National Security and the impact of Cyber Threats on the average citizen.

JC Jansen van Vuuren
Research Group Leader: Cyber Defence
CSIR
Broadband access in South Africa

- Broadband Policy for South Africa
- Current RSA Europe link 120 Gbps and RSA Asia link 130 Gbps
- Future 12.28 TB
SUB SAHARAN UNDERSEA CABLES

CURRENT

ANTICIPATED

How to own a continent

STEALING THE NETWORK

CSIR our future through science
Broadband access in South Africa

• Result in higher cyber crime due to the more opportunities for computers to be exploited.
• This has been witnessed in countries such as Brazil, Turkey and Poland.
• In the Broadband policy the government recognise its role as the provider of cyber security as part of national security.
Classification of cyber threats

- Data threats - *Data Interception, Data Modification and Data theft.*
- Network threats - *Network Interference, Network Sabotage*
- Access threats - *Unauthorized Access, Virus Dissemination, Aiding and Abetting*
- Other related threats - *Computer-Related Forgery and Computer-Related Fraud.*
The provision of security to the state and of human security to its citizens as well as the protection of national and human interests together with state borders through the projection of national power.

Phahlamohlaka 2008
Jablonsky National Power

- \( Pp = (C + E + M) \times (S + W) \) in which:
  - \( Pp \) = Perceived power
  - \( C \) = Critical mass: population and territory
  - \( E \) = Economic capability
  - \( M \) = Military capability
  - \( S \) = Strategic purpose
  - \( W \) = Will to pursue national strategy
National security analysis

- **Natural determinant**
  - Geography and resources
  - Population

- **Social determinant**
  - Economic,
  - Political,
  - Military,
  - Psychological,
  - Informational
National security analysis
Natural determinant analysis

- **Population**
  - Highest growth in internet users
  - World 29% internet users; Africa 3.9% south Africa 7%
  - Threads increase, especially botnets
  - If infected Pc’s person, pandemic

- **Geography and resources**
  - Africa 80% infected – UK 30% infections
  - Poverty
    - piracy software
    - Anti viruses
Worldwide infections of computers
National security analysis

Social determinant analysis

- **Economical**
  - SARS payments to wrong people
  - World cup
  - SAA
  - Bankserv

- **Political**
  - Donations using political figures names
  - Rumours causing instability

- **Military**
  - Attacks on other systems across the globe.
  - DOS attacks without government or military knowledge
National security analysis
Social determinant analysis

- **Psychological**
  - Messages on website with DOS attack
  - Social Networks

- **Informational**
  - Influence on average citizen access, service delivery
Practical Example: Identity theft

- Knowledge prior to search
  - Name and surname
  - University where he studied
Practical example
Danie Van der Schyff
Programmer at Intecon
Johannesburg Area, South Africa

Current Position
Programmer at Intecon

Industry Information Technology and Services

Danie Van der Schyff’s Experience

Programmer
Intecon
(Privately Held; 51-200 employees; Information Technology and Services industry)
Currently holds this position
## Work information

<table>
<thead>
<tr>
<th>Company name</th>
<th>Intecon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occupation</td>
<td>Programmer</td>
</tr>
<tr>
<td>Colleagues</td>
<td>- Help desk</td>
</tr>
<tr>
<td></td>
<td>Trevor Mohasoa - Help desk</td>
</tr>
<tr>
<td></td>
<td>Marista Conradie - Receptionist and Personal Assistant</td>
</tr>
</tbody>
</table>

## Personal information

<table>
<thead>
<tr>
<th>Email address and username/alias</th>
<th><a href="mailto:einad5@gmail.com">einad5@gmail.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td></td>
</tr>
</tbody>
</table>
Data gathered from Google profile and gmail email address

- Information gathered from Google Buzz account
  - Operating System preference (complains about Mac and Linux a lot on his posts)
  - Religious and political views
  - More friend links, frequent contacts and topics of discussions
  - Link to a Blog controlled by him
    (http://www.blogger.com/profile/09)

- Most Buzzed sites
  - Dilbert
  - News24
  - CodeProjects
Data from Google profile and gmail email address

- Google profile -
- Found Twitter account ([http://twitter.com/einad5](http://twitter.com/einad5))
- Information gathered from Twitter account
  - Contains mostly the same data as Buzz but contains a few more links to friends and family especially father and sister (names + occupations)
Data from his personal Blog

• Location: Pretoria, South Africa
• Information on his favourite books, movies and games
• Information about a car he recently bought
• Photos of the car (presumably taken at his home) showing the number
Data from the university website

- Found previous community based assignment he worked on for studies
- Site contained his cell number and degree information.
- Found new email address: s26358345@tuks.co.za/siand@tuks
- Found student number: 26358345
Data from the university website

• Using his student number
  – Found degree studied: Bachelors in Information Technology, 2006-2009
  – Found information on his collaborative projects at the university (friends, subject, interests)
  – Discovered he tutored subjects at the university
    • COS 110 – Introduction to Java
    • COS 212 – Data Structures and Algorithms
    • COS 214 – Design Patterns
  – Can guess his year of birth
Family info

- Two people with the surname Van Der Schyff also posted on his Buzz account
  - Aneen van der Schyff (Possibly Mother)
  - Daniel Van Dr Schyff (Possibly Father)
Information on mother

- Mothers google Buzz account is closed to the public so no info could be retrieved via google Buzz.
- Localized google on mothers name - several references with similar name in Pretoria North High School.
- Articles age shows not possibly be Danie’s mother but might be family. Person active in sport (several endurance events) Would expect her to be at Two Oceans April 2011.
Information on father

• From Buzz account find gmail address as well as security tips from specific company.
• Used his person info plus standard email address of company to determine if employee
• Found a person working for company plus work phone number and short bio
• From his bio we determined could possibly be Danie’s father.
• Not much else was found except a LinkedIn account.
Lessons learned

- Lock Social Network accounts
- Do not display personal information e.g. Id numbers
- Safe surfing (adware, spyware) – antivirus
- Desktop security: passwords, file sharing etc.
Important for national security to

- Monitor rural areas and identify the risks
- Set up awareness programs to educate citizens
- Implement a CSIRT in RSA
- Appoint national security advisor for RSA reporting to president