SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

MANCOSA

Web 2.0 as an Attack Vector against Strategic Security

Brett van Niekerk – School of IS&T, UKZN
Trishana Ramluckan - Mancosa
Manoj Maharaj - School of IS&T, UKZN

defence
Department: Defence
REPUBLIC OF SOUTH AFRICA

ARMSCOR

CSIR
our future through science

LEDGER University Research Program

MICSSA 2011

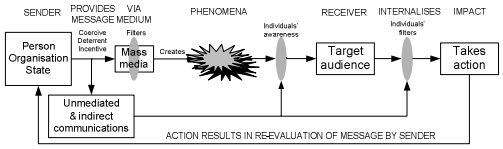
Introduction

- Web 2.0 is becoming one of the most pervasive technologies.
- Results in a new threat landscape:
  - Mass demonstrations
  - Targeted attacks
  - Increased military use of Web 2.0
- Propose models describing the use of Web 2.0 in mass influence operations and targeted attacks.

Information Warfare

- Actions taken to attack & defend information assets
- Multiple contexts / spheres:
  - Global – military, political
  - Corporate/economic
  - Social/community & personal
- Functional areas:
  - Network warfare & information infrastructure warfare
  - Intelligence-based warfare
  - Psychological operations

PSYOPs: Message Flow Model



Adapted from Cox (1997)

Web 2.0

- Concept of user-generated content, information sharing, collaboration, and collective intelligence.
- Many-to-many communications.
- Content on demand.
- Security issues:
  - Users expect Web 2.0 style information access at the workplace.
  - Users are trusting - possibility of leaks.
  - 'Hacking Executives' Dhanjani, Rios, & Hardin (2009), *Hacking: The Next Generation*
  - More technical vulnerabilities than traditional Web.
  - Phishing & malware

Web 2.0: Security Issues & IW Applications

As of October 2010, presented at the Workshop on ICT Uses in Warfare and the Safeguarding of Peace:

- Israeli military operation cancelled due to careless posting
- British head of intelligence had personal and family information posted on Facebook
- Wikileaks
  - Helicopter gunship
  - Afghanistan war logs
- Israel training specialist 'Web 2.0 units' to monitor social media and 'Flotilla Fiasco'
- US military undecided whether to ban social media

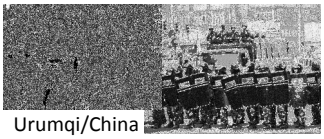
Web 2.0: Security Issues & IW Applications

Since October 2010:

- Wikileaks
  - Iraq War logs
  - Diplomatic cables
  - Crowdleaks – HBGary hack.
- US Military & Persona software
- US military appears to have allowed social media
- False flag operation on LinkedIn – Pentagon warning
- 'Robin Sage' experiment

Protests – Oct 2010

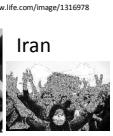
Philippines http://www.life.com/image/1316978



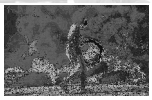
Urumqi/China

Moldova

Iran

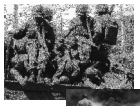


Protests – Subsequently...



Mozambique

Tunisia



Uganda

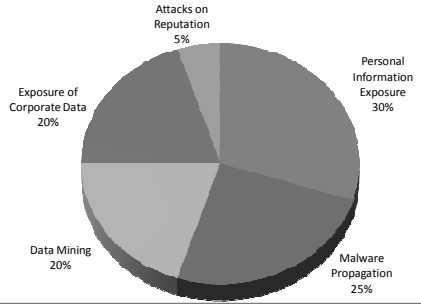
Egypt

N. Africa & Middle East...

Web 2.0: Security Issues & IW Applications

- 2nd most prevalent type of malicious website
- False Flag operation on LinkedIn
  - Fake profile, using photo of retired colonel
  - Attempting to contact members of US IO community
- 'Robin Sage' experiment
  - Fake profile, claiming to have advanced degree, work in network defence for military
  - Many senior officials did not realise this was a fake profile
- Sex appeal is top social engineering tool
  - Can use to get target's attention, lure targets into 'embarrassing behaviour'.

Trends on social media attack types



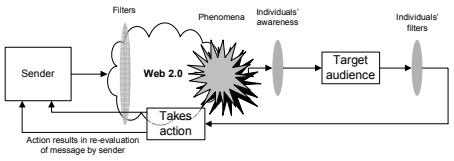
Source: *Trustwave Global Security Report 2011*

Proposed Models

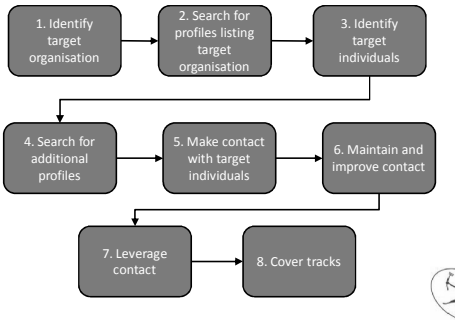
3 Models will be proposed:

- A message flow model for Web 2.0 in mass communications;
- Targeted attacks against individuals;
- The role of Web 2.0 in IW.

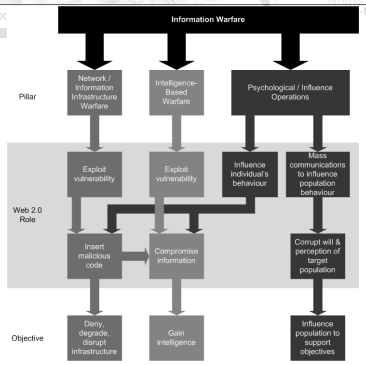
Message Flow Model for Web 2.0



Framework for Targeted Attacks using Web 2.0



Web 2.0 in IW



Countermeasures

- Banning access.
  - Access through personal device – restrict access.
- Monitoring.
  - Will not prevent, only detect.
- Education & awareness training.
  - Human error, apathy.
- Defence-in-depth.
- Social media honey-pots?

Conclusion

- Web 2.0 is a technology based on information sharing.
- These technologies can be seen as a threat / IW tool.
  - Mass communications / influence operations
  - Target individuals.
- Models were proposed to describe Web 2.0 attacks.
- Suggest a defence-in-depth approach to mitigate Web 2.0 threats.
- Social media 'honey-pots' may be used to gain more information on attack methodologies using Web 2.0.

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

MANCOSA

Thank You.
Questions / Comments / Discussion

Brett van Niekerk
School of IST&T, UKZN
+27 (0)31 260 8521
vanniekerkb@ukzn.ac.za
brettvn@gmail.com

Trishana Ramluckan
Mancosa
+27 (0)31 300 7200
trishana.ramluckan@mancosa.co.za
trishr@live.co.za

Manoj Maharaj
School of IS&T, UKZN
+27 (0)31 260 8521
maharajms@ukzn.ac.za

defence
Department: Defence
REPUBLIC OF SOUTH AFRICA
ARMSCOR
CSIR
LEDGER University Research Program