CentralNic Group plc
Specialist developer and operator of software platforms for domain names

Long-running commercial Registry Service Provider entering its 23rd year

Listed on the London Stock Exchange (AIM: CNIC) with all the compliance and transparency requirements of a public company

300 staff in 14 countries

Manager of SK-NIC and Services Provider to 8 other ccTLDs
Legal and Regulatory Trends in relation to Illegal activity online

- Consensus of more abuse more harassment, fake webshops, fraud, phishing, spam, pharming on the Internet

What negative consequences, if any, do you foresee if cross-border legal challenges on the Internet are not properly addressed?

- 60% Legal Uncertainty
- 54% Loss of some key cross-border benefits of the Internet
- 54% Restrictions of expression
- 52% Compliance costs for online businesses
- 35% Inability to address online abuses

Top 5 answers by respondents

SOURCE: Internet & Jurisdiction Policy Network Internet & Jurisdiction Global Status Report 2019
Responsibility of intermediaries is changing from exemption of liability to responsibility of intermediaries. Registries cannot ignore the pressure to take more action to prevent, mitigate or stop harm online.
What are the current trends for ccTLD operators in relation to domain abuse and how to manage the responsibility to take actions?
What Methodology to manage abuse and illegal activities?

Levels of actions
- Types of abuse
- Thresholds

Notices
- Notices components
- Notices types
- Due Diligence by Notifiers

Actions
- Types of actions

Procedural Guarantees
- Transparency
- Notifications to Registrants
- Recourse for Registrants/Appeals
What types of abuse?  What thresholds should be used? What Actions

Abuse widely accepted:
- Botnets
- Malware
- phishing
- Pharming
- Spam (most but not all)

Content related Issues
- Trademark infringement
- Fraud, fake webshops
- Phishing
- Pharming

- Child Sexual Abuse Materials

- Illegality depending upon Jurisdictions
- Illegal gaming, betting,
- pornography
Protection of Rights of Third Parties use of UDPR via WIPO or own managed Dispute Resolution Policies

- WIPO – 75 ccTLDs
  - WIPO ccTLD program launched in 2000 as a body under the UN operates with the 6 UN languages
  - WIPO helps establish policies to curb abusive registrations and sets minimum standards for IP protection

- ccTLD manage Abuse most others have their own ADR (As we learned at APTLD KL Sept)
  - MYNIC uses its MYDRP
  - VN has its Domain Name Dispute Resolution Procedures
  - .NZ Dispute Resolution Service
  - .SK Alternative Dispute Resolution (UDRP)
European Union laws relating to illegal content online

- EU has many measures both binding and non-binding to – Directive to combat sexual abuse and sexual exploitation of children and child pornography,
- The Terrorism Directive (Interpol – removing online content)
- Proposed measures to reform copyright and the Audio-Visual Media Services Directive (AVMSD)
- Code of Conduct on Countering Illegal Hate Speech Online
- Guidance on Unfair Commercial Practices
- MOU on counterfeiting goods
KEY EU regulation – E-COMMERCE DIRECTIVE

- For Registries, Registrars and online platforms the Directive established some limitations to liability of certain online platforms and intermediaries (i.e., providing mere conduit, caching or hosting services).

- Article 15 of the Ecommerce Directive prohibits Member States from imposing a general obligation on providers to monitor information which they transmit or store nor an obligation to seek facts indicating illegal activity but...

- The Directive requires a development of a rapid and reliable procedures for removing and disabling access to illegal information.

- Thus creates obligation to systematically enhance cooperation with competent authorities and encourages the creation of technical interfaces to allow them to cooperate more effectively.

- Encourages voluntary measures.
IPC3 Intellectual Property Crime Coordination Coalition

Europol’s Intellectual Property Crime Coordinated Coalition (IPC3) has seized 33.654 domain names distributing counterfeit and pirated items online. The websites distrusted items such as counterfeit pharmaceuticals, pirated films, television shows, music, software, electronics and other bogus products. The joint international operation also involved the US National Intellectual Property Rights Coordination Center¹ and law enforcement authorities from 26 countries including EU Member States and third parties², which was facilitated by INTERPOL.

- **33.654** domain names seized
- **12** suspects arrested
- accounts worth over **EUR 1 million** seized.
- Duration 2018 11 months have been reported.
- **27 Countries coordinated:** Albania, Austria, Belgium, Bulgaria, Bosnia and Herzegovina, Colombia, Czech Republic, Denmark, France, Greece, Hungary, Hong Kong-China, Ireland, Italy, Netherlands, Peru, Republic of Korea (South Korea), Republic of Moldova, Republic of Serbia, Romania, Slovakia, Spain, Portugal, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America.
Case Study #1 SK-NIC
What about unlawful activities – cooperation by ccTLDs?

CCTLD .SK Case Study

Action is limited to:

1) Court Orders
2) Police in the jurisdiction
3) Cooperation procedures with the Customs Officers (agreed but no recent cases)

- Policies for .SK domains – include Domain Name Blocking
- 4.6.2.1 distribute malware (viruses, keyloggers, rootkits, exploits etc.),
- 4.6.2.2 feign content relating to a different service (mainly phishing) or
- 4.6.2.3 manage a network of devices infected without authorization for the purpose of executing illegal activity (mainly botnet).

- Not for Spam
- SK-NIC has the rights to block services to a domain name holder, refer matters to ADR
- Local Law Enforcement and

Recent changes of abuse management has been implicated by GDPR – because increased mandatory security requirements change of retention policies but otherwise no change.

- E-evidence Directive

- requirements to be proactive for domain abuse – phishing, botnets, malware and spam
Case Study #2 .NL Netherlands

Case Study .NL – Notice and Take Down at the Registry Level

SIDN roles to illegal content and use

1) SIDN actively strives to keep .NL zone safe and trusted environment by

   a) having knowledge of illegal activities
   b) Stimulating cooperative actions against illegal content (work with hosting providers, registrars, registrants, law enforcement)
   c) Deploying policies that limit illegal activities (includes removing domain names from the zone if proportionate)

Reasoning?
RFC 1591 (Trustee of the domain and duty to serve the community)

Procedure:

- Voluntary, contractual basis (with indemnity given)
- Last resort
- Blatantly Illegal under local laws
- Weigh up the potential damage of removing a domain name (look at proportionality)
- Reversible and appeal possible by refer to an appeals board

- Comply with Dutch laws on Dutch National Notice and Take Down code of Conduct

From August 2017- March 2019 – defected 20,000 suspicious domains

4,455 fake web shops have been removed

What they found:

- 80% suspect domain names were re-registrations registrations deleted domains – registered after the 40 days (registrars which offer automated APIs – scammers wait for domains to be released registered and fully automatically install and standard shore that they make minor changes.)

- Fake Webshops – have Sales, lots of dead links

- The Registry using the database started to identify patterns of registrations, better able than law enforcement.

- Email addresses linked to the registration – were using gmail and 25% were using Chinese email 163.com Many suspicious names were registered during Beijing office hours rather than Dutch office hours. Found common pattern of networks (not necessarily Chinese networks)
Case Study #3 – CentralNic as a RSP
CentralNic as a Registry Services Provider – what we do

- Abuse Monitoring Services – for registry clients mandatory for gTLDs but voluntary for our ccTLD clients (using sources to scan the zonefiles for phishing pharming, malware, botnets, spam)
- Cooperate directly with Law Enforcement to suspend domains
- Framework to Address Abuse Along with industry – Afilias, Neustar, GoDaddy, Donuts, Amazon Registrar, Nominet, Public Internet Registry, Tucows, KeySystems, Name.com, objectives to increase dialogue and cooperation, safety and security of the DNS. *Abuse defined to include: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for other DNS Abuse)
- Cooperation with IWF Internet Watch Foundation – SCAM – implement for all our TLDs (Safeguards around protection of staff and ongoing law enforcement security operations)
- Looking into other International Cyber Crimes Coordination
DNS Abuse vs Content set out some of the complexities for Registries and Registrars

- Content – issues – No universal standards, jurisdictional differences, freedoms of expression,
- Disproportionate and collateral damage (movie fan forums – segregating legitimate content from bad
- However some content should be addressed: 1) CSAM, 2) illegal distribution of opioids online (3) human trafficking, 4) specific and credible incitements to violence

Outcomes: - a step in the right direction
Need for more education for regulators and enforcement of the DNS and its limitations
Need for more collaboration across registries, registrars, and law enforcement