



Security  
Innovation &  
Technology  
Consortium

Knowledge and  
capability for  
global security  
and resilience

# Security Innovation and Technology Consortium

Cyber Terrorism and Espionage  
A Public – Private Partnership

Steve Swain MBA CMgr FCMI  
Chief Executive Officer

# Cyber Terrorism

## Definition of Cyber Terrorism:

It is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples.

Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

# Cyber Terrorism

Threat

Capability

# Espionage

Espionage is unauthorised and usually criminal access to confidential systems and information for the purposes of gaining a commercial or political advantage.

The threat from espionage (spying) did not end with the collapse of Soviet communism in the early 1990s.

Espionage against UK interests continues from many quarters.

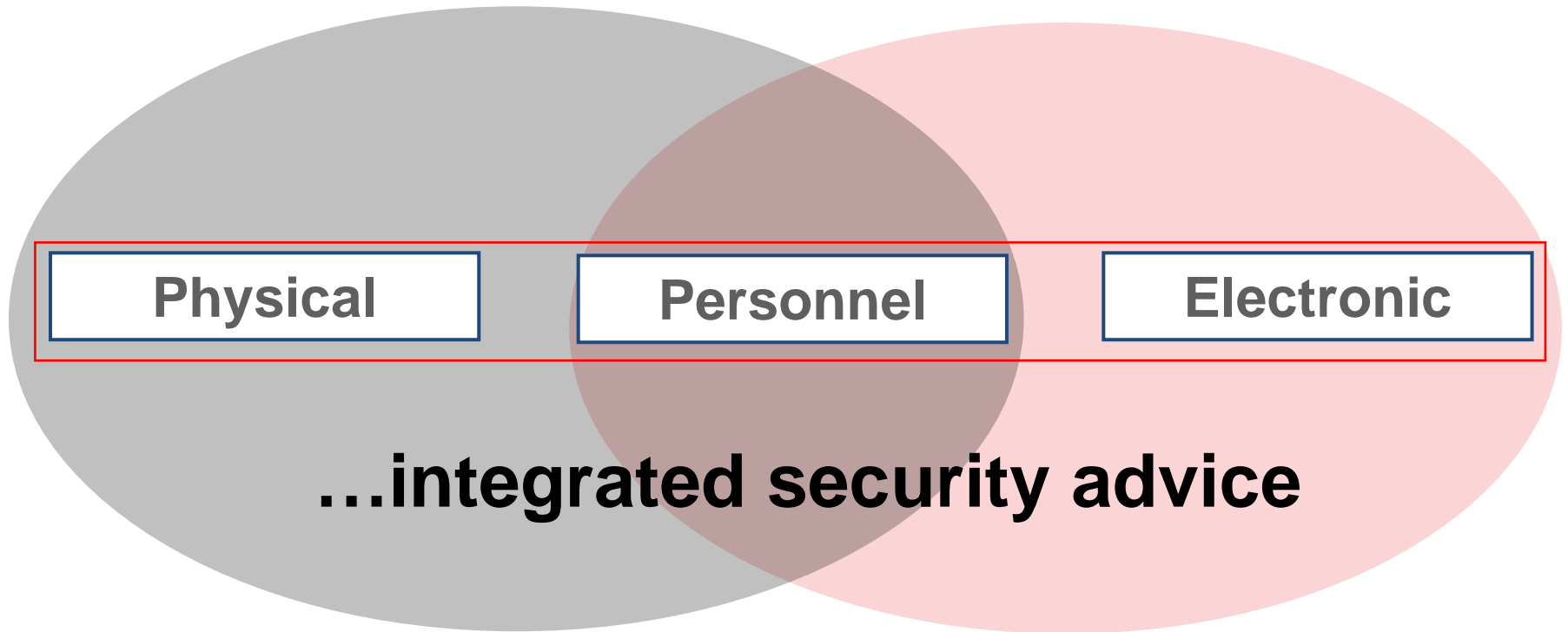
In the past, espionage activity was typically directed towards obtaining political and military intelligence. This remains the case, but in today's high-tech world, the intelligence requirements of a number of countries also include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields.

The UK is a high priority espionage target and a number of countries are actively seeking UK information and material to advance their own military, technological, political and economic interests.

# Different threats...

**Terrorism**

**Espionage**



Threat, Opportunity, Capability, Motivation

# The Second Oldest Profession

Traditional incarnations of espionage have not gone away

The methods used have adapted to the 21st Century...



Security  
Innovation &  
Technology  
Consortium

Knowledge and  
capability for  
global security  
and resilience

# The Rise of Cyber Attack



- Targeted Trojan emails
  - Office (Word, Excel, Powerpoint)
  - PDF
  - Links to compromised websites
- Social Engineering
  - Spoofer senders
  - Use of original documents
- Compromised Websites
  - Service Denial
  - Obfuscated Javascript
  - Zero pixel iframes

2003 – First new incidents

2005 – First public warning

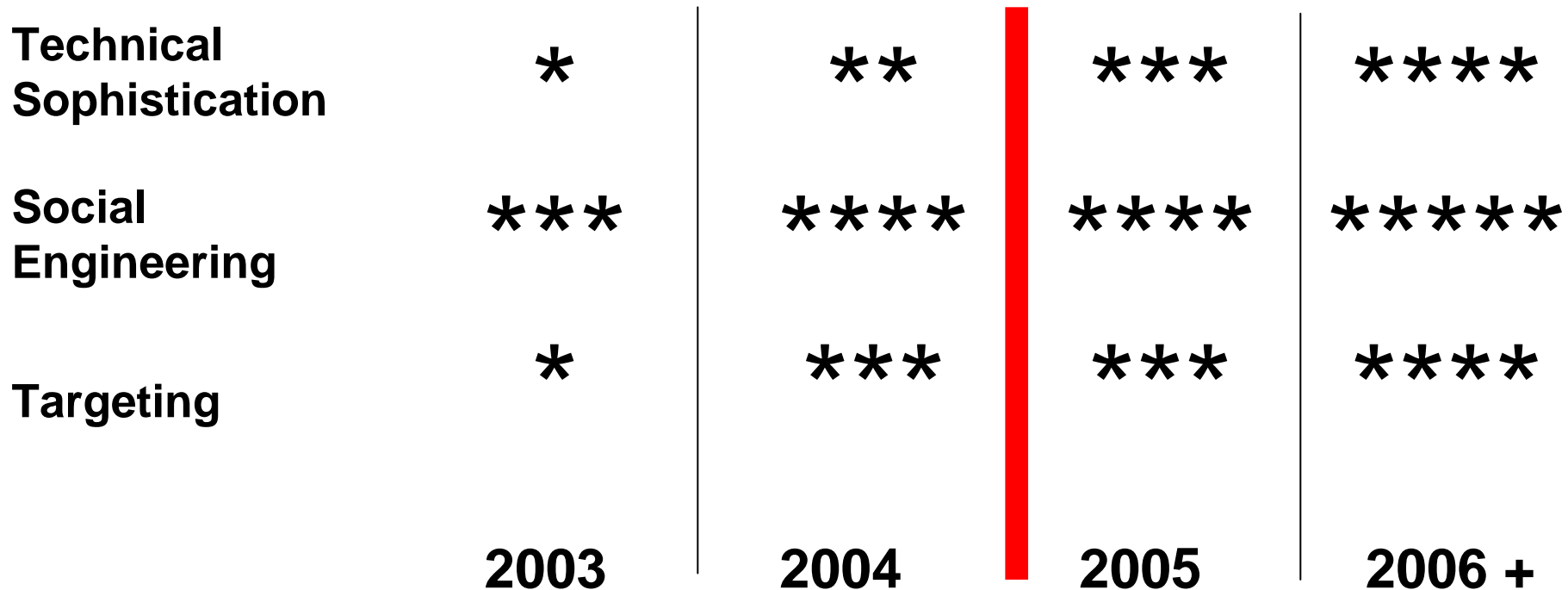


Security  
Innovation &  
Technology  
Consortium

Knowledge and  
capability for  
global security  
and resilience

# Threat Actor Cyber Capabilities

**CAPABILITY EXCEEDED INDUSTRY BASELINES**



Most networks still susceptible to basic attacks



Security  
Innovation &  
Technology  
Consortium

Knowledge and  
capability for  
global security  
and resilience

# Targeting of UK Industry



There have been successful compromises across all sectors

Compromises have resulted in the loss of large amounts of data

The range of targets is increasing and now goes beyond national infrastructure

Company data can be randomly located on the Internet. Huge potential for bad publicity

# Disruption Challenges

Sensitising industry to the threat

Improving coverage of the threat and understanding of harm

Guiding response activities

Resourcing increasing numbers of cases

Identifying solutions

# Protecting the National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the recognised UK government authority for protective security advice to the national infrastructure.

It protects national security through:

Minimising risk to the national infrastructure; *by*

Delivering authoritative advice; *to*

Reduce the vulnerability of the national infrastructure to terrorist and other threats.



# The CPNI can

Provide threat advice

Explain traditional and technical modus operandi

Attribute incidents

Provide professionally researched tools

Leverage the benefits of secret intelligence

## ... but cannot

Manage and investigate every incident reported

Investigate commercial espionage and other related forms of criminality

Respond to every briefing request

Perform risk and impact assessments

Provide end-to-end solutions

# CPNI Engagement with Consultancies

There are opportunities for consultancies to support their clients in reducing their vulnerabilities and responding to incidents

Consultancies can act as valuable conduits for information

In return, CPNI will provide authoritative advice to support commercial services

# Current CPNI Advice and Tools

Guide to espionage risk assessment

Business focused espionage threat advice

Technique focused threat advice

Security culture tool

Personnel security advice

# Planned CPNI Advice and Services

Counter-espionage advice for overseas travellers

Investigation guides

Guide to counter-cultivation

Guide to managing espionage incidents

Network Intrusion Detection Analysis Service

Joint products with SOCA

# A Public – Private Partnership

## Fundamental Issues

Innovative technology is a vital component of an effective Cyber Security regime

The Private Sector & Government Agencies need innovative technology to help them prevent cyber attacks

Innovation comes from the agile SME community

SME's have limited resources and often find it hard to access major customers

Customers often lack the time to go and find the innovative solutions they need

SME's are often invisible to the major customers they need to contact



# A Public – Private Partnership

Access to the threat information

Security Clearances

Trust

# The Security Innovation and Technology Consortium (SITC)

1. Focused on the Security and Resilience Sector
2. Not for profit, funded from the Public Purse, performing the role of an 'Honest Broker'
3. A 'free to join' consortium developing collaborations to drive innovation
4. Find/develop high tech innovative security solutions for the end user community
5. Become a 'One Stop Shop' for security innovation
6. Currently 260 members, working on a number of projects



# SITC Objectives

1. Help businesses get access to actionable market intelligence
2. Facilitate collaborations between businesses and people across the global supply chain – to win business together
3. Get businesses and collaborations in front of major customers
4. Join up the region's business support services so they give businesses the back-up they need throughout this journey

# Special Interest Groups

## SECURITY and RESILIENCE

1. **Transport and physical security** - fences, barriers, access control, IDS, protection, container security, metal detectors, mm wave sensing
2. **Surveillance, tracking and biometrics** - sensing, counter surveillance, analytics, video management, CCTV, UAVs, RFID
3. **Sensors and detectors** - Sensing, planning, management
4. **Information Systems** - data mining, network systems, fusion, info analysis, digital forensics and watermarking, DRM
5. **Information Assurance** - firewalls, cryptos, secure comms, pen testing etc
6. **Governance, Risk and Compliance** - business continuity, training, exercise, planning, policy

# Questions?

SITC Contact Details

[www.securityintech.com](http://www.securityintech.com)

+44 (0) 1793 785164

[sswain@securityintech.com](mailto:sswain@securityintech.com)

+44 (0)7966 134503