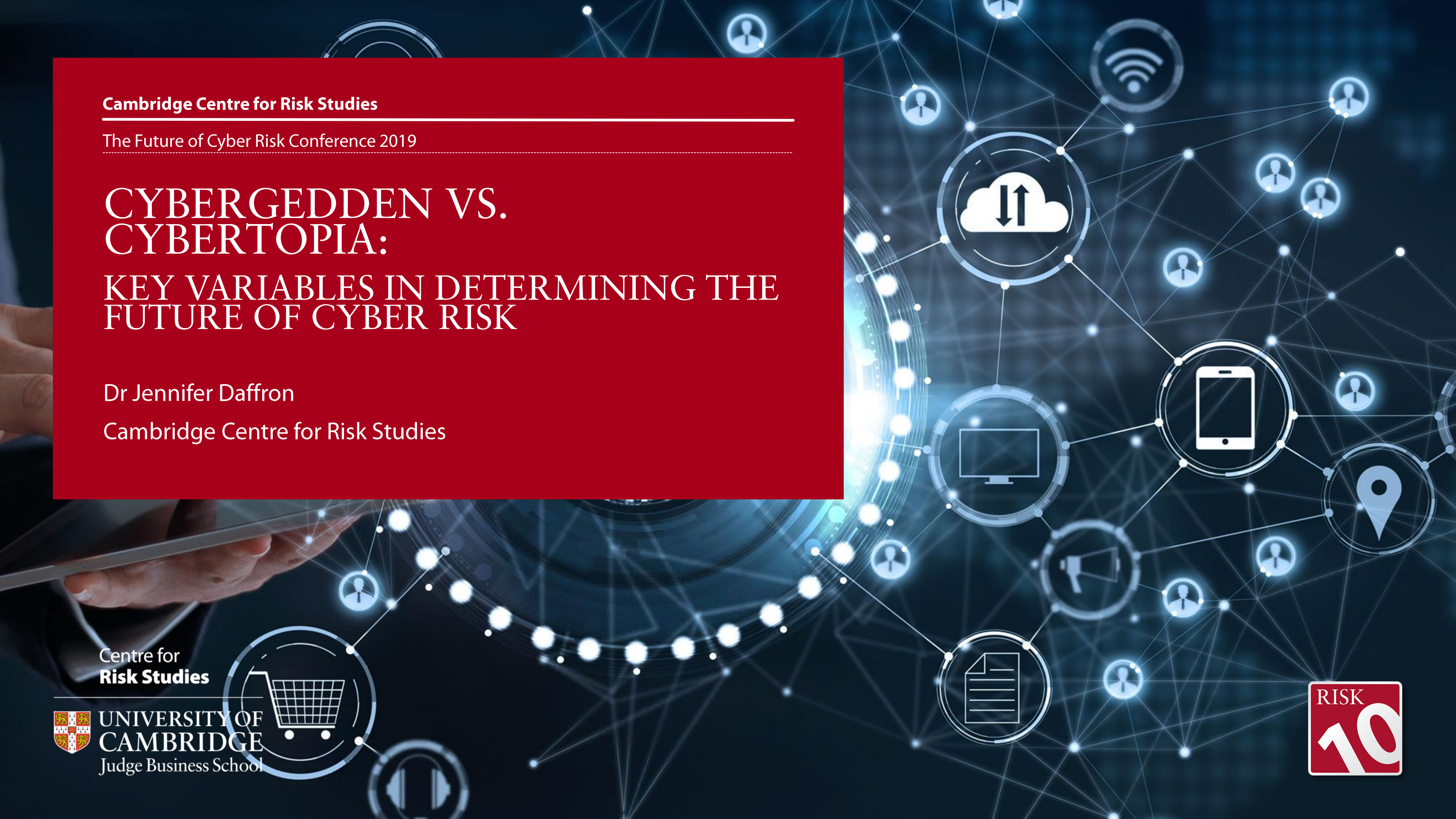


Cambridge Centre for Risk Studies

The Future of Cyber Risk Conference 2019

CYBERGEDDEN VS. CYBERTOPIA:

KEY VARIABLES IN DETERMINING THE FUTURE OF CYBER RISK

Dr Jennifer Daffron

Cambridge Centre for Risk Studies

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

RISK 10

The Futures of Cyber Risk

How might the many futures of cyber risk play out?

Cybergeddon

Refers to cataclysm resulting from a large-scale sabotage of all computerized networks, systems and activities

Goodwin, 2014

Cybertopia

A utopia in cyberspace or achieved by means of computer technology and user education.

The Futures of Cyber Risk

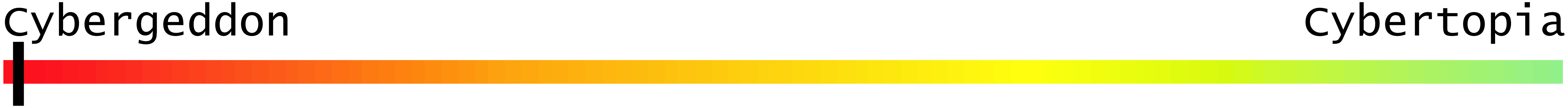
How might the many futures of cyber risk play out?

Cybergeddon

Cybertopia

The Futures of Cyber Risk

How might the many futures of cyber risk play out?



Cybergeddon

Cybertopia

Hacker hordes rise

Constantly increasing attack surface

Vulnerable technologies

Powerful attack technologies

No data is safe

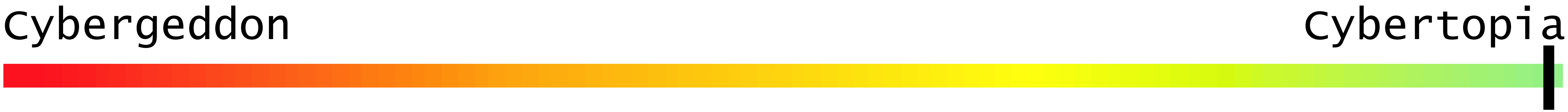
Splinternet

Consumer ecommerce dies

Cyber war

The Futures of Cyber Risk

How might the many futures of cyber risk play out?



Cybergeddon

Cybertopia

Minimal to no organized cyber crime

Complete trust in security

Data is protected

Secure technologies

International cyber regulation and cooperation

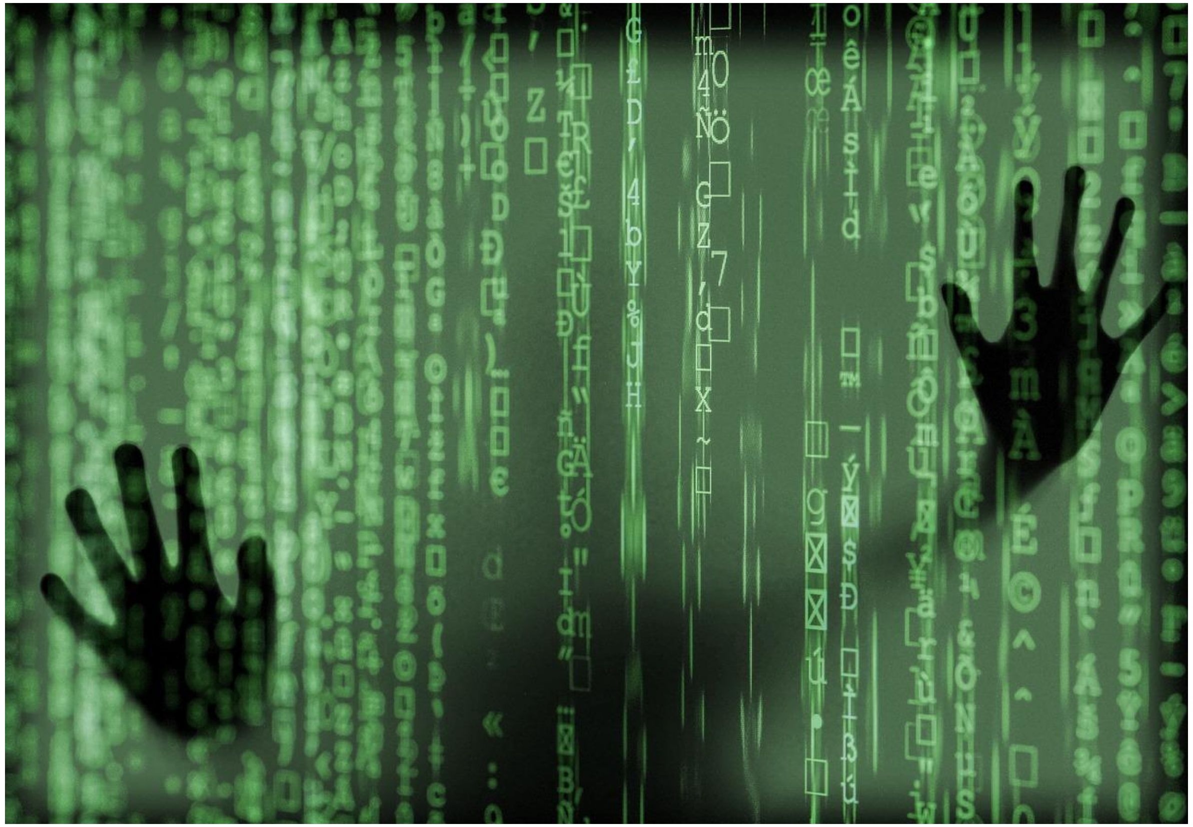
Growth of ecommerce

Complete user education

Key Variables

The future of the cyber risk landscape is unknown, but there are a few key variables that indicate whether we are headed for a cybergeddon, cybertopia, or a mix of the two.

1. International cyber regulation
2. The cost / benefit balance of holding data
3. Logistical burden of cyber crime



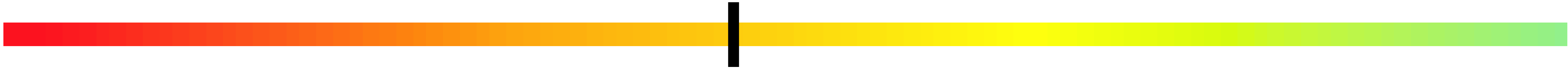
International Cyber Regulation

Complexities of International Cyber Regulation:

- Jurisdiction: Unlike traditional physical crimes, cyber crimes are not necessarily easily placed on a map and often have a global spread.
- Conviction Rates: The traditional evidence needed for conviction of physical crimes are difficult to procure for cyber crimes.
- State-Sponsored: Cyber technologies are being developed for offensive and defensive warfare capabilities, leading to low transparency and coordination.
- Geopolitical Events: Political climate between countries affects cooperation in cyber regulation

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

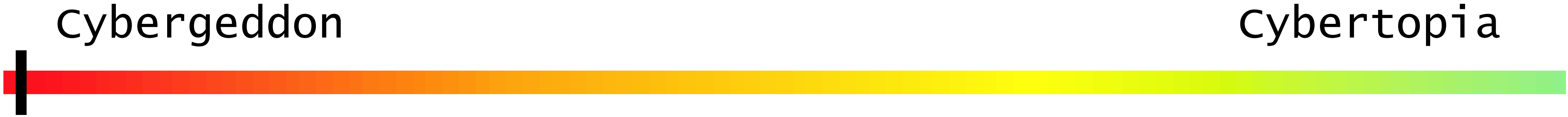
International Cyber Regulation



Cybergeddon

Cybertopia

International Cyber Regulation

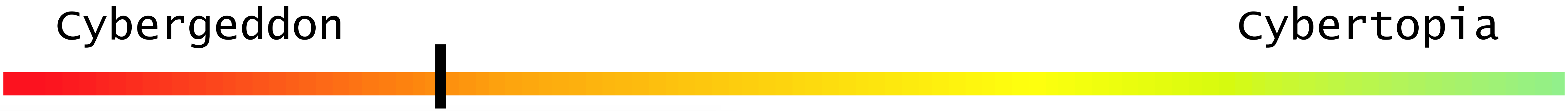


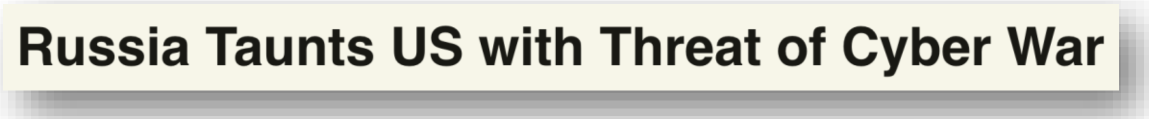
Cybergeddon

Cybertopia

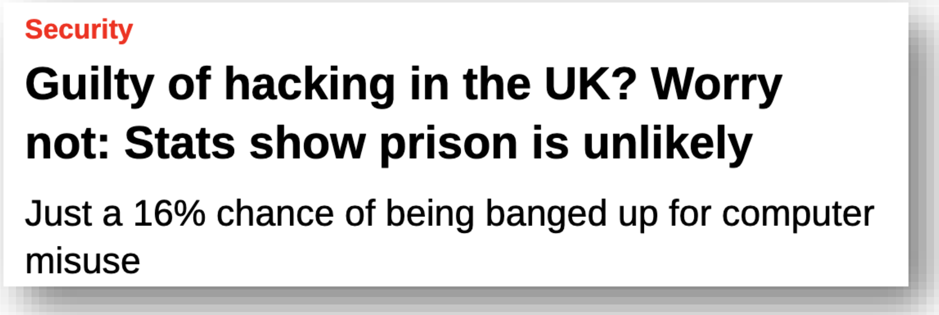
- Lack of international cyber regulations
- Low conviction rate
- Issues of jurisdiction for criminal vs. crime
- Increased state investment in cyber warfare
- Decrease in budgets for attracting new talent to cyber defense

International Cyber Regulation and Cooperation





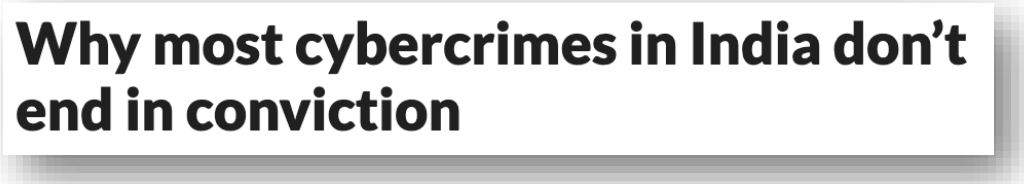
Russia Taunts US with Threat of Cyber War



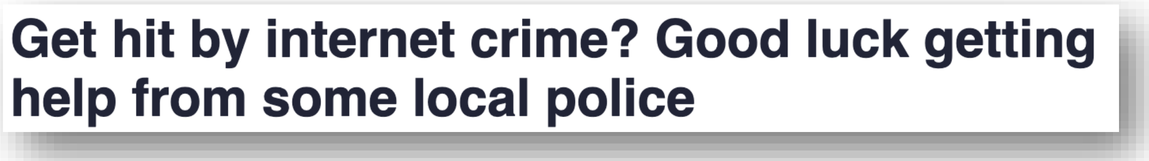
Security

Guilty of hacking in the UK? Worry not: Stats show prison is unlikely

Just a 16% chance of being banged up for computer misuse

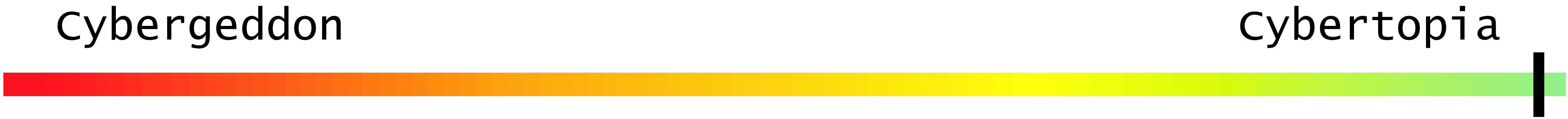


Why most cybercrimes in India don't end in conviction



Get hit by internet crime? Good luck getting help from some local police

International Cyber Regulation

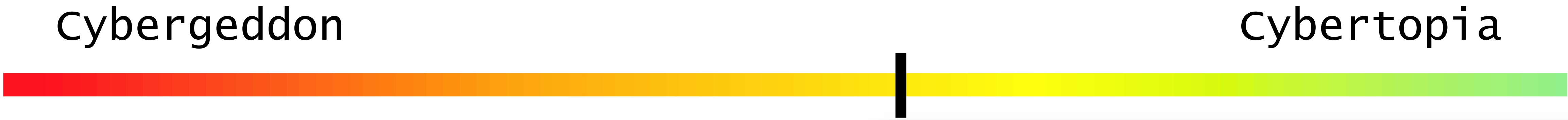


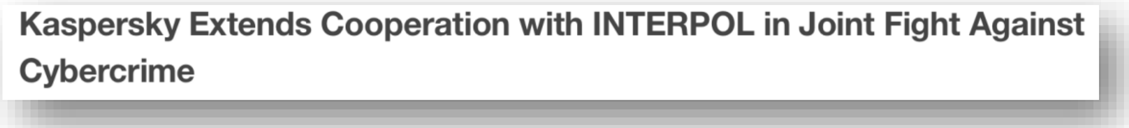
Cybergeddon

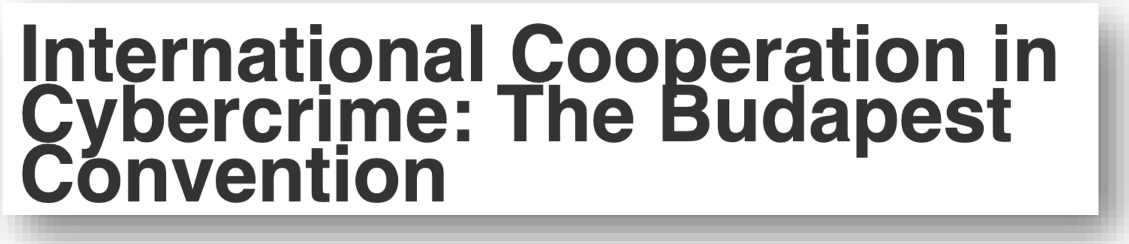
Cybertopia

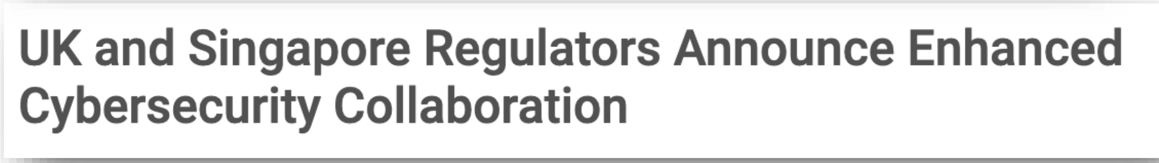
- Reinvention of law enforcement
- Establishment of international cooperation and regulation
- Political support for cyber crime reduction
- Higher conviction rate
- Close of dark web trading platforms

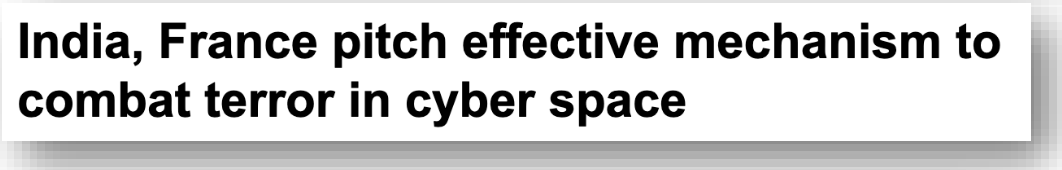
International Cyber Regulation and Cooperation

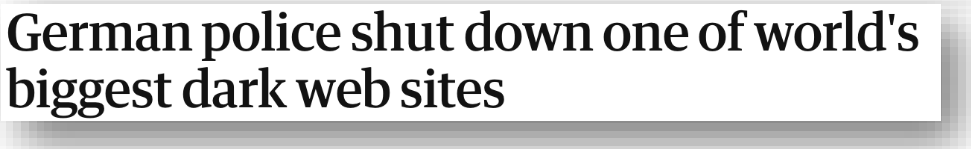



Kaspersky Extends Cooperation with INTERPOL in Joint Fight Against Cybercrime


International Cooperation in Cybercrime: The Budapest Convention


UK and Singapore Regulators Announce Enhanced Cybersecurity Collaboration


India, France pitch effective mechanism to combat terror in cyber space

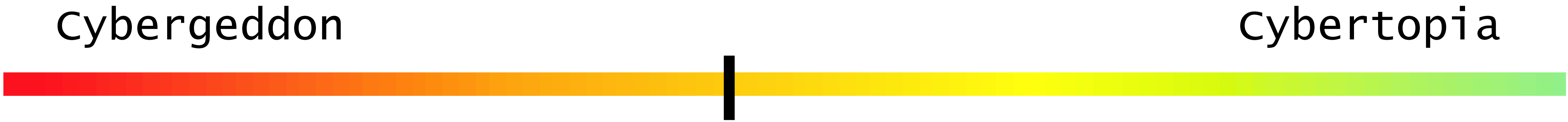

German police shut down one of world's biggest dark web sites

The Costs and Benefits of Data

Complexities of the Costs and Benefits of Holding Data:

- Data is constantly being collected, analyzed, and stored. This data can inform trading patterns, customer purchase trends, the impact of news and monetary decisions.
- As personal data becomes more essential to business practices, its price to consumers, companies and criminals increases.
- Protection standards and fines for misconduct when done correctly can allow for trust in the security of data, but when these standards and fines begin to negatively impact the bottom line of companies, shortcuts are likely to be taken and security mistrusted.
- Migration of computing and storage to the cloud means security failures are likely to be rare, but catastrophic when they occur with the potential for hundreds of thousands of companies to be impacted by a single breach

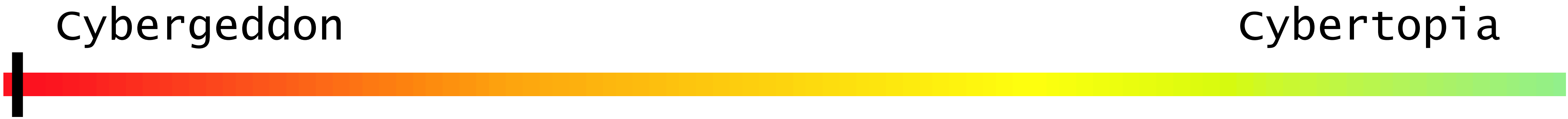
The Costs and Benefits of Data



Cybergeddon

Cybertopia

The Costs and Benefits of Data

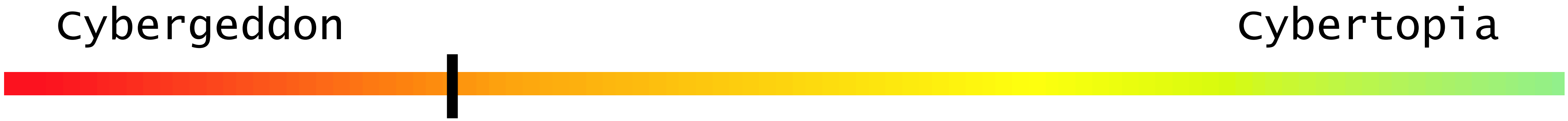


Cybergeddon

Cybertopia

- The costs for maintain and safeguarding data become too high to make big data analytics profitable
- Clients withdraw their permissions for big companies to use their data
- Fines for data loss prevent companies from collecting data
- Third-party data stores are not trusted

The Costs and Benefits of Data



Cybergeddon

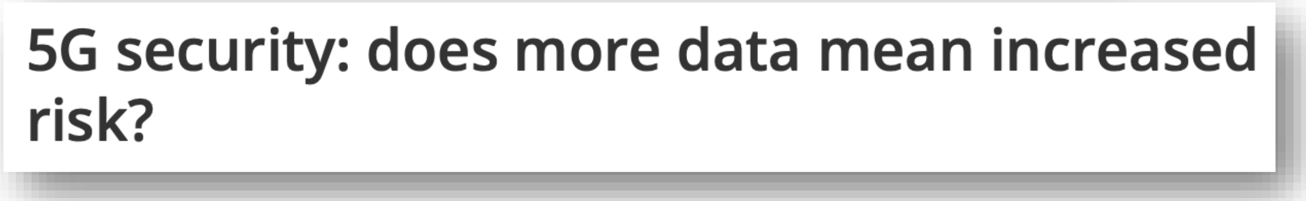
Cybertopia

Business

LabCorp discloses data breach affecting 7.7 million customers

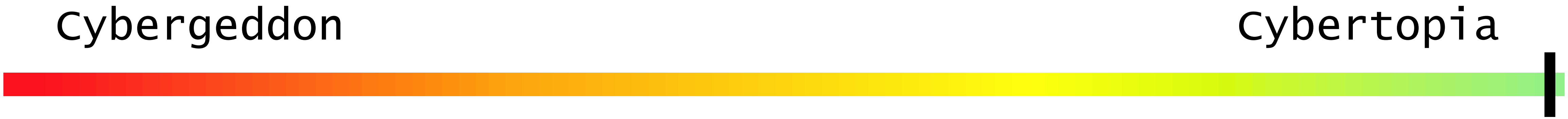
Facebook Must Face Lawsuit Over 29 Million-User Data Breach

Average cost of a data breach exceeds $3.8 million, claims report



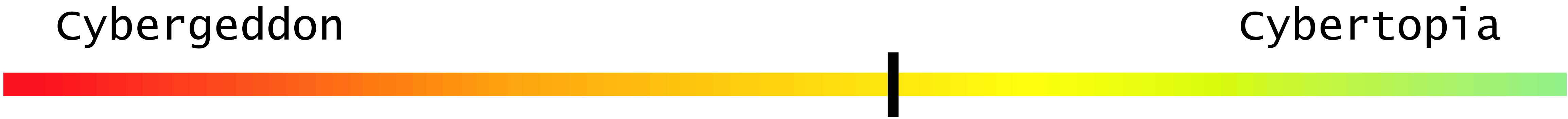
5G security: does more data mean increased risk?

The Costs and Benefits of Data

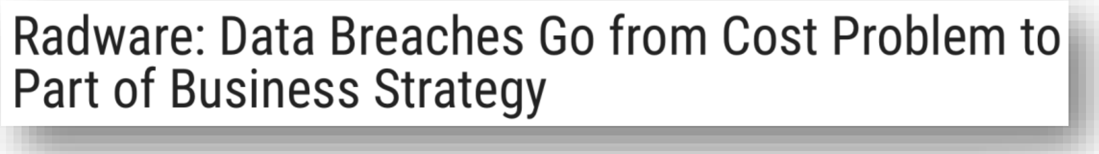


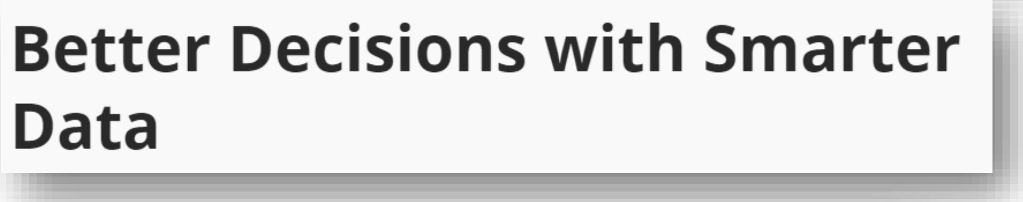
- Low costs for high quality products allow for data to be safely secured
- Big data analytics allow for smarter and more efficient work practices
- Data regulations keep companies from misusing customer data which instills greater trust and allows for greater data transfer

The Costs and Benefits of Data



GDPR rules prompt spike in data breach notifications


Radware: Data Breaches Go from Cost Problem to Part of Business Strategy


Better Decisions with Smarter Data

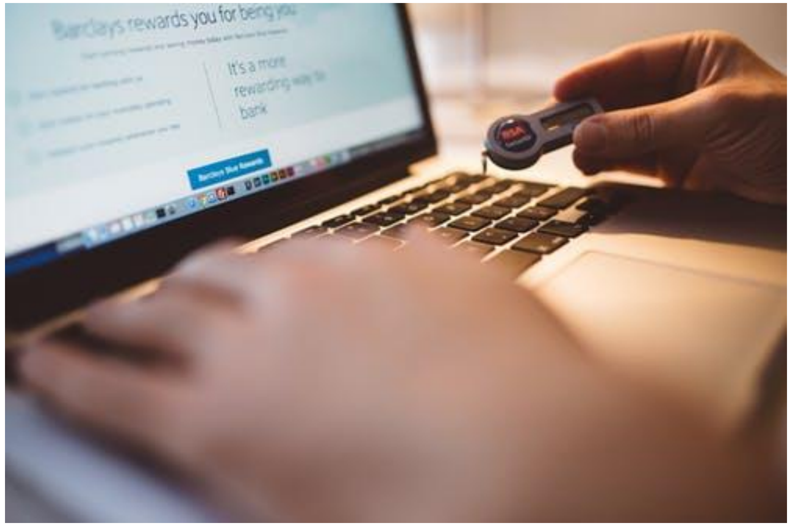
Big Data Analytics

What it is and why it matters

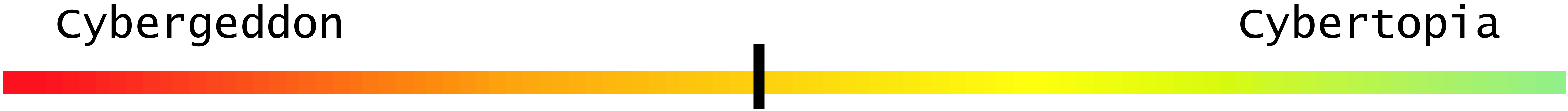
Logistical Burden of Cyber Crime

Complexities of the Logistical Burden of Cyber Crime:

- The logistical burden of a cyber attack considers the amount of effort and capital it will take to receive a reward. Protection of a network does not necessarily have to be perfect but it has to require more effort than attackers are willing to give.
- Commoditized malware reduces skill and cost needed for development
    - Malware as a service, ransomware as a service
- Resources, capabilities and tools available to nation state hackers would result in much more severe and extensive attacks
- Many more well-educated hackers become active, as an alternative to increasing graduate youth unemployment
- The past year has seen one of the lowest conviction rates for cyber criminals in recent years despite record levels of cyber crime


Barclays rewards you for being you
It's a more rewarding way to bank

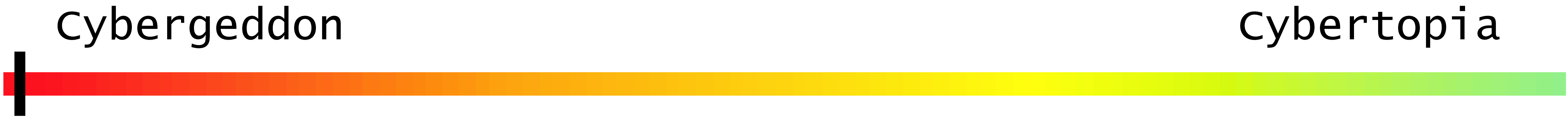
Logistical Burden of Cyber Crime



Cybergeddon

Cybertopia

Logistical Burden of Cyber Crime

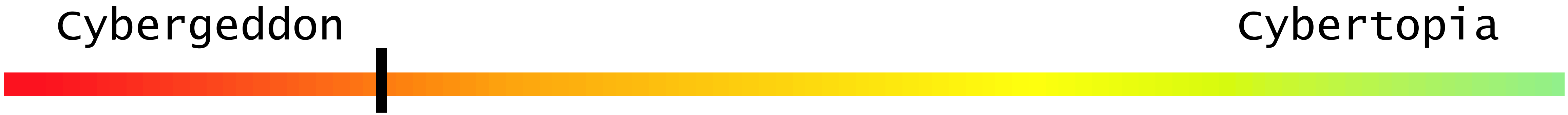


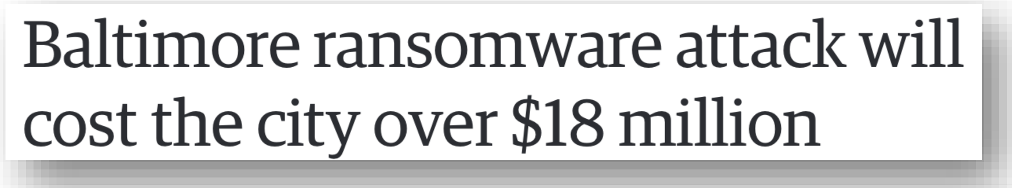
Cybergeddon

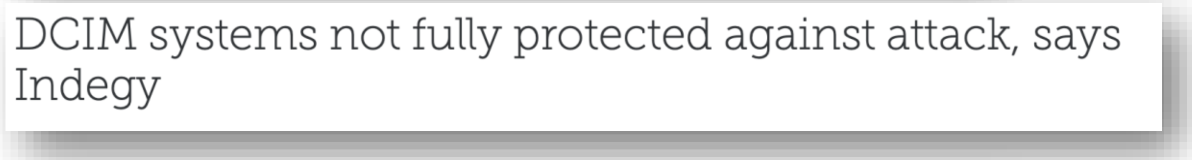
Cybertopia

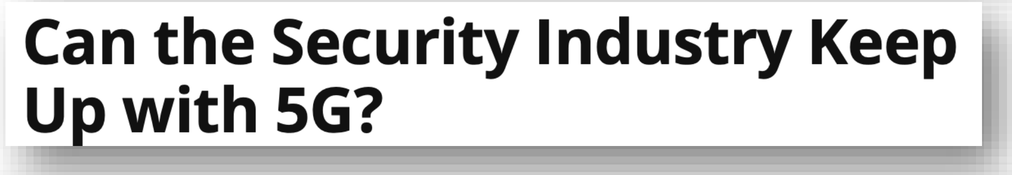
- Unchecked growth of IoT leaders to billions of vulnerabilities
- Opacity of victims prevents sharing of dangerous vulnerabilities
- Increased in rate of production of software prevents the development of necessary safety measures and patch rollouts
- Little to no law enforcement to deter cyber criminals
- Increase in payments of ransomware
- Industrialization of Malware

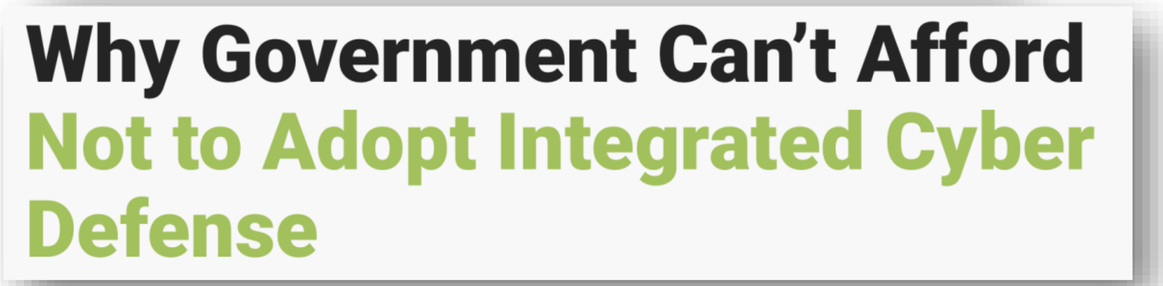
Logistical Burden of Cyber Crime



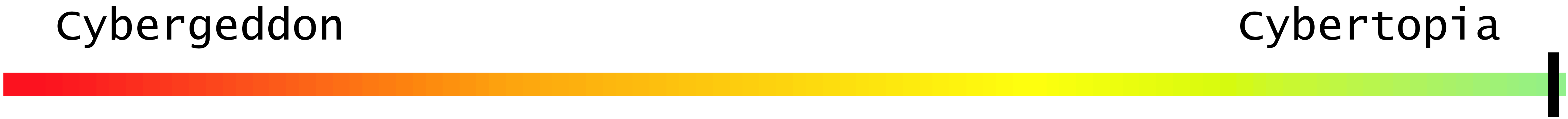

Baltimore ransomware attack will cost the city over $18 million


DCIM systems not fully protected against attack, says Indegy


Can the Security Industry Keep Up with 5G?


Why Government Can’t Afford Not to Adopt Integrated Cyber Defense

Logistical Burden of Cyber Crime



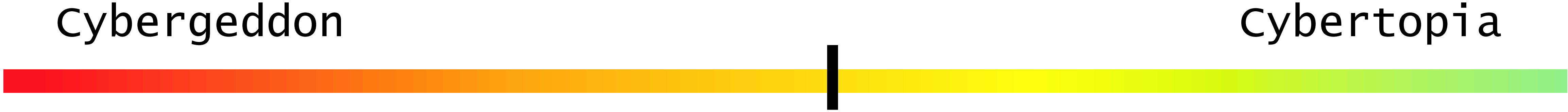
Cybergeddon

Cybertopia

- Software providers take responsibility and liability of software provided which increases security
- Patches are rolled out quickly and automatically which lowers the time cyber criminals have to take advantage of a vulnerability
- Transparency of victims allows for better prevention across industries
- High paying jobs for security professionals to defined
- High levels of law enforcement and conviction rate to deter crimes

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

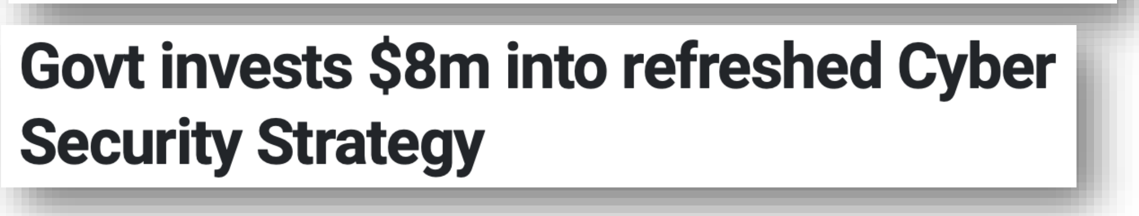
The Costs and Benefits of Data



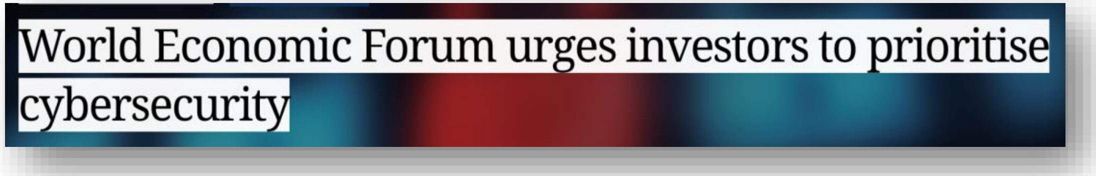
Cybergeddon

Cybertopia

Three-Tiered Security for the Internet of Things



Govt invests $8m into refreshed Cyber Security Strategy



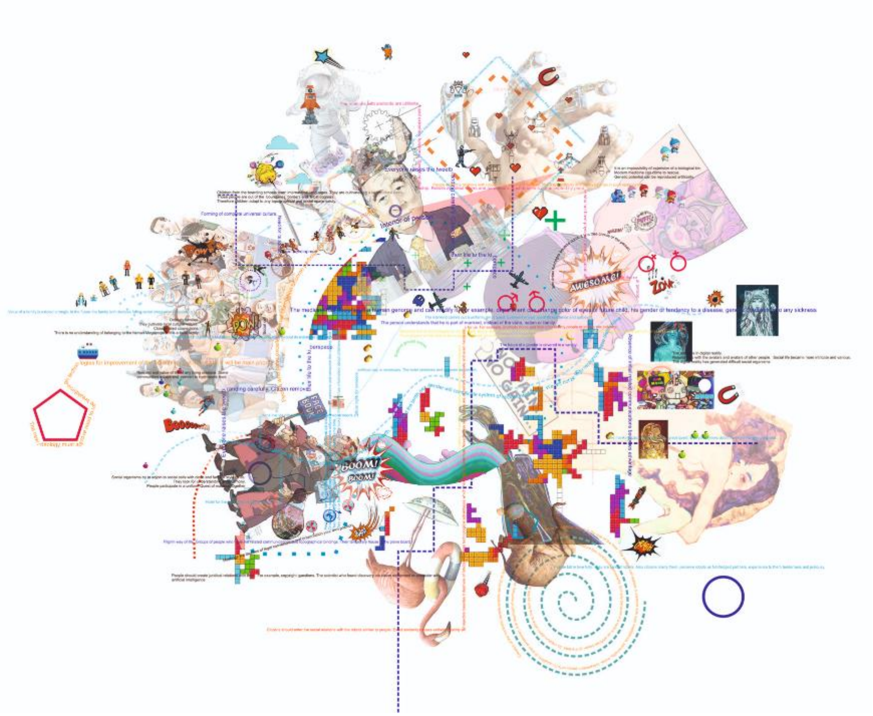
World Economic Forum urges investors to prioritise cybersecurity

The Futures of Cyber Risk

The cyber risk landscape is constantly changing, but key variables such as international cooperation, the costs and benefits of holding data and the logistical burden of cyber crime can help us to understand if we are headed for a cybertopia or cybergeddon.

There is a constant ebb and flow to where we fall on the spectrum but the these topics are **variable.** We have a say in what future of Cyber Risk will play out.

Source: BUSINESSTECH



Model of future society. Egor Orlov

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

RISK 10