Defining CyberWarfare

Peter Sommer
P.M.Sommer@lse.ac.uk
Peter@pmsommer.com
We have been here before...

John Deutch, CIA 25/06/96:

“… our government, business and citizens have become increasingly dependent on a network of telecommunications and computer-based information systems…

“… critical backbone for the entire US public and private sectors….

“… I am concerned that this connectivity and dependency makes us vulnerable to information warfare attacks
We have been here before...

“My greatest concern is that hackers, terrorist organisations, or other nations might use information warfare techniques as part of a coordinated attack to seriously disrupt infrastructures ….

“Virtually any ‘bad actor’ can acquire the hardware and software to attack information-based infrastructures…”

??? Electronic Pearl Harbor ????
"This is the battleground for the future," CIA Director Leon Panetta, "The next Pearl Harbor may very well be a cyber attack." 10/02/2011
“Cyberthreat difficult to overstate” (James Clapper, US Director of National Intelligence, 10/02/2011)
“Information Warfare”: Possible Contexts

New Battlefield Technologies

- **electronic counter-measures** - jamming, rf dominance, information dominance
- **attacks on command-and-control centres** - Gulf War etc
- **smart weapons** - Gulf war etc
- **remote control of battlefield** - soldiers with sensors, satcomms, VR display control rooms etc
“Information Warfare”: Possible Contexts

New military “Doctrine”

• what is “the national interest”?
• what kind of threats?
• what kind of wars / operations?
  ➔ symmetric, high intensity
  ➔ asymmetric, low intensity - peace keeping, humanitarian, coalition activities

• what kind of army? - people, weapons, skills, readiness etc
“Information Warfare”: Possible Contexts

Industrial Espionage

- industry-sponsored
- state-sponsored
  - economic intelligence
  - contract intelligence
- computer aids
“Information Warfare”: Possible Contexts

Psychological Warfare

- misleading the enemy
- direct injection of false information
- indirect inject via misleading background info >> media manipulation
- counter-will / counter-forces / counter-commander
“Information Warfare”: Possible Contexts

Logical attacks on systems

• breach of confidentiality - hacking etc
• denial of service - trojans, viruses etc
• compromise of service - making computer systems unreliable
• viruses and trojans as weapons - the embedded hardware trojan?
“Information Warfare”: Possible Contexts

Physical attacks on systems

• bombs
• attack on key points
• minor but significant attacks - results not immediately obvious
• EMP weapons
“Information Warfare”: Possible Contexts

Still more contexts …

- **IBW: Intelligence-Based Warfare**
- **Economic Information Warfare** - denying access to technologies, comms links, data sources
- **Cultural Warfare / Information Imperialism**
- **Crypto Warfare**
- **Cyberwarfare**
Criminal Act? Act of War?

Ambiguous Law

Anonymous Adversaries

Simple Technology

Lots of Targets

Psychological

Information

Demand

Supply

Time

No Spatial Boundaries

No Quick Fixes

No Political Boundaries

No Geographic Boundaries

Uncertain Responsibilities

Poorly Defined Remedies

No Temporal Boundaries
Extending the Subject …

- “Information Operations”
- “Information Power”
Information Power

- “Combination of information content and technology used as a strategic instrument to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security strategies & objectives”
  
  » Drs Dan Kuehl & Bob Neilson, Georgetown’s NSSQ 1999

- “The relative ability to operate in and exploit the information environment — the aggregated and synergistic combination of CONNECTIVITY, CONTENT, & COGNITION.
  
Information Operations (US)

- Current: “Integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own”
  - IO Roadmap of 2003: Joint IO Doctrine 3-13 of 2006

- Future: “The planned and integrated employment of capabilities in the information environment across the spectrum of military operations”
  - in coordination, not yet formally approved
• Crime (every day)
  - Use of cyberspace and cyber capabilities for criminal activity
    - ID Theft; Extortion

• Espionage (every day)
  - Most “cyberattacks” are really this
  - Economic and Military
    - Terrabytes (= a lot!)

• Terrorism (not yet)
  - Not terrorist use of the Internet
  - Sufficiently destructive or disruptive as to equal kinetic actions

• War (not yet) = ?
  - Conduct of military warfighting operations in/via Cyberspace
    - Negating air defense radars/controls
  - Creation of warfare-like effects on critical national security infrastructures
    - Electricity, Money, Telecomms

“The global hub for educating, informing, and connecting Information Age leaders.”
• *It is easy to add more and more elements to our subject-matter ...*

• *But is this at the expense of understanding the new phenomena?*
The words we use to describe things influence our thoughts about what phenomena we are viewing – and the sorts of solutions to any problems that might exist

- **CyberWar** implies the military world
- **CyberCrime** implies the police
- **CyberSecurity** implies techies
- **Cyber Incidents** implies ????
Words understood in context

- **Ryle**: Philosophy as cartography; mapping words and phrases to generate implication threads

- **Example in law**: “possession”
  - “possession” of narcotics
  - “possession” of child sexual abuse images
  - “possession” of real property – land, a building, an apartment
In Cyber War:
• What is the test for “war”?
• How important is the “cyber” element?
• What are the objectives and motives for the conflict?

In Cyber Crime:
• How important is the “cyber” element?
• What are the objectives and motives of the criminal?
What is “computer (cyber) crime”?

- Any crime with the word “computer” in it
- Computer-related crime: any crime which requires a computer for the commissioning
- Computer-related crime: any crime which is touched by a computer
- Quasi-crimes, eg industrial spying
CyberCrime Convention
(Treaty of Budapest, 2001)

- **Offences against systems**
  - Illegal access
  - Illegal interception
  - Data interference
  - System interference
  - Misuse of devices (hacking tools)

- **Substantive offences**
  - Computer-related forgery
  - Computer-related fraud
  - Child pornography
  - Copyright infringements
  - (Aiding and Abetting, Attempts)
  - (Corporate liability)
Substantive Law: UK

Fraud Act, 2006

Money Laundering
- Proceeds of Crime Act, 2002; Serious Organised Crime & Police Act, 2005

Extortion / Blackmail
- S 21 Theft Act 1968 (unwarranted demand with menaces)

Indecent Images of Children
- Protection of Children Act, 1978, s 160 Criminal Justice Act, 1978 (as amended)

Extreme Pornography
- S 63 Criminal Justice & Immigration Act 2008

Intellectual Property Piracy
- Copyright Designs & Patents Act 1988, s 107
- Trade Marks Act, 1994, s 92
- Digital Economy Act, 2010
Substantive Law: UK

Terrorism

- Terrorism Act, 2000
  - Definitions, interpretation
  - Fundraising
  - Possession of articles connected with etc etc
  - Powers: arrest, stop & search

- Anti-Terrorism, Crime & Security Act, 2001
  - Terrorist cash & property, disclosure powers, toxins, police powers, retention of communications data

- Prevention of Terrorism Act, 2005
  - Control orders etc

- Terrorism Act, 2006
  - Encouragement of terrorism, publications, preparation, training

- Counter-Terrorism Act, 2008
  - Post-charge questioning, powers over those subject to control orders, money laundering, DNA database
Substantive Law: UK

Data Protection offences (DPA, 1998)

- S 55 Unlawful obtaining of personal data
- (s 21: processing personal information without registration)
Substantive Law: UK


- **S 1**: Unauthorised access (12 months)
- **S 2**: Unauthorised access with intent to commit a further crime (5 years)
- **S 3**: Unauthorised data modification / with intent to impair (10 years)
- **S 3A**: “hacking tools” / making or supplying (2 years – can also use s 7 Fraud Act 2007)
How far is it worth producing a taxonomy of cyber criminals?

- Hackers – recreational
- Hackers – “professional”
- Insiders
- Discontented employees and ex-employees
- Hacktivists
- Fraudsters
- Blackmailers
- Copyright thieves
- Terrorists
- ??
Roger Grimes (InfoWorld, 02/2011)

“Your guide to the seven types of malicious hackers”:

- Cyber criminals
- Spammers and adware spreaders
- Advanced persistent threat (APT) agents
- Corporate spies
- Hactivists
- Cyber warriors
- Rogue hackers
Let’s compare “Car” Crime...

• parking on single yellow line
• speeding and other “driving” offences
• car as getaway after raid
• ramraiding
• car as murder weapon
• theft of car for resale
• garage repair frauds
• garage committing tax offences

>> Is there such a thing as “computer crime”?
Why categorise?

Do we concentrate on the substantive offence or the means by which it has been committed?

- Implications for law reform
- Implications for crime prevention / mitigation
- Implications for policing
History of the word “hacker”

- clever programmer
- network adventurer
- cracker - attack on security systems
- all-purpose synonym for “computer criminal”
What is a cyber “incident”?

- Software failure
- Hardware failure
- Successfully detected malware
- Successfully prevented intrusion
- Attempted theft of data
- Denial of Service attack
- Loss of computer hardware
- Loss of data (accidental / deliberate)
- Physical attack on computer system
What is a cyber “attack”?

- Successfully detected malware
- Successfully prevented intrusion
- Attempted theft of data
- Denial of Service attack
- Theft of computer hardware
- Loss of data (accidental / deliberate)
- Physical attack on computer system
How do we calculate losses?

- **Immediate cost of hardware, data media**
  - Replacement or “as new”
- **Cost of reconstructing data**
  - Clerical, or re-sourcing
- **Compensation to third parties**
  - On what basis?
- **Loss of revenue / profits**
  - How do you prove?
- **Remedial costs**
  - What do you include / exclude?
- **Lost business opportunities**
Who is analysing?

Definitions influenced by pre-occupations of analyser

- Access control vendors concentrate on “hackers”
- Anti-malware vendors concentrate on malware
- Consultants concentrate on business risks
  - Extortion
  - Insider threat
  - Situations where consultancy analysis may provide remedies
- Owners of copyright material concentrate on piracy
- Children’s Charities concentrate on threats to children
First Annual Cost of Cyber Crime Study
Benchmark Study of U.S. Companies
Despite widespread awareness of the impact of cybercrime, cyber attacks continue to occur frequently and result in serious financial consequences for businesses and government institutions.

Key takeaways from this report include:

- Cyber crimes can do serious harm to an organization’s bottom line. We found that the median annualized cost of cyber crime of the 45 organizations in our study is $3.8 million per year, but can range from $1 million to $52 million per year per company.

- Cyber attacks have become common occurrences. The companies in our study experienced 50 successful attacks per week and more than one successful attack per company per week.

- The most costly cyber crimes are those caused by web attacks, malicious code and malicious insiders, which account for more than 90 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks requires enabling technologies such as SIEM and enterprise threat and risk management solutions.

The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the devastating consequences of an attack.
Leading to fewer reported incidents, ....

After the peak in 2004, the number of companies reporting a security breach has returned to roughly the level seen in 2002. However, audits and controls in some companies mean that incident statistics are probably understated. For example, companies that carry out risk assessments are four times as likely to detect identity theft as those that do not. In addition the average seriousness of incidents has increased, so roughly a quarter of companies had a serious breach, the same as in 2005.

<table>
<thead>
<tr>
<th>Companies that had a security incident in the last year</th>
<th>45%</th>
<th>72%</th>
<th>96%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of incidents, median (mean)</td>
<td>6</td>
<td>15</td>
<td>&gt;400</td>
</tr>
<tr>
<td>(100)</td>
<td>(200)</td>
<td>(&gt;1,000)</td>
<td></td>
</tr>
<tr>
<td>Average cost of worst incident in year</td>
<td>£10k to £20k</td>
<td>£90k to £170k</td>
<td>£1m to £2m</td>
</tr>
</tbody>
</table>

But some big exposures remain.

Confidential information is increasingly at risk, especially in large businesses, where:

<table>
<thead>
<tr>
<th>Exposures</th>
</tr>
</thead>
<tbody>
<tr>
<td>13% have detected unauthorised outsiders within their network.</td>
</tr>
<tr>
<td>9% had fake (phishing) emails sent asking their customers for data.</td>
</tr>
<tr>
<td>9% had customers impersonated (e.g., after identity theft).</td>
</tr>
<tr>
<td>6% have suffered a confidentiality breach.</td>
</tr>
</tbody>
</table>

Many companies are not doing enough to protect themselves and their customers' information.

<table>
<thead>
<tr>
<th>Exposures</th>
</tr>
</thead>
<tbody>
<tr>
<td>10% of websites that accept payment details do not encrypt them.</td>
</tr>
<tr>
<td>21% spend less than 1% of their IT budget on information security.</td>
</tr>
<tr>
<td>35% have no controls over staff use of Instant Messaging.</td>
</tr>
<tr>
<td>48% of disaster recovery plans have not been tested in the last year.</td>
</tr>
<tr>
<td>52% do not carry out any formal security risk assessment.</td>
</tr>
<tr>
<td>67% do nothing to prevent confidential data leaving on USB sticks, etc.</td>
</tr>
<tr>
<td>78% of companies that had computers stolen did not encrypt hard discs.</td>
</tr>
<tr>
<td>79% are not aware of the contents of BS 7799/ISO 27001.</td>
</tr>
<tr>
<td>84% of companies do not scan outgoing email for confidential data.</td>
</tr>
</tbody>
</table>

To protect your business in this changing world:

1. Understand the security threats you face, by drawing on the right knowledge sources.
2. Use risk assessment to target your security investment at the most beneficial areas.
3. Integrate security into normal business behaviour, through clear policy and staff education.
4. Deploy integrated technical controls and keep them up to date.
5. Respond quickly and effectively to breaches, e.g., by planning ahead for contingencies.
CSI Computer Crime & Security Survey
The latest results from the longest-running project of its kind

By Robert Richardson, CSI Director

For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they’ve taken to secure their organizations. Over 500 security professionals responded. Their answers are inside...

2008 CSI Computer Crime and Security Survey

Key Findings
This year’s survey results are based on the responses of 522 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. This is the 13th year of the survey.

The most expensive computer security incidents were those involving financial fraud...
...with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with “bot” computers within the organization’s network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.

Virus incidents occurred most frequently...
...occurring at almost half (49 percent) of the respondents’ organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

Almost one in ten organizations reported they’d had a Domain Name System incident...
...up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

Twenty-seven percent of those responding to a question regarding “targeted attacks”...
...said they had detected at least one such attack, where “targeted attack” was defined as a malware attack aimed exclusively at the respondent’s organization or at organizations within a small subset of the general business population.

The vast majority of respondents said their organizations either had (68 percent)...
...or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.
PISSED OFF AND RIPPED OFF
AND LEFT FEELING RESPONSIBLE

Adults all over the world are feeling angry, annoyed and cheated by cybercrime.
It causes intense emotions...

Top 10 emotional reactions to cybercrime

- 58% ANGRY
- 51% ANNOYED
- 40% CHEATED
- 38% UPSET
- 38% FRUSTRATED
- 36% VIOLATED
- 30% DISGUSTED
- 30% DISTUSTFUL
- 29% FEARFUL/WORRIED
- 26% HELPLESS
Symantec Internet Security Threat Report

<table>
<thead>
<tr>
<th>Overall Rank 2009</th>
<th>Country</th>
<th>Percentage 2009</th>
<th>Percentage 2008</th>
<th>2009 Activity Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>19%</td>
<td>23%</td>
<td>Malicious Code: 1, Spam Zombies: 6, Phishing Hosts: 1, Bots: 1, Attack Origin: 1</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>8%</td>
<td>9%</td>
<td>Malicious Code: 3, Spam Zombies: 8, Phishing Hosts: 6, Bots: 2, Attack Origin: 2</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>Malicious Code: 3, Spam Zombies: 11, Phishing Hosts: 4, Bots: 12, Attack Origin: 4</td>
</tr>
</tbody>
</table>

Table 1: Malicious Activity Rank
Source: Symantec
Figure 1: Total reports processed and proportion considered potentially criminal, by category

Figure 2: 2006-2009
Child sexual abuse URLs and domains, worldwide

Figure 4: The top level domains most often used for distribution of child sexual abuse content in 2009
THE COST OF CYBER CRIME.

A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE.

STUDY METHODOLOGY

To address the complexity of less understood cyber crime we have developed a causal model, relating different cyber crime types to their impact on the UK economy. The model provided a simple framework to assess each type of cyber crime for its various impacts on citizens, businesses and the Government. We used the model to map cyber crime types to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macro-economic models of the UK. We then calculated the magnitude of the costs of cyber crime using three-point estimates (worst-case, most-likely case and best-case scenarios), focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors.

During this study, we have drawn on information in the public domain, supplemented by the enormous knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private sector organisations. We are indebted to those individuals and organisations who contributed their time and expertise.
Cost of IP theft by industry sector

Espionage impact by business sector
Defining CyberWar

- Attacks solely from computers to other computers
- An attack that is equivalent to a conventional “kinetic” attack – damage measured in terms of intensity, scope and duration

Or anything less you care to put the name to?
Defining CyberWar

Legal Implications - “The Law of Armed Conflict”

• Retaliation justified by UN Charter Article 51 – “Self Defence”

• Defence must be:
  ➔ Militarily necessary
  ➔ Proportionate
  ➔ Avoid collateral damage to innocent third parties

Retaliation implies you are sure you know who is attacking you – the problem of attribution
We have chosen, however, to use the term ‘cyber warfare’ in order to focus discussion on activities which are ‘warlike’ but which may or may not be ‘war’ per se. ‘Warfare’ is a more open-ended term, more useful in exploring an environment that is not only virtual but also largely uncharted. However, some of the activities described here as cyber warfare might well have little to do with war at all, as conventionally understood.

**Threats**

- Direct military threats
- Indirect and non-military threats
- Terrorism and extremism
- Cyber espionage
- Economic cyber crime
- Psychological cyber warfare
Out of all this definitional and statistical confusion ....

Is there a route which will help us understand the problems

And analyse the risks  ???
Cyber Weapons

- Concept focuses on weapons’ capabilities and qualities
- Recognises there are several different types
- Forces analysts to recognise limitations of cyberweapons as well as advantages –
  ➔ What are all the ingredients necessary for success?
- Says nothing immediate about reasons for deployment
- Forces analysts to think about aims, motives, strategies of deployers
CyberWeapons

- Operate in CyberSpace
- Attacks can be mounted from anywhere on to Internet-Connected Computers
  - Alternate attacks also possible via physical access, but means of access has to be devised
- International – multi-jurisdictional
- Anonymising is trivial / Attribution is difficult
- Basic tools widely available and easy to deploy
  - But simple, well-known tools are also easily detected
CyberWeapons

- Tools require very little resource to deploy
- Usually people don't die
- It is difficult to cause direct physical damage
- To be a weapon, it needs to have the ability to be controlled and directed
- There may be consequential losses
Types

- Use of Social Networks / Feeds / Psy-Ops
- Internet Blocking
- Unauthorised computer access
- Web-site take-over / defacement
- Denial of Service / Distributed Denial of Service
- BotNets
- Computer wiping
- Computer take-over / remote control
- Physical compromise of some computer devices
- Attacks on computer / comms switches
- Computer impersonation
Motivations for Deployment

- **Recreational hacking**
  - To gain notoriety

- **Propaganda**
  - To gain acceptance of a view
    - Web defacement
    - Short-period DDOS

- **Hactivism:**
  - Another form of civil disobedience
    - Web defacement
    - Short-period DDOS
Motivations for Deployment

- Espionage
- As part of a scheme to make money
  - Extortion / Protection
- Social Control
  - Internet Blocking
- Demonstration of political power / intent
- To disrupt enemy activities
- Force multiplier for conventional weaponry
War Motives

- Dispute over Territory
- Access to Essential / Valuable Resources
- Ethnicity
- Religion
- Remedying of Earlier Grievance
- “Power”
Steps towards Total War

- Diplomatic Exchanges
- Demonstrations by Concerned Citizens
- Summoning of Ambassador
- UN Resolution
- Going on Manoeuvres/Exercises
- Sanctions
- Psy-Ops
- Brief Interruption of Essential Services
- Slight Territorial Incursion
- Blockade
- Insurgency
- Brief Attack and then Pause
- Total War
Steps towards Total War
Sub-State Actors

- Political Activity
- Demonstrations – legal
- Demonstrations – civil disobedience but illegal
- Bombs – no significant harm intended
- Bombs aimed at significant harm
- Assassination of key figures
- Suicide Bombs: large scale terror
CyberWeaponry Escalator

- Propaganda websites, blogs, feeds
- Website defacement, spam
- Psy-Ops
- Website DDOS – short-term incapacity
- Website DDOS – longer term aims
- Data destruction
- Attacks on CNI, Military
  - Logical
  - Physical
The words we use to describe things influence our thoughts about what phenomena we are viewing – and the sorts of solutions to any problems that might exist.
In Cyber War:

• What is the test for “war”?
• How important is the “cyber” element?
• What are the objectives and motives for the conflict?

In Cyber Crime:

• How important is the “cyber” element?
• What are the objectives and motives of the criminal?
Defining CyberWarfare

Peter Sommer

P.M.Sommer@lse.ac.uk
Peter@pmsommer.com