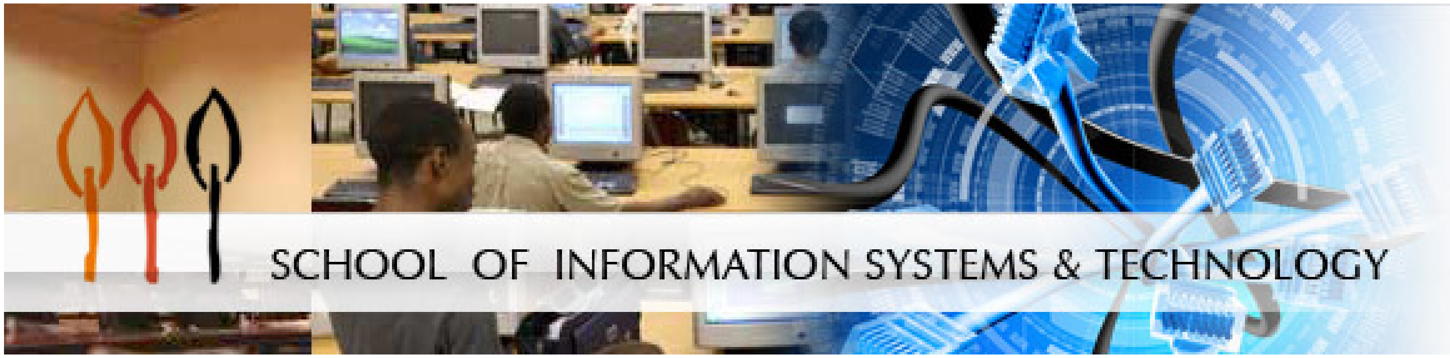


UNIVERSITY OF
KWAZULU-NATAL

Weaponisation of the Net

B van Niekerk

MS Maharaj

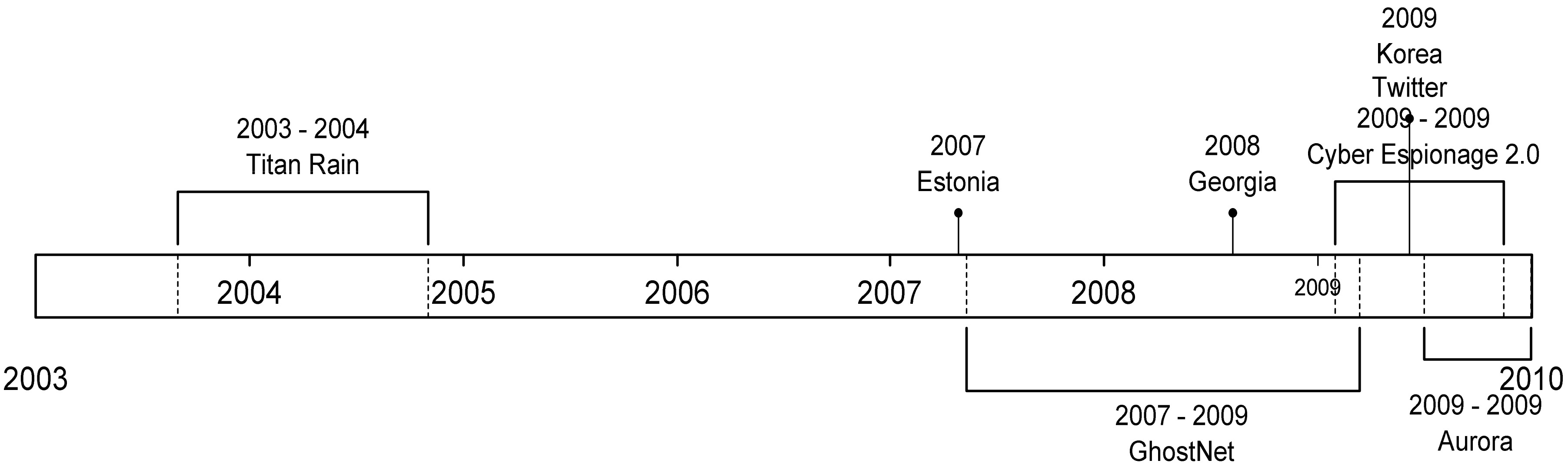
Introduction

- Concern over the possibility of cyber-based attacks societies & nations.
- Information war / Cyber-war not limited by physical or political boundaries.
- New tools becoming available to conduct attacks.
- Consequently, legislation is being introduced in attempt to counter malicious activity.
- South Africa listed as 7th on the global cyber crime list.

Outline

- Incident case studies
- CERT data analysis
- Implications for Africa
- Legislation
- Conclusion

Incident Timeline



Incidents (1)

- **Titan Rain (2003-2004)**
  - Cyber-espionage
  - 4 facilities compromise in 12 hours during Nov 2004
- **Estonia (2007)**
  - Cyber-war
  - Large scale DDoS attacks
  - Major bank lost $1 million
  - NATO Cyber Defence Centre

Incidents (2)

- **Georgia (2008)**
  - Cyber-war; in conjunction with Russian involvement in South Ossetia
  - Large scale DDoS attacks
  - Hindered communications
- **South Korea (2009)**
  - DDoS attacks against websites in US and South Korea
- **Twitter Attacks (2009)**
  - 2 DoS attacks, linked to Georgia and S. Korea

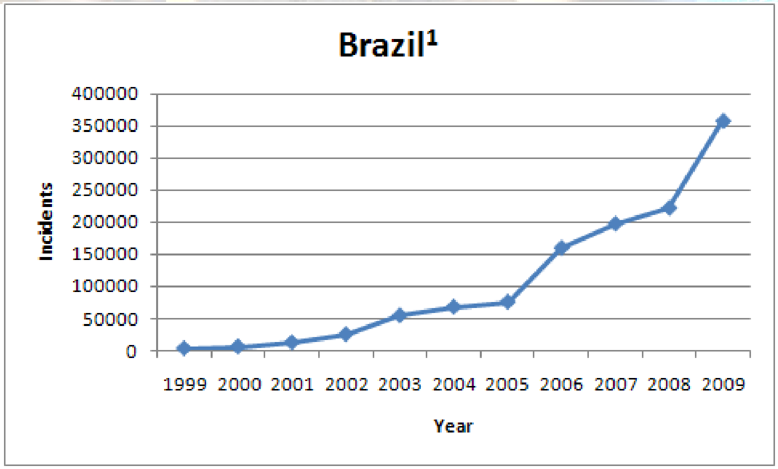
Incidents (3)

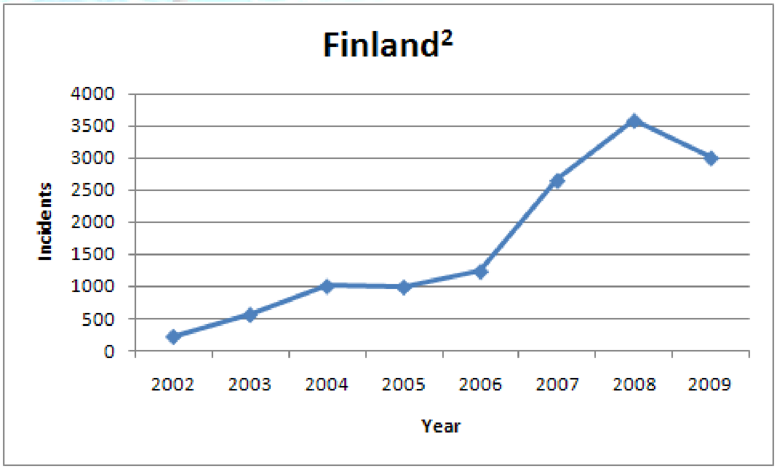
- **GhostNet & ShadowNet (2007-2010)**
- Cyber-espionage
- Appeared to be Chinese targeting Dalai Lama
- 1300 computers infected in 103 countries.
- Emails with social engineering contained malicious code.
- A more sophisticated and persistent version released in 2009, targeting primarily India.

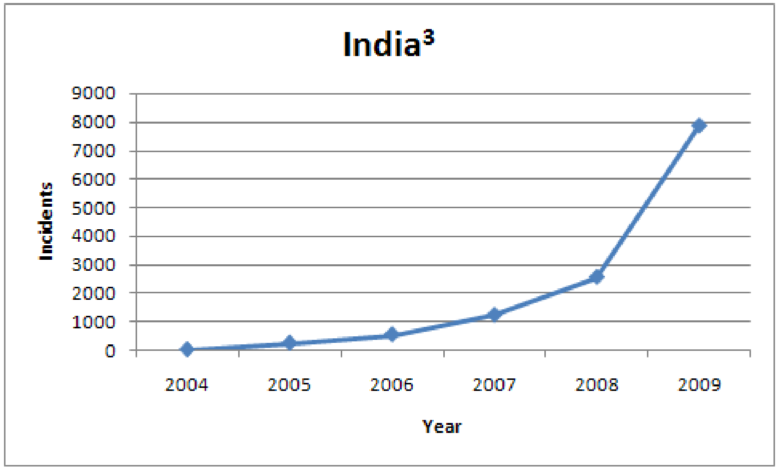
Incidents (4)

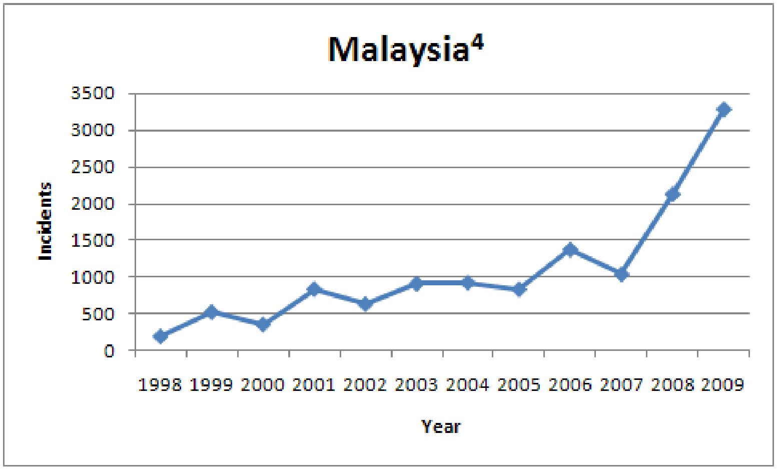
- **Google: Operation Aurora (2009-2010)**
- Appears to be state-sponsored corporate espionage.
- Lawyers suing China for software piracy were targeted by a cyber-attack.
- Possible for attackers to gain complete control over compromised computers.
- **Other Incidents**
- Social & political unrest.
- Wikileaks.

CERT Data Analysis (1)









Sources:

1. (CERT.br, 2010), 2. (CERT-FI, 2010), 3. (CERT-In, 2010), 4. (MyCERT, 2010)

CERT Data Analysis (2)

Top Threats by Prevalence

	Brazil[1]	**Finland[2]**	**India[3]**	**Malaysia[4]**	**Netherlands[5]**
1	Fraud	Malware	Malware	Website & malware	Malware
2	Scanning	Intrusions	Intrusions	Phishing	Vulnerabilities
3	Worm	Fraud	Social engineering	Virus & malicious code	Other
4	Web server attack	Virus & malicious code	Vulnerabilities	Scanning	Phishing
5	Other	Harassment	Systems break in	Other	Hacking

Sources:
1. (CERT.br, 2010)
2. (CERT-FI, 2010)
3. (CERT-In, 2010)
4. (MyCERT, 2010)
5. (GovCERT.NL, 2010)

Implications for Africa

- Increasing availability of internet.
- Lack of awareness.
- South Africa 7th, Nigeria 3rd in cyber-crime list
- South Africa does experience attacks on infrastructure
- South Africa & Morocco still developing CSIRTs
- Tunisia, Mauritius, Kenya have operational CSIRTs

Legislation

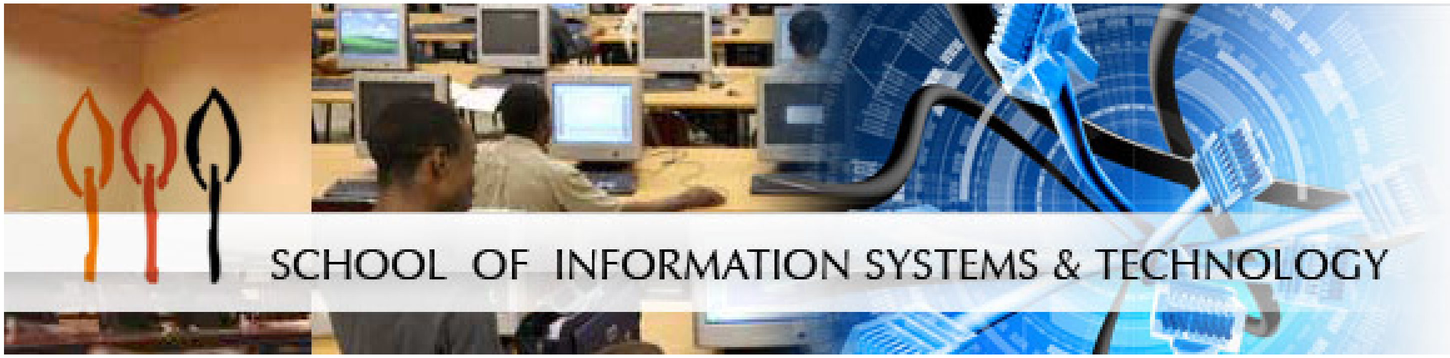
- Electronic Communications & Transmissions Act
- Regulation of the Interception of Communications Act
- Protection of Personal Information Act (2009)
- Draft Cyber-security policy (2010)
- Still to be tested in court

Legislation

- Problems with definitions.
- In the US, cyber-espionage is not considered an attack.
- DoS is an attack, and may be considered an act of war.
- But what if it was a 15 year old?
- How do you prove a cyber attack was state sponsored?

Conclusion

- Available tools & incidents indicate the internet is becoming increasingly weaponised.
- International collaborations & agreements regarding cyber-security issues.
- South Africa has not tested the relevant legislature and does not have fully operational CSIRTs.
- Organisations need to take some responsibility for security compliance.
- Increasing bandwidth may increase vulnerability.



Thank you.
Questions & comments...

B van Niekerk	991160530@ukzn.ac.za +27 (0)31 260 8521
MS Maharaj	maharajms@ukzn.ac.za +27 (0)31 260 8023