Why Olympics?

- Global platform
- Long lead times
- Complex threat landscape
- Complex cyber security arrangement
- Multi-stakeholder approach
- Increasing reliance on ICT
Overview of cyber attacks

A spoofed copy of the Vancouver Organising Committee’s website, hosted in Ukraine, distributed a video containing codec malware.

July 27 2012 saw a massive 40-minute DDoS attack on the Olympic Park’s power systems starting at around 5:00 p.m. and was likely intended to disrupt the opening ceremony.

Unauthorized ticket selling on fake websites and data leaks from government and Olympics-related organizations (e.g. the World Anti-Doping Agency)
Overview of actors and motivations
Overview of lessons identified

- Include in broader security planning
- Use targeted cyber defence campaigns
- Plan early
- Define all stakeholder roles & responsibilities
- Allocate resources
- Common security goals
- Cooperate and share information
- Know the mission