military’s technological advantage, or to reach past it to attack our critical infrastructure at home, [3].

# Criminals are enemies of the state

- Recent research suggests that the costs to the UK of cyber crime  could be in the order of £27 billion per year [12].

# UK Panic

- The British government published its new "cyber-security" strategy, [4], that includes the use of bans on social networks such as Facebook and Twitter for those who have been accused of misusing the Internet for criminal means, [10].
- Even more alarming, the strategy includes a plan to introduce surveillance technology that could be used to inform the authorities when banned users are breaking the bail or sentencing conditions that have been set on their Internet use.

# UK Panic

- Prime Minister David Cameron's position on Internet freedom has been staggeringly inconsistent.
- He has publicly pledged his commitment [11], to a free and open Internet, saying "Governments must not use cyber security as an excuse for censorship," and he has also called on his government to explore the possibility of shutting off access to Internet social media in case of civil unrest. [12].

# Why fight in the cyberspace

- Internet rapid communications
- Low cost
- Ubiquity
- Ease of use + sophistication of tools
- Anonymity

# Attack/Threat sources

- Foreign governments (States)
- Terrorists (Politically motivated)
- Hacktivists (Politically motivated)
- Criminals (Profit motivated)
- Dummies (Hackers for fun and excitement)

# How about cyber terrorism???

- There are very few documented cases of cyber terrorism.
- **WHY?**

# Cyber Terrorism vs. Other Computer Attacks

| | MOTIVATION | TARGET | METHOD |
|---|---|---|---|
| **Cyber Terror** | **Political change** | **Innocent victims** | **Computer-based violence or destruction** |
| **Cracking** | **Ego, personal enmity** | **Individuals, companies, gov’ts** | **CNA, CNE (sometimes overt)** |
| **Cyber Crime** | **Economic gain** | **Individuals, companies** | **Fraud, ID theft, blackmail, CNA, CNE** |
| **Cyber Espionage** | **Economic gain** | **Individuals, companies, gov’ts** | **CNA, CNE (rarely overt)** |
| **State-Level Info War** | **Political or military gain** | **Infrastructure, military assets** | **CNA, CNE, physical attack** |

# What are the cyber war weapons?

- Virus
- Worm
- Trojan
- DoS
- DDoS . . . .

# True cyber war weapons!?

- Data mining
- Data fogging,
- steganography
- Image processing
- Visual pattern recognition
- Data patter recognition
- Super computing
- Super sized storage
- New laws
- Propaganda
- . . . . .

# Cyber war, WW III & WW IV?

- Each new world war has been decided by the shockingly new weapons and new strategies.
  - WW I – Trench war
  - WW II – Mechanized and air war.
  - WW III - We all thought that it will be the star war fought in the space!

  - However, nobody dreamed about cyber space, digital robots and cash wars !!

# Summary

- Cyber space sharing and peaceful coexistence is one of the finest examples of a community self-organizing, as civil society, academia, the private sector, and governments work together democratically to ensure its effective management.
- Most important of all, this space continues to grow, develop, and promote prosperity, security, and openness as it has since its invention.
- Cyberspace & Internet are global world bonding vehicles in the international environment, and that is why it is so important to protect it, [9].

# Summary: US is behind the curve?

- "…the U.S. is dangerously behind the curve in countering terrorist use of the Internet…"

[Dr. Bruce Hoffman, "at Washington Foreign Press Center briefing on "The Status of the War on Terrorism"]


Director of the Center for Peace and Security Studies at Georgetown University, Ex Director, RAND Washington Office.

# Summary: US is already in peril of losing the cyber war

- Cyber war is about:
  - technology,
  - government,
  - military strategy;
  - about criminals,
  - spies,
  - soldiers, and
  - hackers.
- Cyber war is the war of the future that we may already be in peril of losing it.

**Richard Alan Clarke Special advisor to Pres. G. W. Bush on Cybersecurity**

# Summary: Globalized control of cyberspace

- This cyberspace is defined by four key characteristics:
  - Open to innovation
  - Interoperable world wide
  - Secure enough to earn people's trust
  - Reliable enough to support their work

# Summary: Maintain open Internet!

- We should never forget that hackers and cyber aggressors love cyber space!

# The End

# Reference

[1] IMS Research, 19 August 2010
[2] Internet World Map 2007, IP Ligence
[3] The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, Rt Hon Francis Maude MP Minister for the Cabinet Office and Paymaster General, November 2011.
[4] R. A. Mihajlovic, Intrusion detection and counter hack procedures.
[5] Civil affair operation, Department of the US Army, Sept. 2006.
[6] Public Affairs Operations, US Army Field Manual, FM 46-1, 1997
[7] Public affairs operations, US Air Force Doctrine Document 2-5.4, 2005
[8] Reto E. Haeni, Information Warfare; an introduction
The George Washington University, Cyberspace Policy Institute
Washington DC, January 1997
[9] International strategy for cyberspace – Prosperity, security and opennes in a networked world, The White House Memo, May 2011
[10] Z. Whittaker, UK government reneges on censorship-free web promise; Plans to ban 'cyber-criminals' from the web, ZD Net Nov. 28, 2011,

# Reference

[11] Kate Solomon, Internet must remain open, says UK government Talkin' to you, November 1st 2011 TechRadar.com
[12] Eva Galperin, British Prime Minister Does a 180 on Internet Censorship, Electronic Frontier Foundation, AUGUST 11, 2011
[13] Omnibus Crime Control and Safe Streets, Public Law 90-351; 82 STAT.197, [H. R. 5037]
[14] A wave of media suppression in Vietnam, CPJ, New York, October 22, 2010
[15] Sari Horwitz, Shyamantha Asokan, U.S. Probing Use of Surveillance Technology in Syria, Freeepress, November 17, 2011
[16] DisgruntledTunaFan, Criminal charges for accessing “extremist”, “offensive” or “inappropriate” sites, PatsFans.com, Oct. 2006.