Cambridge Judge Business School

Cambridge Centre for Risk Studies 2018 Risk Summit

CYBER RISK LANDSCAPE

Dr Jennifer Daffron, Research Associate
Centre for Risk Studies

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

The Cyber Risk Landscape

Internationalisation of Cyber Crimes

Cryptocurrency Gold Rush

Multiplicity of Ransomware

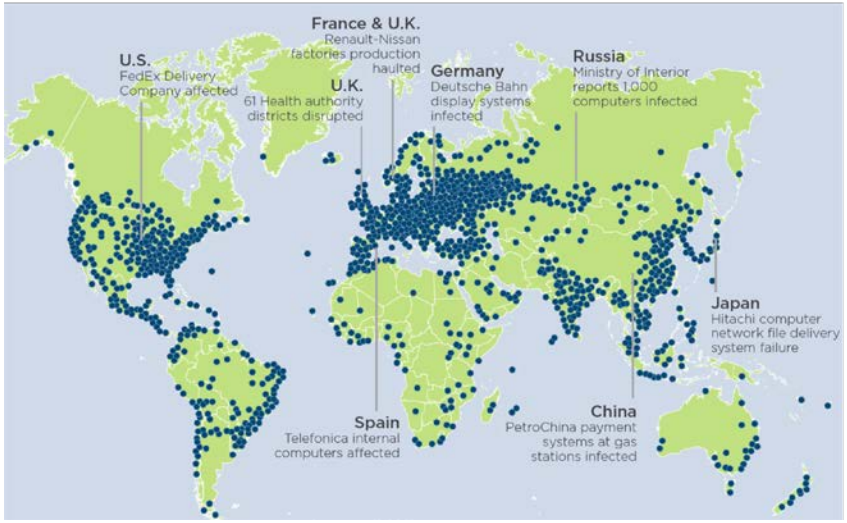
Cyber Crime as a Service

Supply Chain Attacks

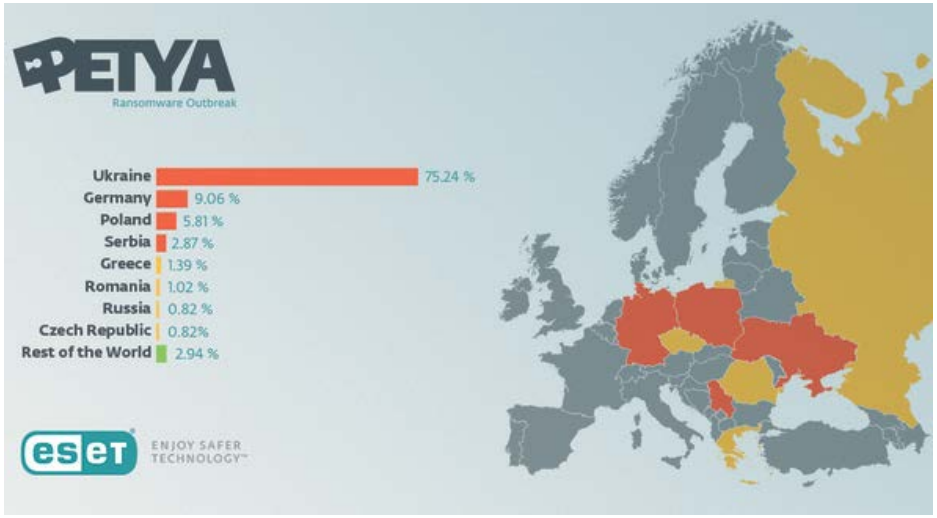
Internationalisation of Cyber Threats

- Cyber losses are now being reported in almost **every country** of the industrialized world with individual malware attacks flowing across international boarders.
  - Increased complexity
  - Increased connectivity with IoT

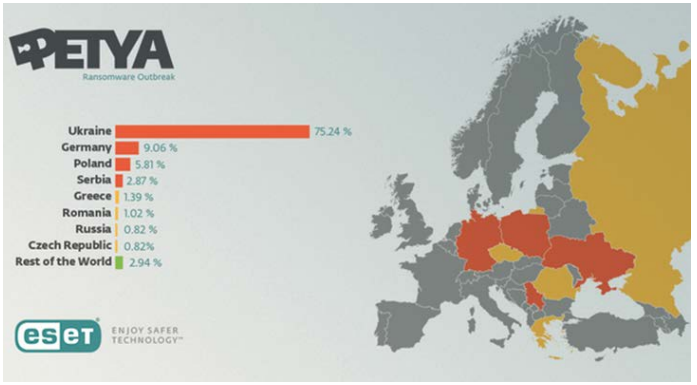
WannaCry

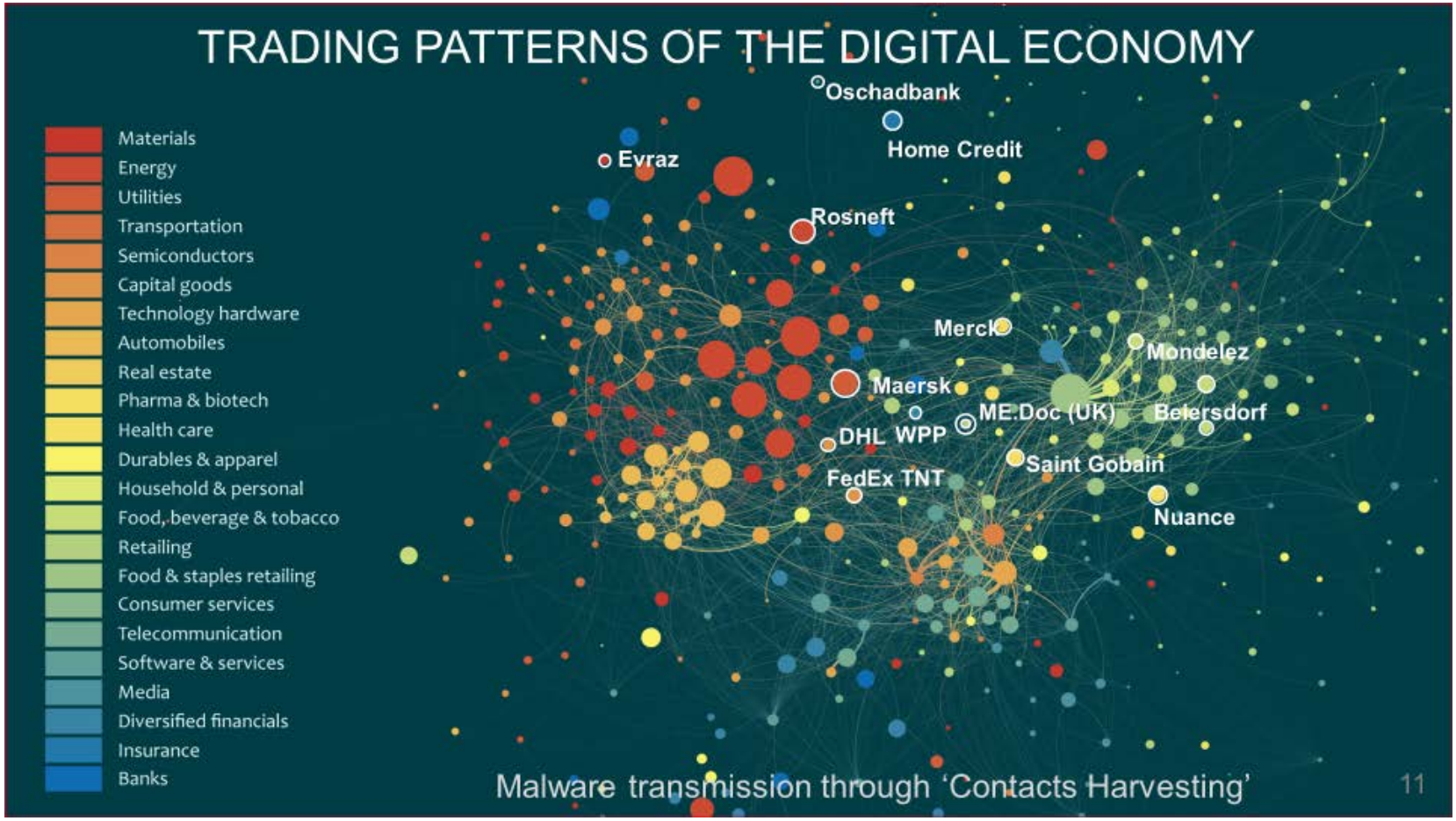


Not Petya

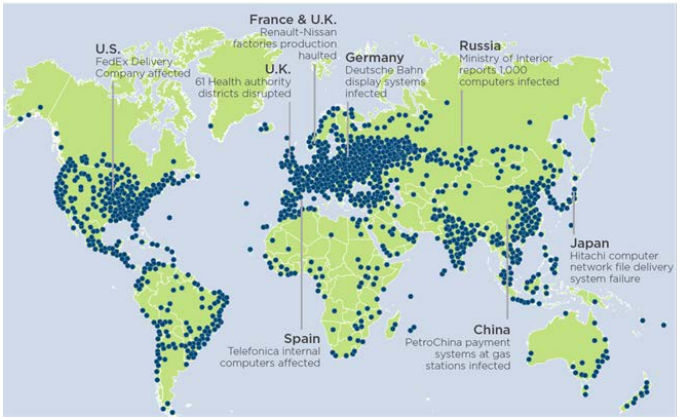


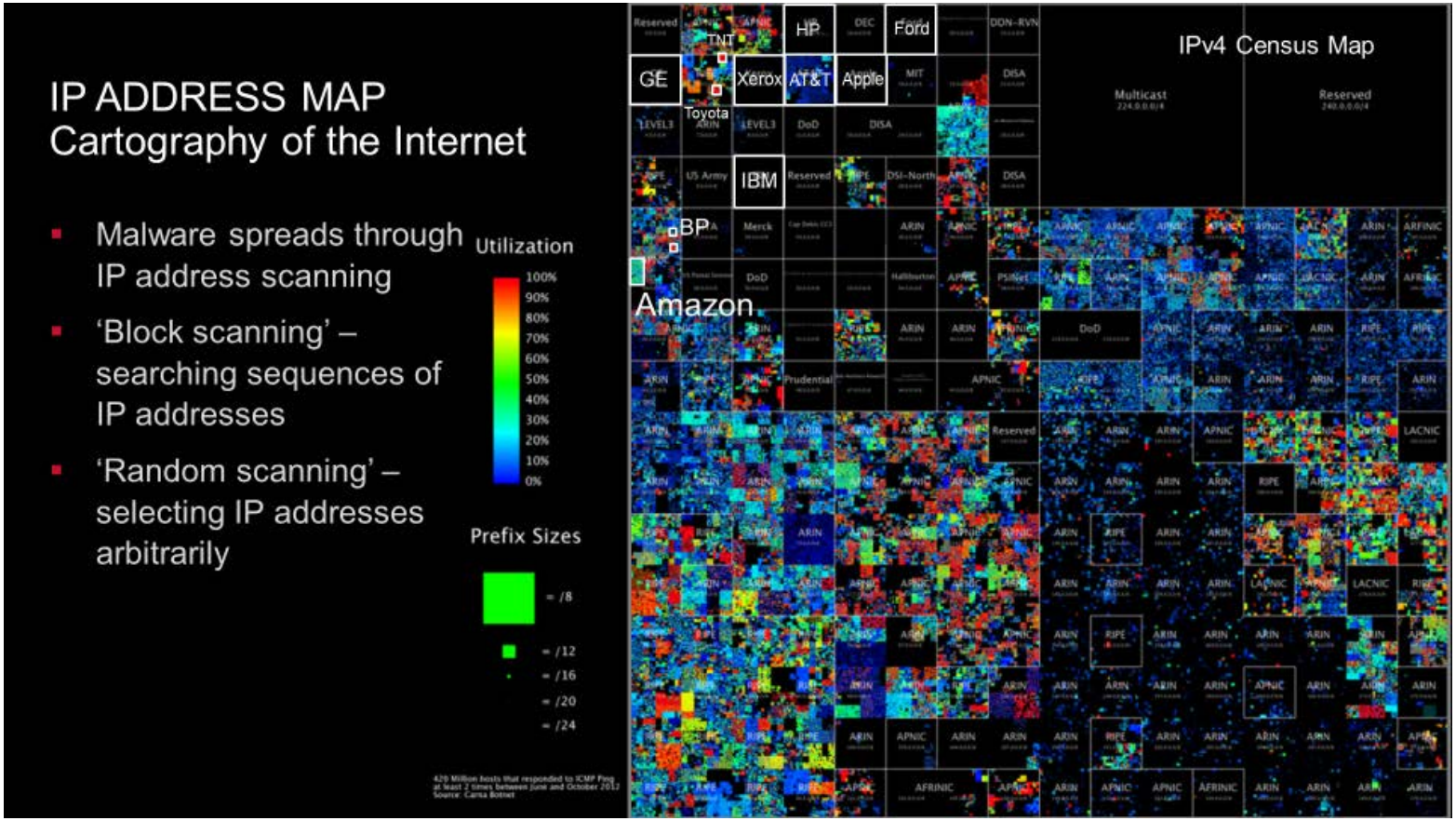
Global Geography – Not Petya





Internet Geography - WannaCry





Cryptocurrency Gold Rush

- **Cryptocurrencies:** digital currencies created by using computer programs and computing power and reported on the block chain.
- **Cryptomining:** the devoted use of a device's computing power to 'mine' for cryptocurrencies.

2017 saw coin-mining activity increase by over 34,000%

Rise in value of cryptocurrencies

Browser based mining systems

- **Cryptojacking:** using the computing power of a device to mine for currency without consent.
  - ***Adylkuzz*** is described as a piece of malware that infects computers through the same means as WannaCry but, instead of locking files on computers, hides in the background and uses victims processing power for cryptomining.
    - significantly predates the WannaCry attack and is ongoing
    - Blacked SMB port from further exploitation

Multiplicity of Ransomware

- **Ransomware** is known for encrypting and preventing access to files, but it has also been used as a cover for other types of attacks.
    - Data Exfiltration
    - Disk Wiping
    - Data Corruption

- **Case study: Sandworm Cyber Espionage 2016**
    - Rendered computers unusable by encrypting operating system files
    - Used against Ukrainian electricity grid
        - Cut power to up to 80,000 customers for about 6 hours
        - Similar to a DDoS attach in that it prevented effective communication and response management

Cyber Crime as Service

- Cyber criminals **no longer** need the know-how for an attack
  - Internal Zero-Day Exploit: **Up to $1 million**
  - Commodity Zero-Day Exploit: **$5,000-$100,000**

Type	Malware Name	Price
Exploit Kits	Whitehole	$600 / month
	Sweet Orange	$1800 / month
	Eleonore	$1000
	Gpack	$1000
	Cool (+cyrpter+payload)	$10,000 per month
Zero-Day	Windows	$60,000
	Microsfot Office	$50,000
	Mac OSX	$20,000
	iOS	$100,000
	Chrome/Internet Explorer	$80,000
	Adobe Reader	$5000

- **Case Study: Counter Antivirus Service reFUD.me**
  - Allows programmers to test whether their malware would be stopped or detected by antivirus software.
    - One month: $7.99
    - Lifetime subscription: $90

Supply Chain Attack

- Outsourced internet connected services allow for an indirect route into a business or customers
- Reported that 56% of organizations have had a breach that was caused by one of their vendors
- At least one large software update supply chain attack reported every month in 2017.

Targeting Supply Chains

- Difficult to detect
- Leverages a less protected trusted channel
- Fast distribution through network access
- Can allow for specific sector targeting
- Potential to access isolated targets
- Additional accessibility privileges

Case Study: 2017 Not Petya

Hackers corrupted a legitimate tax software package 'MeDoc', affecting clients of the software provider.

Case Study: 2014 Heartbleed

Affected millions of websites and mobile devices as well as software by many major vendors including Oracle, VMware and Cisco.

Case Study: 2014 Target Breach

Stolen vendor credentials for a heating and air conditioning contractor allowed access to customer information.

Looking forward…

Cyber risk research continues to grow as priority for corporations. In addition to monitoring and interpreting trends, the Cambridge Centre for Risk Studies works to understand Cyber Risk by creating and researching:

- Contagious Malware Models
- Corporate Cyber Risk Profiles
- Cyber Catastrophe Scenarios
- The Role of Cyber Threats in Terrorism
- The Tactics, Techniques, and Procedures of Threat Actor Groups

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School