

JRC Annual Strategic conference A DNO's perspective on Cyber security — preparing for ED2

Phil Green Information Security and Compliance Manager

Threat to UK ICS

It is **highly unlikely** a hostile nation state actor would seek to conduct a highly destructive cyber attack

Ransomware with specific ICS functionality indicates cyber criminals have highly likely evolved to pose a more direct threat to ICS



Industrial
espionage, learning
and development, and
pre-positioning are
highly likely the
primary threats to UK
ICS asset owners

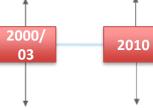
Low-sophistication actors have shown a growing interest in targeting ICS. it is likely their interest and capability against internet-accessible ICS assets will grow

The combination of intent and capability that **almost certainly** make hostile nation state actors a persistent and potentially dangerous threat.



Attack timeline





DAVID-BESSE SHAMOON NUCLEAR DEMONSTRATED SLAMMER WORM LARGE DEPENDENCY CAUSED 5 HOURS ON GLOBABLE LOSS OF SAFETY MARKETS AND SYSTEM VISIBILITY COMMODITY 2003 HARDWARE 2010

STUXNET 1ST ATTACK CAUSING CYBERPHYSICAL DAMAGE AGAINST A NATION STATE 2010



GERMAN STEEL MILL

DISRUPTED CAUSING

PHYSICAL DAMAGE

PROCESS AND

CONTROL WAS

2014

UKRAINE POWERGRID 1ST MAJOR CYBER ATTACK AGAINST A POWERGRID 2015





WATER TREATMENT LARGE-SCALE WATER TREATMENT OT PROCESS ALTERED AND AFFECTED RESIDENTS 2016

NOTPETYA* OVER \$10 BILLION DOLLARS FOR MERCK, MAERSK, MODELEZ AND A UK FIRM 2017

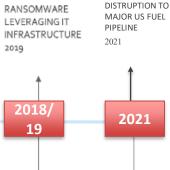


MIRAI BOTNET 1ST MAJOR DDOS ATTACKS USING IOT/IP DEVICES 2017

LABCORE 1ST MAJOR COMMODITY MALWARE AND INCLUDED MODBUS FILTERS 2018







VPN FILTER 1^{5T} MAJOR COMMODITY MALWARE AND INCLUDED MODBUS FILTERS 2018

NORSK HYDRO

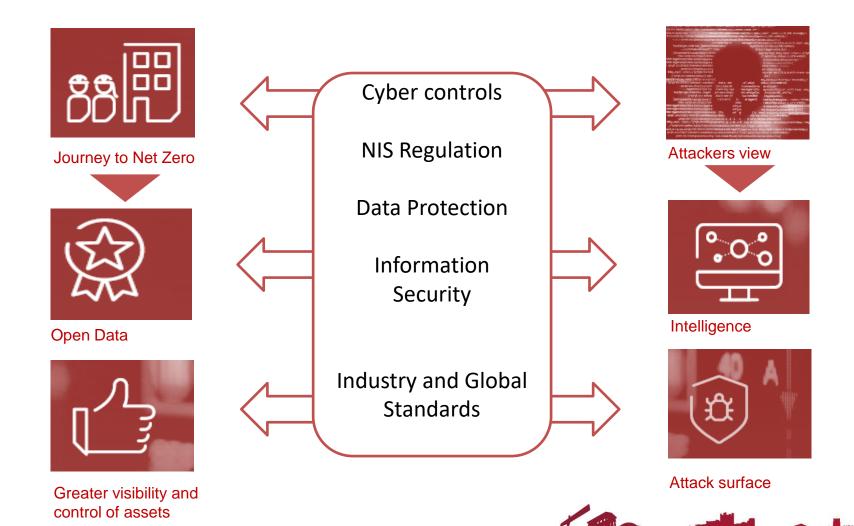
TARGETED



COLONIAL RANSOMWARE



Digitalisation and open data



Security of data in transit

- Exposure
- Routing
- Availability





Secure communications

- Commercial
- Private Radio
- Private Fibre optics
- Rented Fibre optics



Certainty
Spectrum
End of life
Cost

