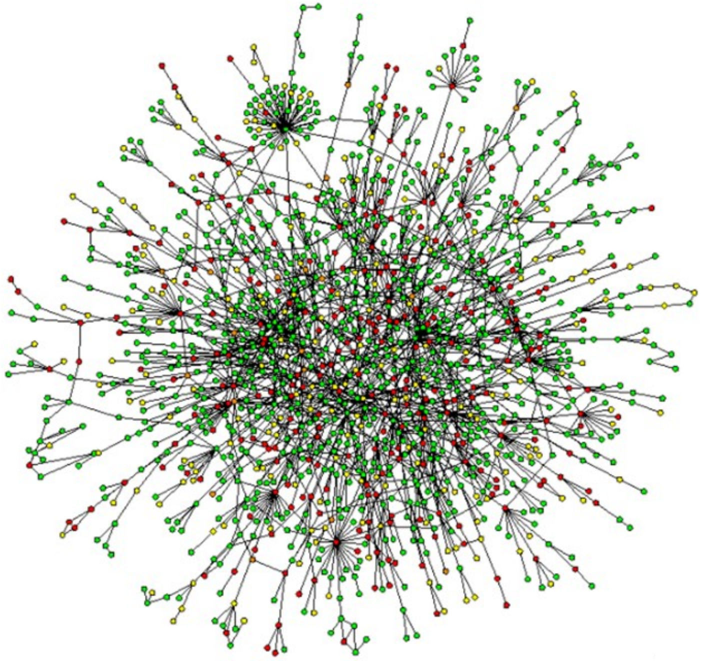
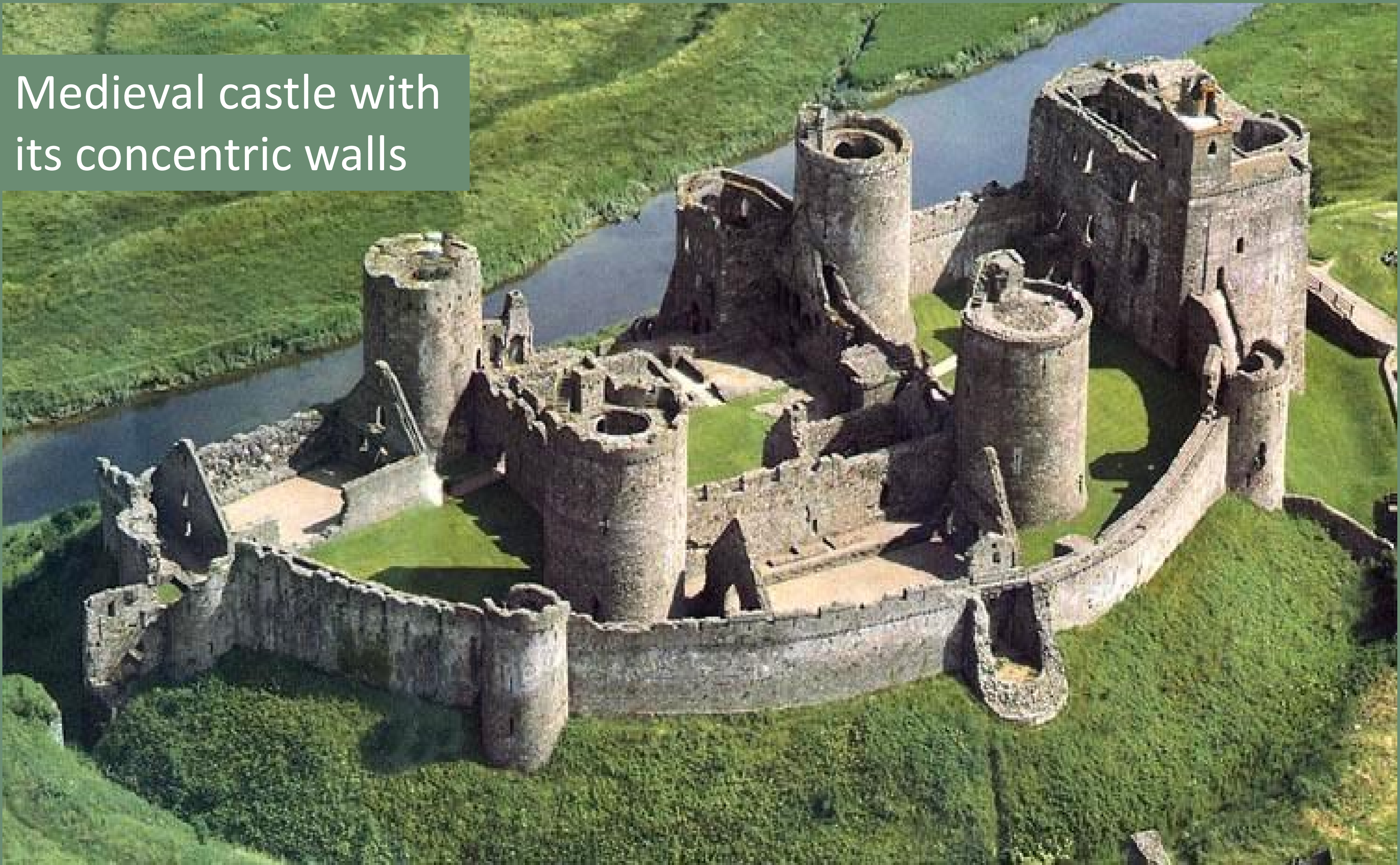
# Differences between defence-in-depth for computer security and physical protection



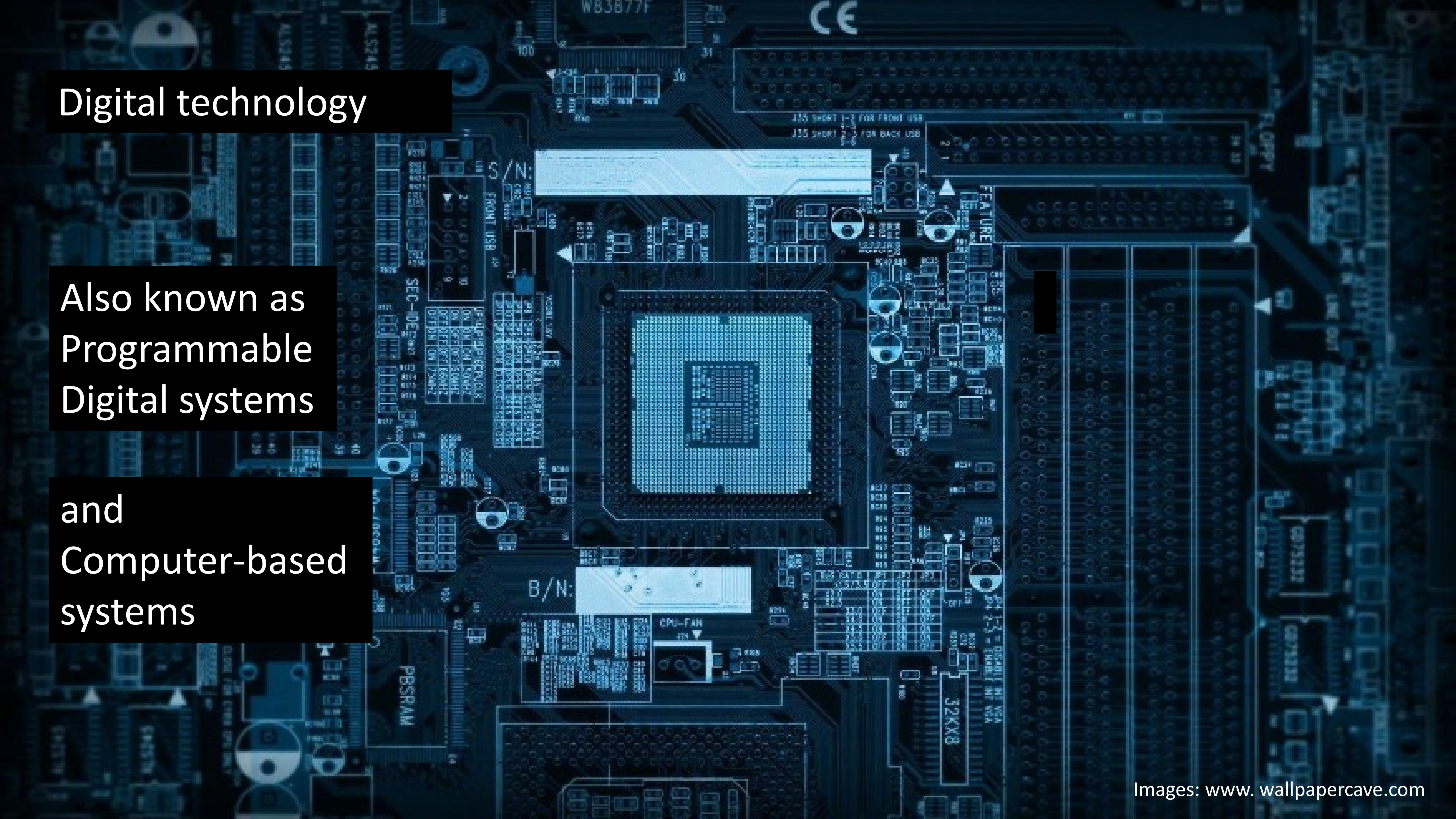
Mike StJohn-Green

Independent consultant, UK

Michael@stjohn-green.co.uk



Medieval castle with its concentric walls

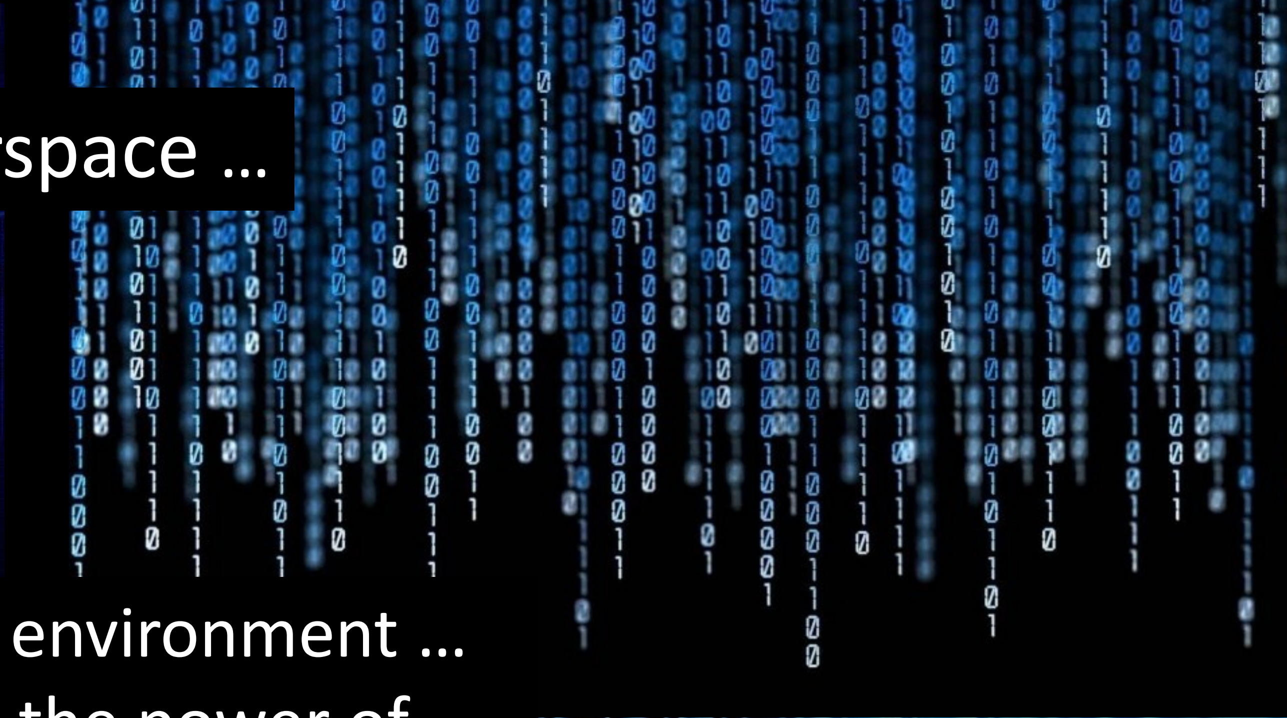


# Digital technology

Also known as Programmable Digital systems

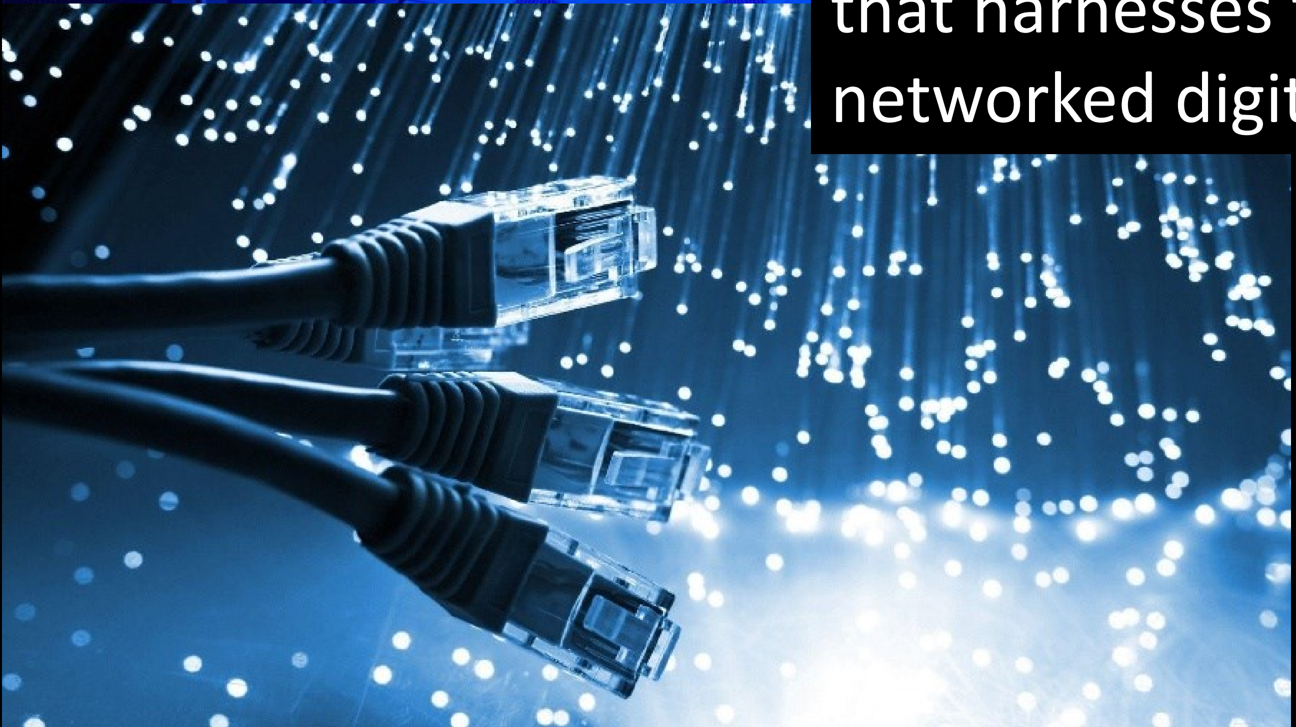
and
Computer-based systems

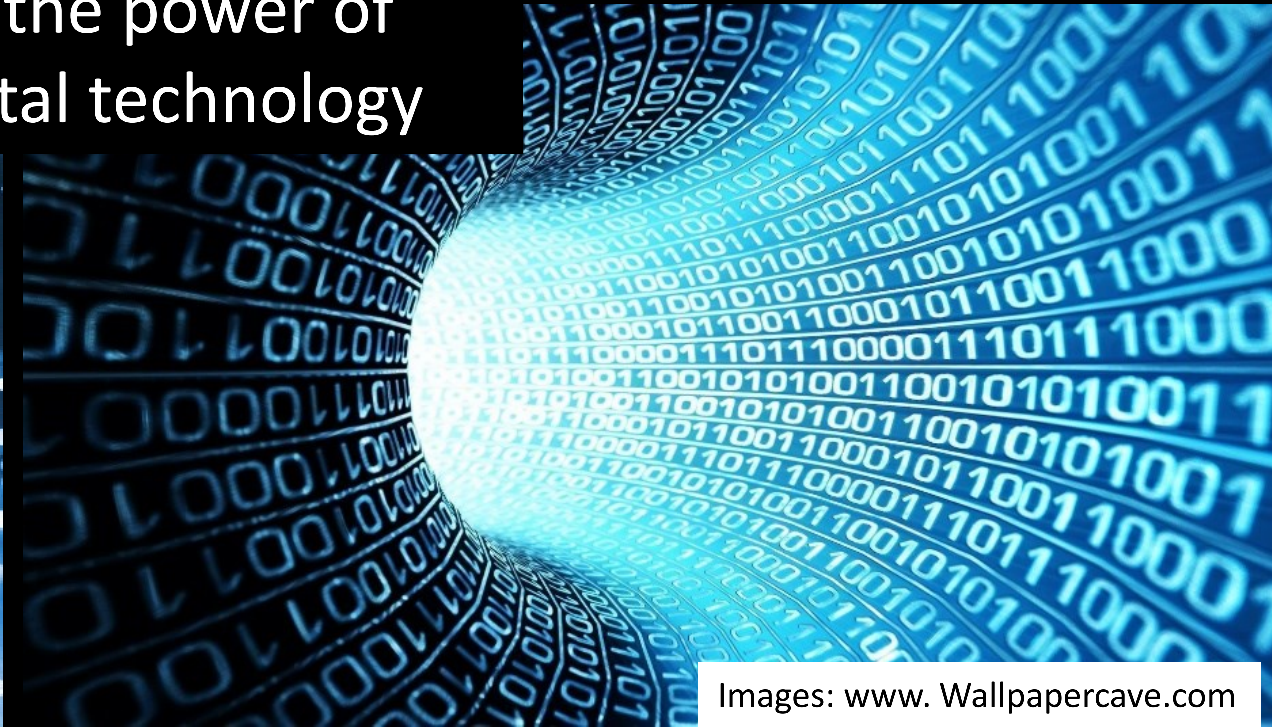
Images: www. wallpapercave.com



# Cyberspace …

Is the notional environment … that harnesses the power of networked digital technology





Images: www. Wallpapercave.com

# Differences between Cyberspace and physical space

1. Lack of determinism, instinct and intuition

https://giphy.com/gifs/super-mario-maker-W9xUtJVpgSyHu

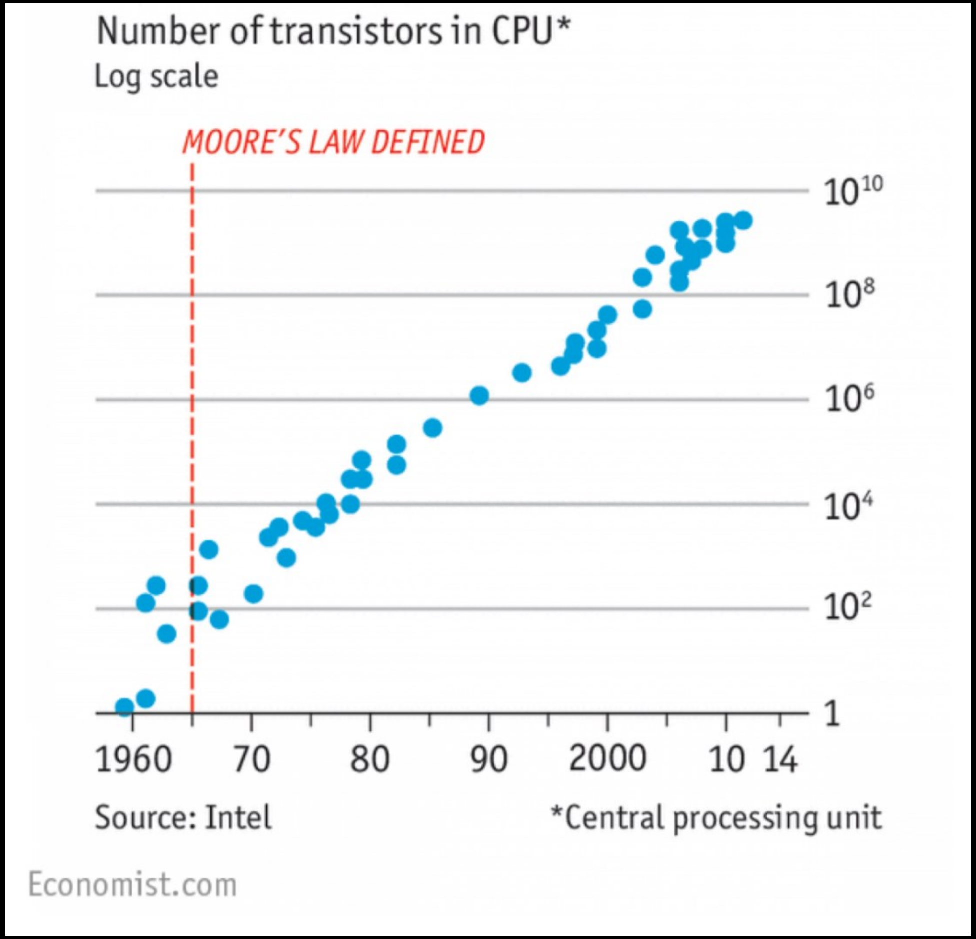
# Differences between Cyberspace and physical space

1. Lack of determinism, instinct and intuition

2. Pace of change

## Moore’s Law

100x increase in transistors every ten years



https://www.economist.com/blogs/economist-explains/2015/04/economist-explains-17

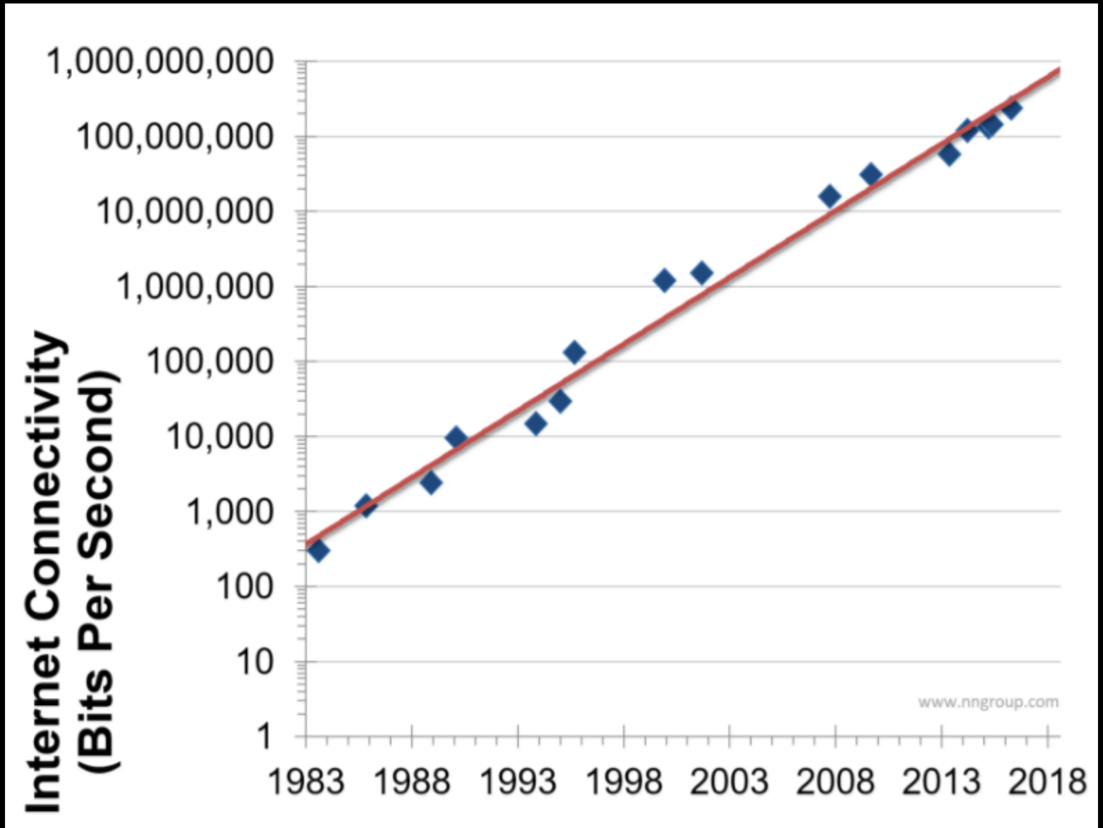
## Differences between Cyberspace and physical space

1. Lack of determinism, instinct and intuition

2. Pace of change

## Neilsen’s Law

50x increase every ten years in Internet connectivity



https://www.nngroup.com/articles/law-of-bandwidth/

# Differences between Cyberspace and physical space

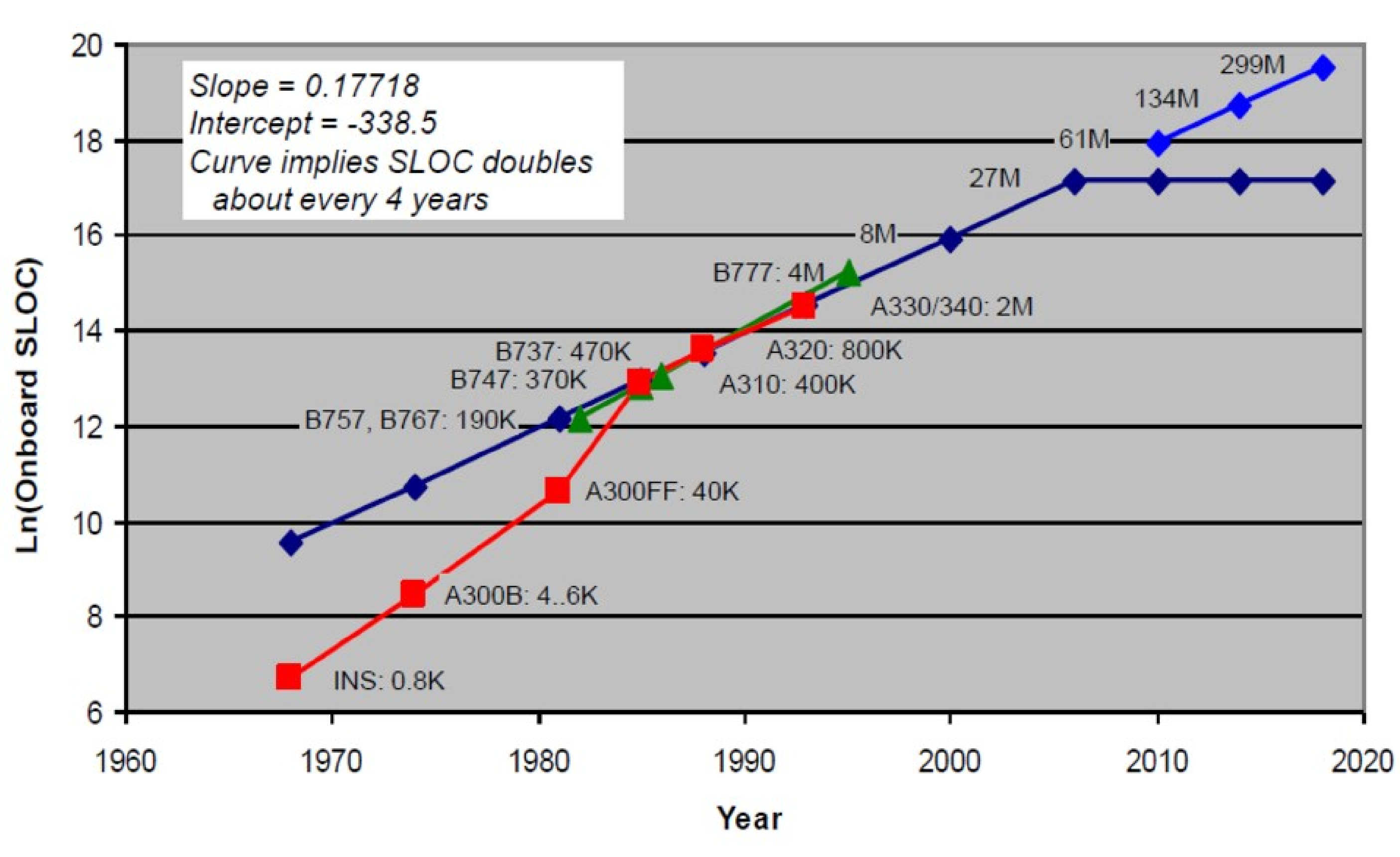
1. Lack of determinism, instinct and intuition

2. Pace of change

3. Unknown vulnerabilities

# PLENTY OF SCOPE FOR FAULTS: SOFTWARE COMPLEXITY

Software size doubles every 4 years



http://www.engineeringnewworld.com

# Differences between Cyberspace and physical space

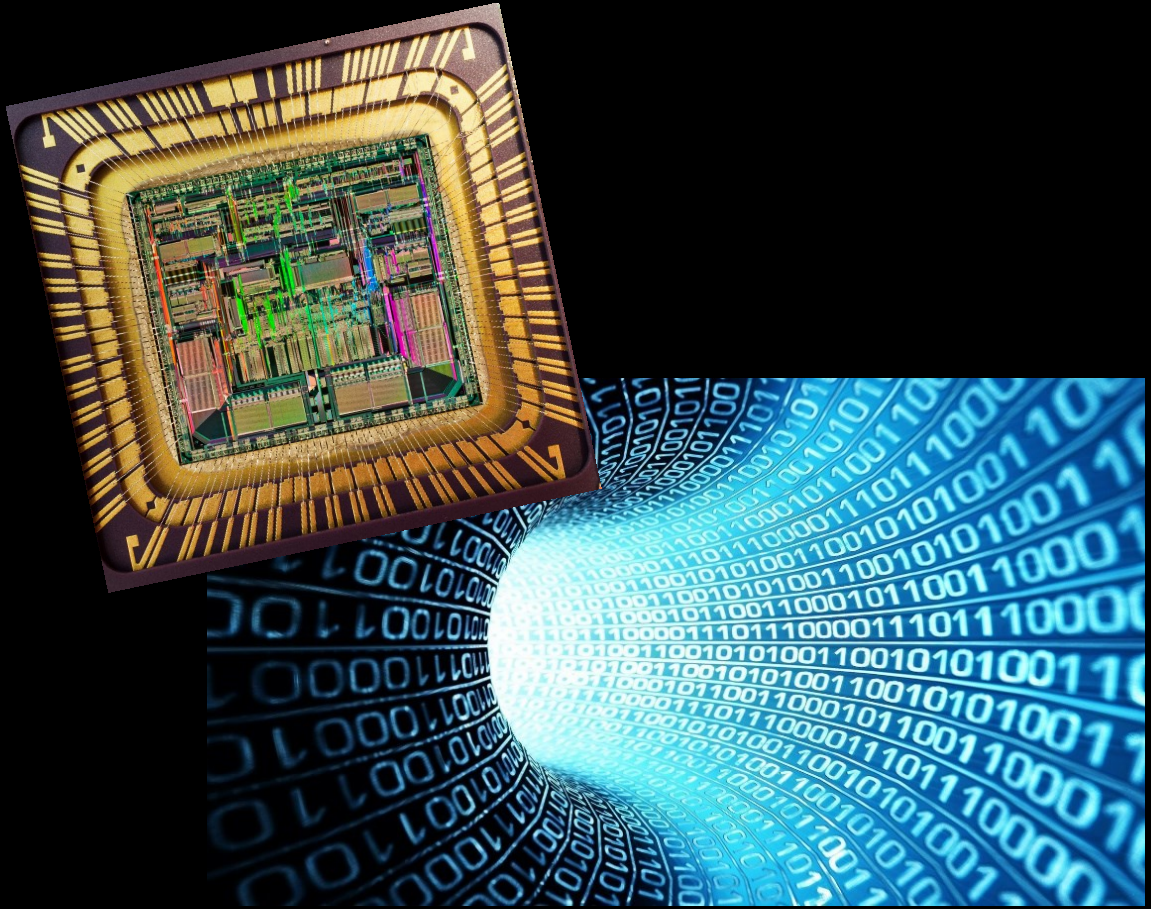
1. Lack of determinism, instinct and intuition

2. High pace of change

3. Unknown vulnerabilities

4. Indistinct boundaries

## ALL DIGITAL TECHNOLOGY IS PART OF THE GLOBAL INTERNET



www.wallpapercave.com, Wikimedia.org – 68040 microprocessor

# Differences between Cyberspace and physical space

1. Lack of determinism, instinct and intuition

2. High pace of change

3. Unknown vulnerabilities

4. Indistinct boundaries

5. Unreliable detection methods

## THE EVIDENCE IS IN PLAIN VIEW:

European companies take an average of 469 days to discover attackers in their system.

Global average is 146 days

– based on analysis by Mandiant in 2016

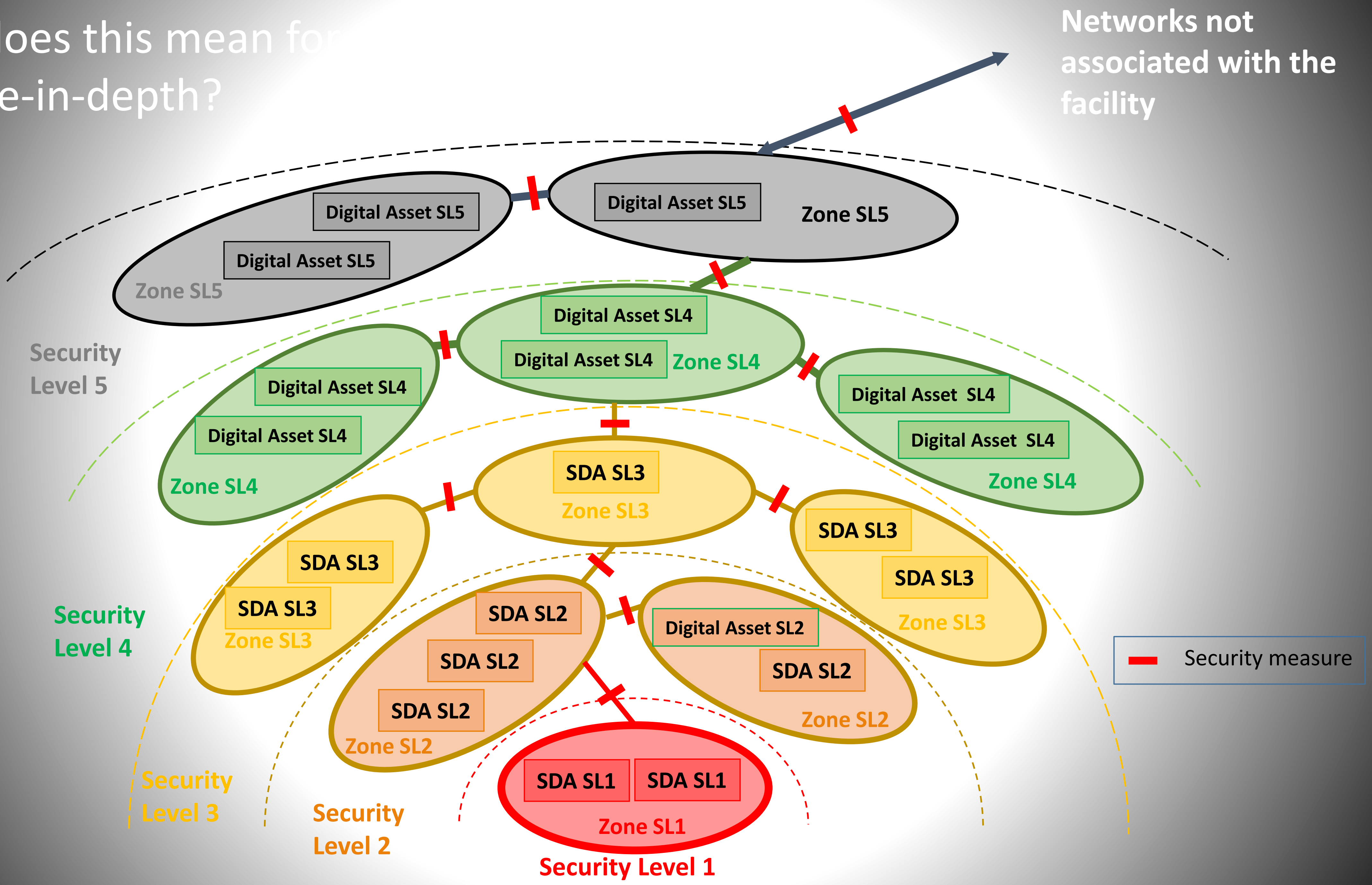
The average dwell-time of attackers is 229 days – FireEye in 2014

www.wallpapercave.com,

# Differences between PPS
# And computer security

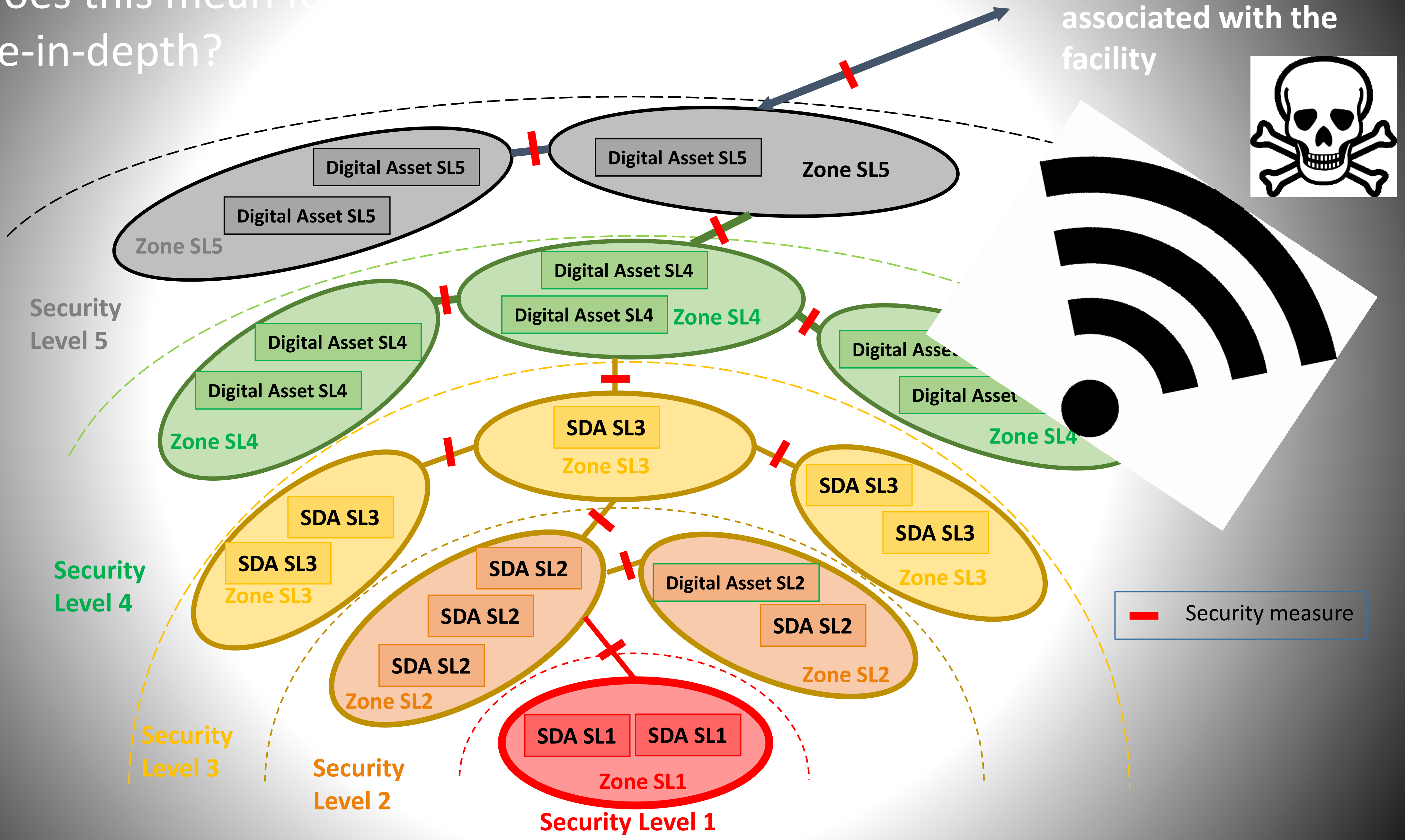
| | |
|---|---|
| 1. Deterrence | ATTRIBUTION IS VERY DIFFICULT |
| 2. Detection | WE HEARD – DECTECTION IS UNRELIABLE |
| 3. Delay | THEREFORE CANNOT RELY ON DELAY |
| 4. Response | RESPONSE IS STILL VITALLY IMPORTANT;<br>FALSE ALARMS MAY BE HIGHER |
| 5. Design Basis Threat | PACE OF CHANGE MAKES THIS CHALLENGING;<br>MUST DEAL WITH BLENDED ATTACKS |

# What does this mean for Defence-in-depth?

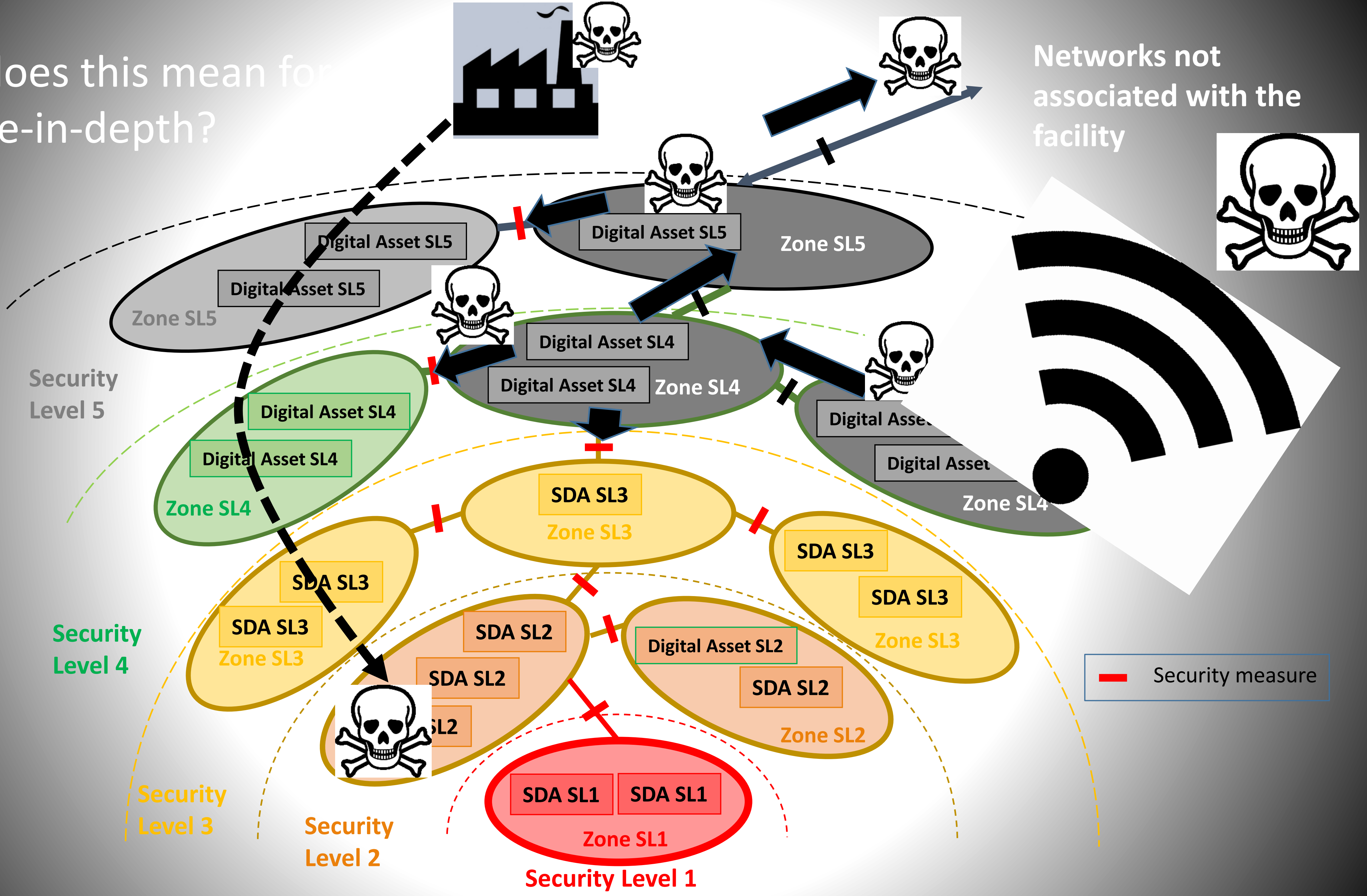


# What does this mean for Defence-in-depth?

Networks not associated with the facility



# What does this mean for Defence-in-depth?



Networks not associated with the facility

# Some conclusions

- Digital technologies bring unparalleled benefits
- Computer security defences are imperfect at best
- Deterrence is difficult, delay is problematic to quantify
- Defence-in-depth is important but different – diversity is significant
- Resilience to cyber-attack may require changing the architecture
- Cyber design basis threat is a difficult concept
- Blended attack scenarios are vital, vital, vital!
- This raises some difficult questions for organisations

# Differences between defence-in-depth for computer security and physical protection

Mike StJohn-Green

Independent consultant, UK

Michael@stjohn-green.co.uk