NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

# Bob Downie

## NISCC

## Telecommunications Outreach Team

# NISCC’s Aim

*To minimise the risk to the critical national infrastructure from electronic attack.*

# The CNI Sectors

- Telecommunications
- Energy
- Finance
- Government & Public Services
- Water and Sewerage
- Health Services
- Emergency Services
- Transport
- Hazards
- Food

# An Interdepartmental Centre

## Government

- ~ Home Office
- ~ Trade & Industry
- ~ Cabinet Office

## Security

- ~ Police
- ~ MI5
- ~ CESG

## Defence

- ~ MOD
- ~ DSTL

contribute to

NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

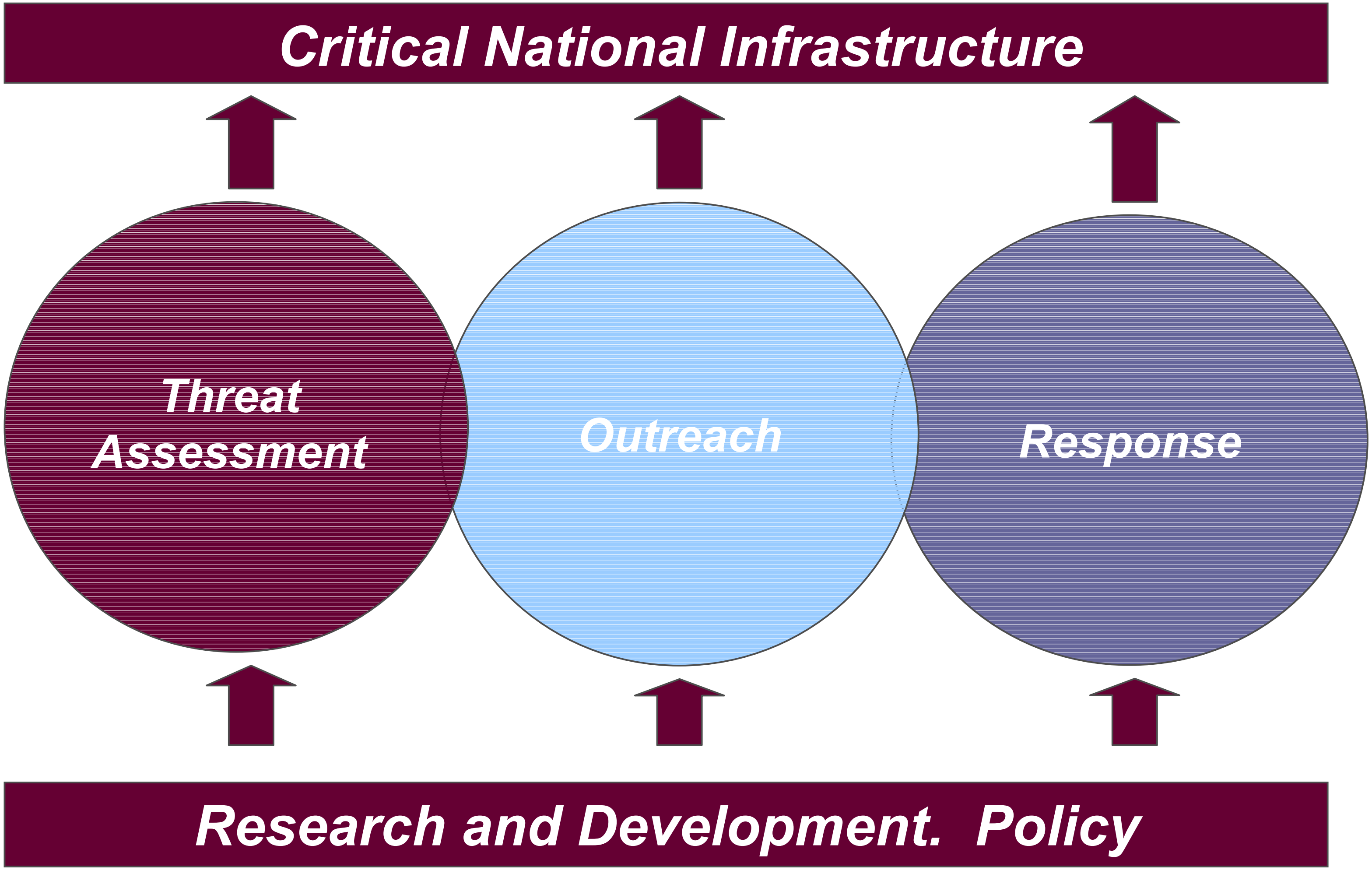
# What is the Threat?

- *foreign states*
- *terrorists*
- *activists*
- *criminals*
- *hackers*
- *insiders*
- *script kiddies*

# However…

- We do not have enough information
- The threat level can change dramatically
- The insider threat is always there (and getting worse)

# How NISCC works



Critical National Infrastructure

Threat Assessment

Outreach

Response

Research and Development. Policy

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

# Investigating and Assessing the Threat

- Making best use of technical, human and open sources to investigate.
- Analysis and assessment.
- Reports and specific threat assessments.
- Disruptions.

# Outreach

Promoting Protection and Assurance:

- Dialogue with all CNI sectors
- Facilitating information exchanges
- Tailored reports

# Response

- Briefings and alerts via UNIRAS
- Responsible disclosure of vulnerabilities
- Assistance with recovery from direct attacks

# Beyond the CNI…

- NISCC alerts and warnings already go wider than the UK CNI.
- NISCC vulnerability disclosure process now world class. Many companies ask us to handle this for them.
- Introduced the concept of WARPs (Warning Advice and Reporting Points) for suitable CNI organisations.

# Vulnerability disclosure

Before…….

Period of greater exposure between disclosure of vulnerability and patches becoming available.

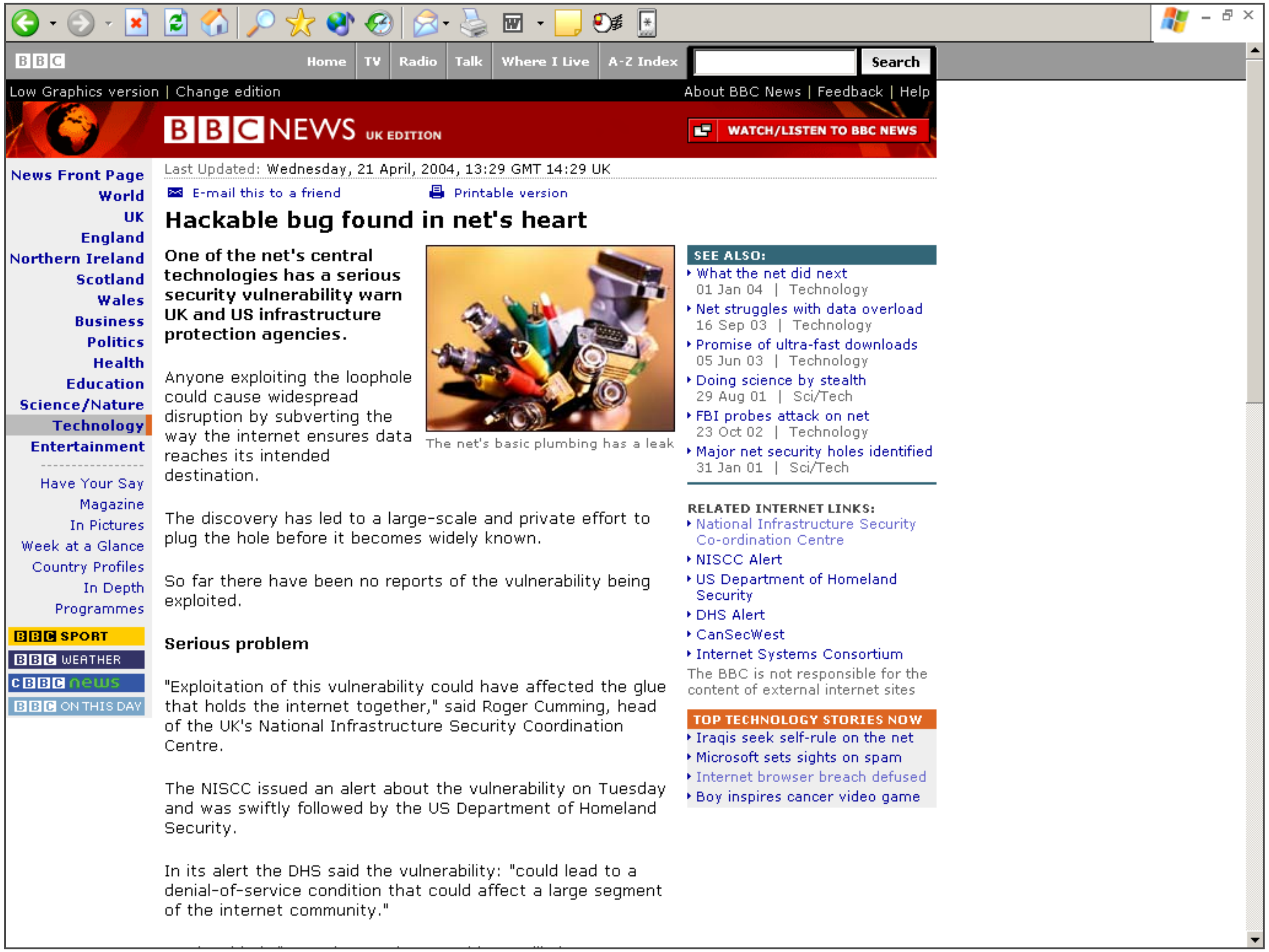
# Vulnerability disclosure…

Now…….

NISCC told of vulnerability.

- Seeks agreements that before set date:
  - Discoverer not to publish.
  - Vendors work on fix, but don’t tell customers
- On agreed date:
  - Discoverer gets credit.
  - Vendors issue patches.
- Use trusted partners to assess the impact and risk
  - This is where we can work together

# TCP/IP Window hits the headlines



Last Updated: Wednesday, 21 April, 2004, 13:29 GMT 14:29 UK

E-mail this to a friend | Printable version

## Hackable bug found in net's heart

**One of the net's central technologies has a serious security vulnerability warn UK and US infrastructure protection agencies.**

The net's basic plumbing has a leak

Anyone exploiting the loophole could cause widespread disruption by subverting the way the internet ensures data reaches its intended destination.

The discovery has led to a large-scale and private effort to plug the hole before it becomes widely known.

So far there have been no reports of the vulnerability being exploited.

**Serious problem**

"Exploitation of this vulnerability could have affected the glue that holds the internet together," said Roger Cumming, head of the UK's National Infrastructure Security Coordination Centre.

The NISCC issued an alert about the vulnerability on Tuesday and was swiftly followed by the US Department of Homeland Security.

In its alert the DHS said the vulnerability: "could lead to a denial-of-service condition that could affect a large segment of the internet community."

**SEE ALSO:**

- What the net did next
  01 Jan 04 | Technology
- Net struggles with data overload
  16 Sep 03 | Technology
- Promise of ultra-fast downloads
  05 Jun 03 | Technology
- Doing science by stealth
  29 Aug 01 | Sci/Tech
- FBI probes attack on net
  23 Oct 02 | Technology
- Major net security holes identified
  31 Jan 01 | Sci/Tech

**RELATED INTERNET LINKS:**

- National Infrastructure Security Co-ordination Centre
- NISCC Alert
- US Department of Homeland Security
- DHS Alert
- CanSecWest
- Internet Systems Consortium

The BBC is not responsible for the content of external internet sites

**TOP TECHNOLOGY STORIES NOW**

- Iraqis seek self-rule on the net
- Microsoft sets sights on spam
- Internet browser breach defused
- Boy inspires cancer video game

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

# UK ‘Self Defence’ Forum

- Already existing Groups but not the right focus
- A widely recognised need for a Forum for Network Operators
- A nucleus of Operators of all shapes and sizes
- A number of issues raised, such as
  - Alerting
  - Reporting
  - Shared technical solutions

# Issues to be addressed

- Infrastructure: Single points of failure and resilience in Service Providers' networks.
- International Cooperation: between ISPs, telcos, police authorities
- Political as well as Technical solutions
- The Deterrent value of publicising arrests and convictions
- A User Awareness Campaign: users spawn virus attacks
- Blacklisting
- Trace-back issues
- A duty of care – by users and by providers
- Legislation and the burden of it
- A **UKNOF**

NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

# Can we help?

- Infrastructure: Protective advice for physical and logical defence
- Cooperation: Building links in Europe, US, Canada
- Political solutions: Access to various Government agencies
- Deterrence: Good linkages with NHTCU & other police agencies
- User Awareness: ITSafe, UNIRAS, WARPS, Publications
- Blacklisting: Keeping the dialogue going
- Trace-back issues: technical support or liaison
- A duty of care: Peer and Customer pressure?
- Legislation/Regulatory: Helping to influence policy
- A **UKNOF**

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

# Thank you

# For more go to…

www.niscc.gov.uk

Or e-mail me at

Robertd@niscc.gov.uk