Co-operation with Law Enforcement Agencies in South Africa

19 September 2008

Internet Service Providers Association

Agenda

- About ISPA
- IMPACT
  - Is cyber-terrorism real?
- Content and DNS
- People trafficking
- Training
- Is this a “bad thing” for ISPs?
- Read my lips – “no new laws”

Internet Service Providers Association

About ISPA

- **Internet Service Providers' Association**
  - Largest industry association representing the Internet industry
  - Two officers on the Board of .ZA DNA
  - Represent largest group of registrars
  - Also has three registries as members
- **Membership by category**
  - Large access providers: 12
  - Medium access providers: 10
  - Small access providers: approx 110
    - The majority of ISPA's small members (and also a majority of all members) are classified as SMMEs
- **Honorary members**
  - Affiliates and honorary members – 12
  - Include e-Schools Network, NetDay, SchoolNet SA, TENET
- **Notable exception**
  - Telkom SA Limited
  - For historical reasons will not join

Internet Service Providers Association

Structure of the Market

- **Previously governed by the 1996 Telecommunications Act**
  - ISPs as VANS – value added network service providers
  - Telkom under its licence + VANS licence
  - MNOs – their licences
- **Now covered by 2005 Electronic Communications Act**
  - All former VANS have network and service licences

Internet Service Providers Association

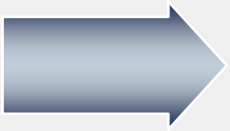
Change in Market Structure

PTT license (eg Telkom)

TV Broadcasting License (eg SABC)

Sentech (wireless / Signal) license

VAN license (eg ISPs)



Content Services

Applications Services

Network Services

Infrastructure Service

Under the old licensing framework all activities related to the provision of a particular service are vertically integrated for the provision of that service

The new licensing framework promotes vertical separation between infrastructure, network, applications, and content

Internet Service Providers Association

Mapping the Old to the New

Content Services	Broadcast Licence	TV / Radio
	No licence for other content	All other
Applications Services	Electronic Communications Service Licence	Voice / data (Internet) / fax
Network Services Infrastructure Service	Electronic Communications Network Service Licence	Fixed line / wireless

Internet Service Providers Association

Participation in IMPACT

- Government invitation to join IMPACT
- Invited ISPA
- Looking to establish a CERT
- Not yet operational

Internet Service Providers Association

What is IMPACT

- The International Multilateral Partnership Against Cyber-Terrorism (IMPACT) is the first global public-private initiative against cyber-terrorism. IMPACT is dedicated to bringing together governments, industry leaders and cybersecurity experts to enhance the global community's capacity to prevent, defend and respond to cyberthreats. IMPACT's permanent secretariat is headquartered in Cyberjaya, Malaysia.
- The foundation of IMPACT is built on four key dynamic pillars, each focused on specific functions that are designed to fulfil the vision of this world's first international multilateral initiative against the real threat of cyber-terrorism. These four pillars are:
  - **Centre for Global Response**
  - **Centre for Policy & International Cooperation**
  - **Centre for Training & Skills Development**
  - **Centre for Security Assurance & Research**

Internet Service Providers Association

Why IMPACT

Dependency of societies on information and communication technologies.
This dependency makes societies highly vulnerable to cybercrimes

- Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading
- Spam nuisance and carriers of malware
- Child pornography and sexual exploitation on the internet increasingly commercial
- Offenders increasingly organising for crime aimed at generating illicit profits
- Offences related to identity theft
- Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)
- Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)
- Growing risk of cyber-attacks against critical infrastructure

But: Vast majority of people use ICT for legitimate purposes
Need to balance security and civil rights concerns

Internet Service Providers Association

Terrorist Use of the Internet

- **Attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life**
  - Real or imagined
  - Only one actual example
    - Estonia
- **Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training**
- **Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses**

BUT

- **Cybercrime is very real**
- **Techniques and technologies (botnets, scripts, root kits) used for spam, DDoS attacks, hacking etc – could be used**

Internet Service Providers Association

People Trafficking

- **Task team on child pornography, trafficking on women and children and related issues**
- **Also includes prostitution**
  - Supposed to be focussed on under-age prostitution
  - Because of legal uncertainty – covers adult prostitution as well
- **ISPA assisting in training and understanding of the Internet and how it works**

Child Pornography

- Film and Publications Board
- Now a member of In Hope
- ISPA Assisting
- Training and awareness
- Process regarding a “protocol” in draft

Police

- **We struggle to get Internet related crime investigated and prosecuted**
  - ADSL log-in theft
  - Spam
  - Etc
- **Co-operating with training**

Responses

- New laws
- Existing laws
  - Convention on Cybercrime and the Convention for the Prevention of Terrorism
  - In SA - ECT Act (Cyber Crimes) and FICA / PoCA
  - ECT Act - critical databases
- New laws?
- Show me the money
  - Government to promote through procurement
- Is this bad for ISPs?
  - Costs
  - More secure networks
    - Fewer exploits
    - Less spam

Internet Service Providers Association

Conclusions

Attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interestets, including loss of life

Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism recruitment or training

Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

Covered by the

- Convention on Cybercrime

in combination with the

- Convention for the Prevention of Terrorism

Internet Service Providers Association

Thank you

Questions?