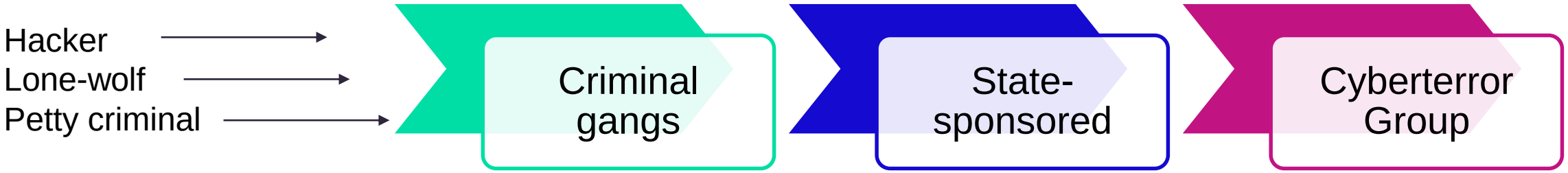
GlobalData.

Conference Debate Session 1
Global Threat Landscape: How Cyber Terrorism Defines Information Security

Introduced and Chaired by Joel Stradling

What is Cyberterrorism?

- Terrorist groups have broader agendas than physically harming civilians
- Objectives have evolved to cyber warfare levels with the objectives of causing disruption politically & economically
- A new supply chain is emerging:

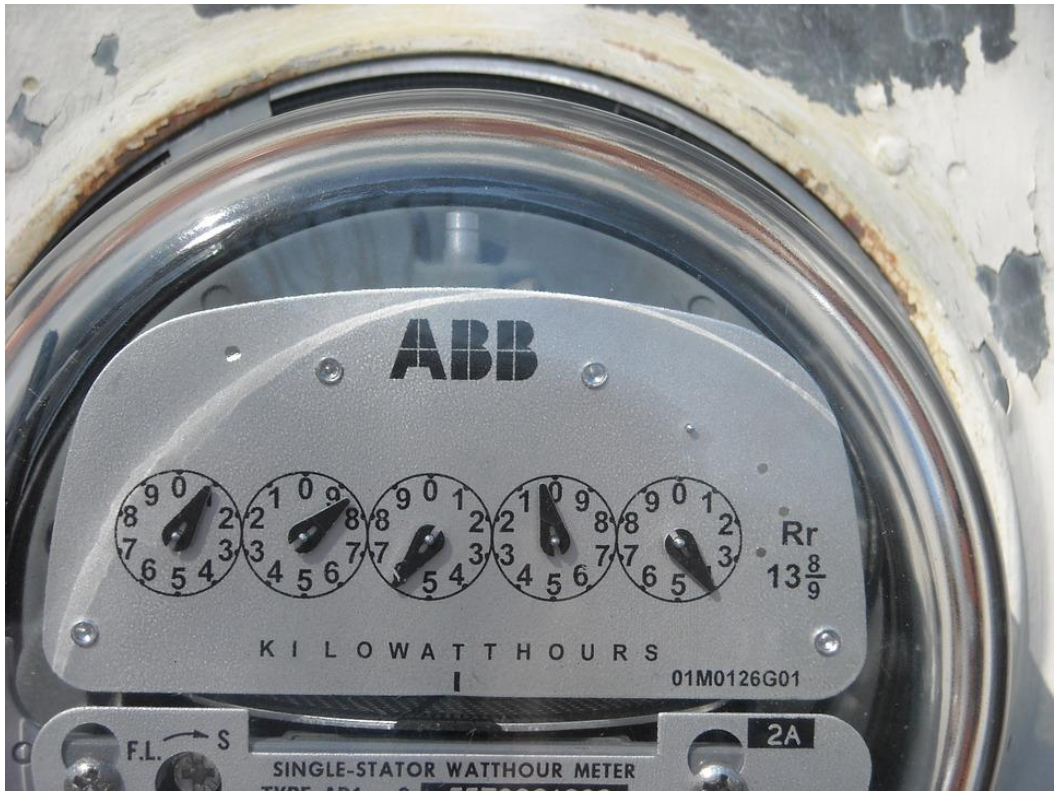


Who is Vulnerable?

- Businesses and governments are increasingly dependent on automated IT systems
- Critical infrastructure management is increasingly on-line
- Physical device security is not very well integrated with IT and network

Who is Vulnerable? (cont.)

- Electrical – smart meters and lights out
- Supply chain and transportation – disruption and ransomware



e.g., Healthcare

- Healthcare cybersecurity is not limited to protecting patient data
- Weak medical device security compromises data privacy, patient safety, hospital operations
- Breaching IoMT devices a relatively simple task for hackers

Cyberterrorism: What is the Danger?

- Ambitions and attention on national infrastructure attacks are on the rise
- Sophisticated tools are widely available on the black market – these can be shared between criminal gangs and state-sponsored terrorist groups

May 3, 2019: German police shut down one of the world's largest illegal online markets in the so-called ‘darkweb’. Operation involved Europol, Dutch police and the FBI and also led to the arrests of two major suppliers of illegal narcotics in the US. The illicit "Wall Street Market" site enabled trade in cocaine, heroin, cannabis and amphetamines as well as stolen data, fake documents and malicious software.

Contacts

Joel Stradling

Research Director

Global Enterprise Network & IT Services

Joel.stradling@globaldata.com

+34 672 766 060

info@globaldata.com

www.linkedin.com/company/globaldata

+ 44 (0) 20 7936 6830

twitter.com/globaldata