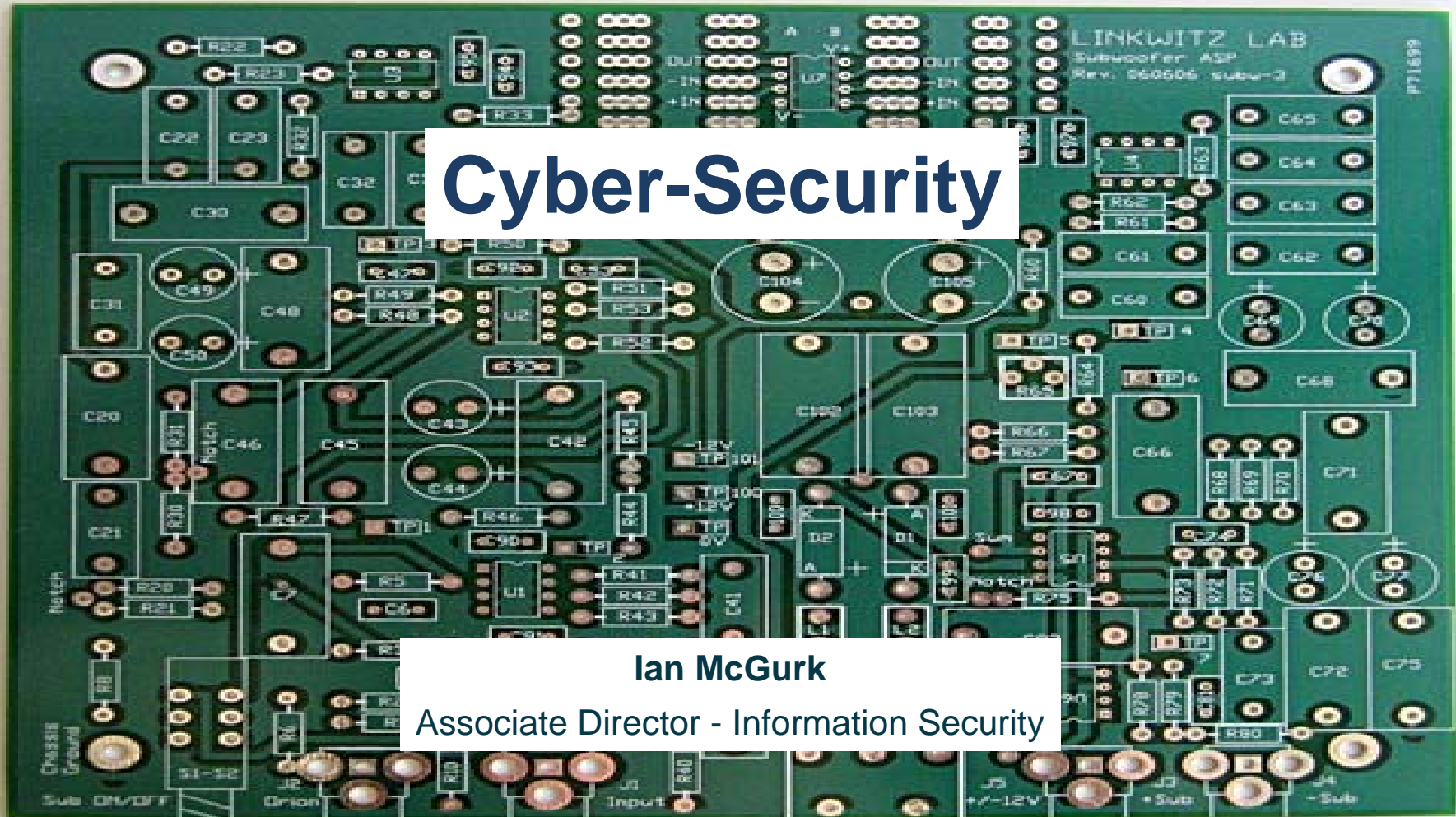


Cyber-Security

Ian McGurk

Associate Director - Information Security



RUSI: Cyber Security (commercial espionage)

Agenda

- Context – Cyber-espionage
- Example investigation
- Threat Actors
- Target Profile
- International – business operation
- Reducing the risks

RUSI: Cyber Security (commercial espionage)

Protect against efforts to:

- Disrupt or damage infrastructure (Cyber-Terrorism)
- Disrupt or damage computer systems (Malware / Hacking)
- Take control of systems (Root-Kits)
- **Steal sensitive information**
 - Phishing
 - Hacking
 - **Trojans (Cyber-espionage)**

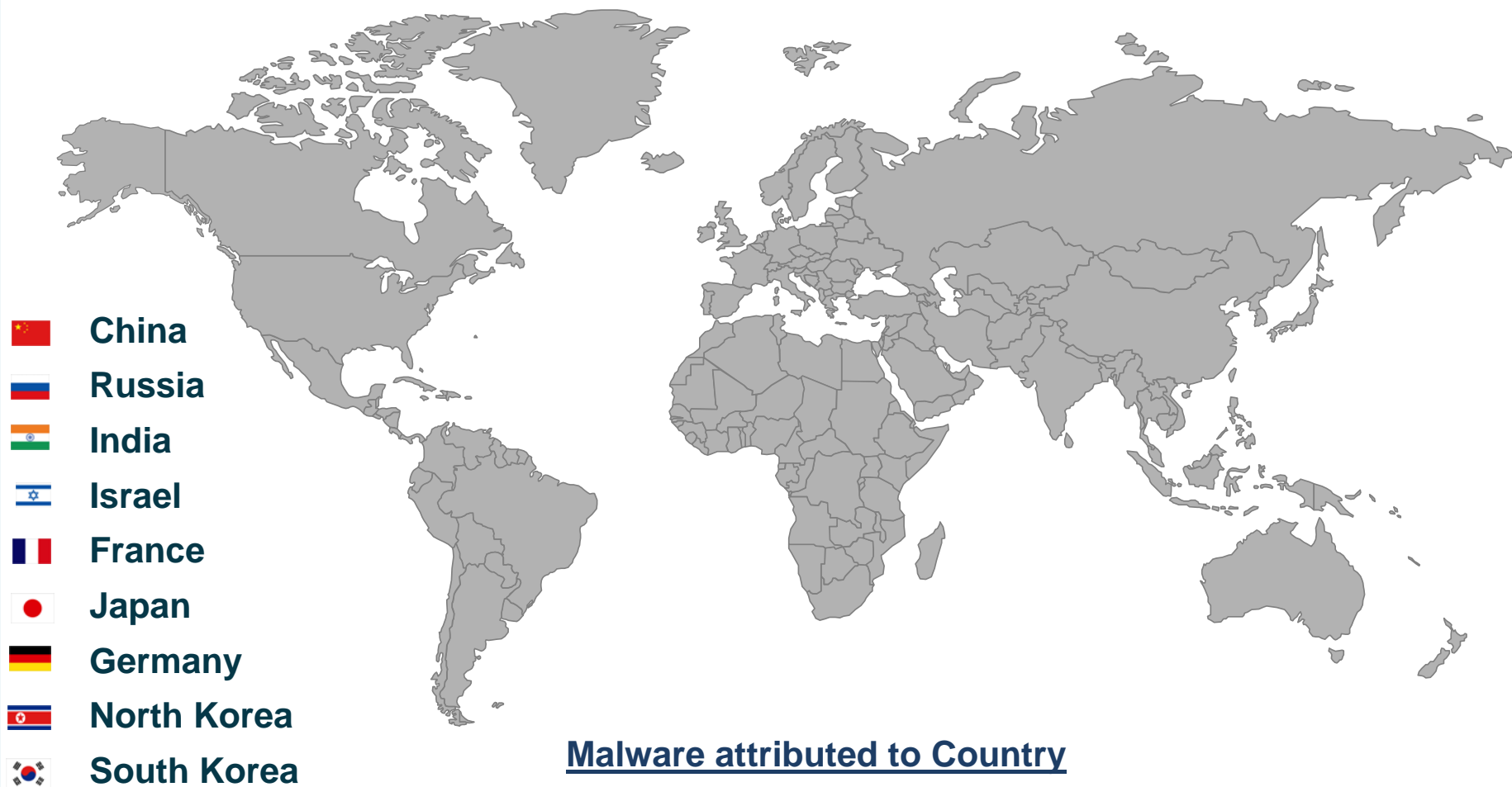
Trends

- From generic attacks to targeted attacks
- Increased sophistication
- ‘State-sponsored’ cyber espionage – methods / techniques / tools same as intelligence gathering for government / defence activities



RUSI: Cyber Security (commercial espionage)

Threat actors



RUSI: Cyber Security (commercial espionage)

Investigations

Control Risks have investigated a number of compromised environments and have detected the presence of crafted malware

Example

- Global company
- Advised of problems

Business analysis (where to look)

Network analysis phase (network traffic and logs)

Host analysis phase (system images)

- Detection of infection
- Method of introduction
- Infection process
- Cleanup process
- Attribution

Issue: Snapshot in time, could be re-infected at any time

Requires Long-term protection strategy

- **changes in infrastructure, operational practices and culture**



RUSI: Cyber Security (commercial espionage)

Target Profile

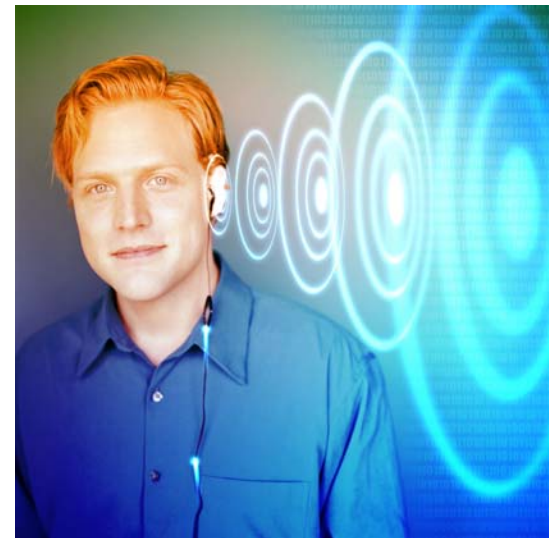
Likelihood of being targeted dependent upon sector, activities and competitors

sectors include;

- Extractives (Mineral / O&G)
- Pharmaceutical
- ICT
- Telecoms
- Legal
- Utilities
- Financial
- Defence

Activities are;

- High value competitive bids
- Research and development
- New product launch
- M&A etc.



RUSI: Cyber Security (commercial espionage)

Business Operation in Country

Our Experience

- Commercial organisations extend their business operation to these locations or enter into a joint venture with a locally established organisation in country;
 - They have not considered the threats and risks
 - They have not considered the potential impact of losing their IPR or sensitive business info.
 - They have not considered how to protect the rest of their organisation

Standard Approach:

- Site to site VPN (open tunnel)

Example:

JV – Chemical – Viability (how much before IPR is lost)



Some countries have laws and practices designed to weaken your defences

RUSI: Cyber Security (commercial espionage)

How to reduce risks

- **Lock down systems with reduced privileges**
- **Do not make a high risk location a direct extension of your corporate network** (utilise standalone email / FTP facilities)
- **Segregation** – determine practical ways of segregating your business critical information from your corporate network
- **Travelling to high risk areas**
 - If possible - do not take devices / sensitive information
 - If must, then take vanilla build PC, as soon as you return re-image the system (do not connect to the network)
 - Access data remotely
 - Utilise One Time Passwords (avoid key-loggers)
 - Access data through protected environment (Citrix or OWA (document viewers))



RUSI: Cyber Security (commercial espionage)

Summary and Conclusions

- Threat is very real / challenge - acceptance
- 'Zero Day' malware - undetectable
- Clean / re-infect
- Information segregated
- Office in-country likelihood increases
- Travelling

