



International Collaboration

International Information Sharing Conference

Wednesday 1st November 2017

↻ MalwareTech Retweeted



NCSC UK  @ncsc · May 13

Finding the kill switch to stop the spread of ransomware bit.ly/2qDoW6r



💬 21 ↻ 716 ❤️ 847 ✉



MalwareTech  @MalwareTechBlog · May 13

Well, that went about as well as anything i do does.

💬 33 ↻ 34 ❤️ 427 ✉

FACEBOOK FOR CYBER THREATS

CYBER CRIME ON THE RISE

FINANCIAL SEC Banks report rise in cyber crime

Secret HQ set up for battle over cyber crime.

The cyber threat is growing. Billions of dollars are lost every year to cyber attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights...to businesses trying to gain an edge...to the sophisticated by building computer networks, from rings of criminal masterminds to individual hackers.

Today, these computer hackers are becoming more sophisticated and are the primary source of cyber crime.

Overcoming the threat. In recent years, we've built a whole new set of technological and investigative capabilities and partnerships to be able to effectively chase cyber criminals in cyberspace as we've done back alley and street criminals.

A Cyber Division at FBI Headquarters "address cyber crime as a coordinated and collective mission."

Specialized cyber units at FBI Headquarters and in each of our 50 field offices, staffed with...

"Agencies and partners who coordinate resources to respond to cyber threats, including cyber terrorism, cyber espionage, cyber fraud, and cyber crime."



Exception and unusual regulated area problems, CA

excepteur sint occaecat

Excepteur sint occaecat...

Excepteur sint occaecat...

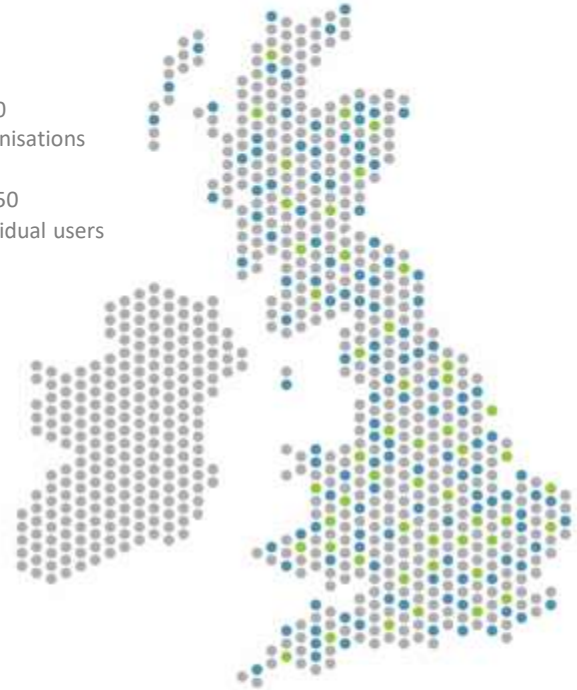


Proven success
With CiSP



Industry and
government work together

- 3,750
Organisations
- 11,750
Individual users



Across 25+ industry sectors



UK CYBER STRATEGY 2011-2016

Chapter 1. Tackling cyber crime and making the UK one of the most secure places in the world to do business

Cybercrime is an important and expanding part of our economy. Our mission is to tackle cyber crime and make the UK one of the most secure places in the world to do business.

Objective	Approach	Actions to include
Tackling cyber crime and making the UK one of the most secure places in the world to do business	Tackling cyber crime - Reducing online vulnerability - Reducing criminal activity online - Promoting more effective partnership Government and Home Office	1. Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for online offences. 2. Create a new national cyber crime capability as part of the new National Crime Agency for 2013. 3. Encourage the use of cyber specialists to bring in those with specialist skills to help the police. 4. Significantly increase the law enforcement agency capability by March 2012, and develop new training going from capacity, investigate and disrupt cyber crime. 5. More resources will go into working with the private partners in 2012, and from now SOCA will increase its international network. 6. Promote greater levels of international cooperation on cyber crime as part of the process begun by CyberSpace. In addition to promoting the Cybercrime (The Budapest Convention) and build on information systems. Contribute to the Data Protection Directive and the new Data Protection Directive and the new Data Protection Directive and the new Data Protection Directive. 7. Review existing legislation, for example that a remains relevant and effective. 8. By the end of 2011, build a system to report cyber or agencies can establish the system and the economy. 9. Commencing this system through. 10. Take action by Spring 2012. 11. Expansion of the UK cyber security sector without. 12. By the end of 2012, harnessing the wider private sector joint working initiative on cyber security to ensure that law enforcement fully engages with business in information sharing and minimising the risks from cyber crime. 13. Working with standards, European, global and commercial standards organisations to stimulate the development of industry led standards and guidance that help customers to navigate the market and differentiate good cyber security products. 14. Work with business services providers (including insurers, lawyers and auditors) to discuss how they can develop the services they offer to businesses to help them manage and reduce the risks. 15. Work with other countries to make sure that we can co-operate on cross border law enforcement and deny safe havens to cyber criminals. 16. Ensure that new national procedures (adopted in May 2011) for responding to cyber incidents, and the developing partnership between government and the private sector, facilitate appropriate information sharing on threats to business, with mitigating action aimed at reducing impacts. 17. Building (and, where necessary, building at pace) new operational partnership between the public and private sectors to share information on threats, manage cyber incidents, develop threat analysis and build cyber security capability and capacity led by the Prime Minister and representatives of industry, in place by March 2012.
	Making a safer to do business in cyberspace - Increasing awareness and visibility of threats - Improving incident response - Protecting information and services - Building a culture that manages the risks - Promoting confidence in cyberspace Government and all	

12. Starting in January 2012, harnessing the wider private sector joint working initiative on cyber security to ensure that law enforcement fully engages with business in information sharing and minimising the risks from cyber crime.

NCSC RESPONSIBLE FOR CISP

Who we work for

The National Cyber Security Centre serves a wide range of UK organisations across the entire spectrum of cyber security issues.

Consequently the service provided will be multi-layered, reflecting the different threats that organisations face, and the skills and resources they have to address them. Owners of networks, systems and data will remain responsible for managing the risks to their organisations: the NCSC will not represent a change to this principle of risk-ownership.

We have defined four categories of engagement to describe the scope of our offer:

The NCSC will provide general advice and guidance. The NCSC will be the lead security technical authority in the UK with overall responsibility for the technical aspects of all cyber security advice from the Government. The NCSC will work closely with the Cabinet Office, Law Enforcement, DCMS and other partners to ensure these messages are deployed as effectively as possible.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.

We propose that **the NCSC will provide tailored advice and guidance to sectors, and provide a forum for discussion from beginner through to expert level.** The NCSC will form the core of the UK's cyber security response, and will be the lead authority for the UK's cyber security response.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.

"Action Fraud will continue to be the first port of call for victims to report suspected cyber crime".

However, when there is a significant cyber incident affecting the UK, the NCSC will have the leading role for government in communicating to the public, to provide reassurance and guidance on what individuals and organisations can do to better protect themselves.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.



UK RESPONSIBILITY



National Cyber
Security Centre

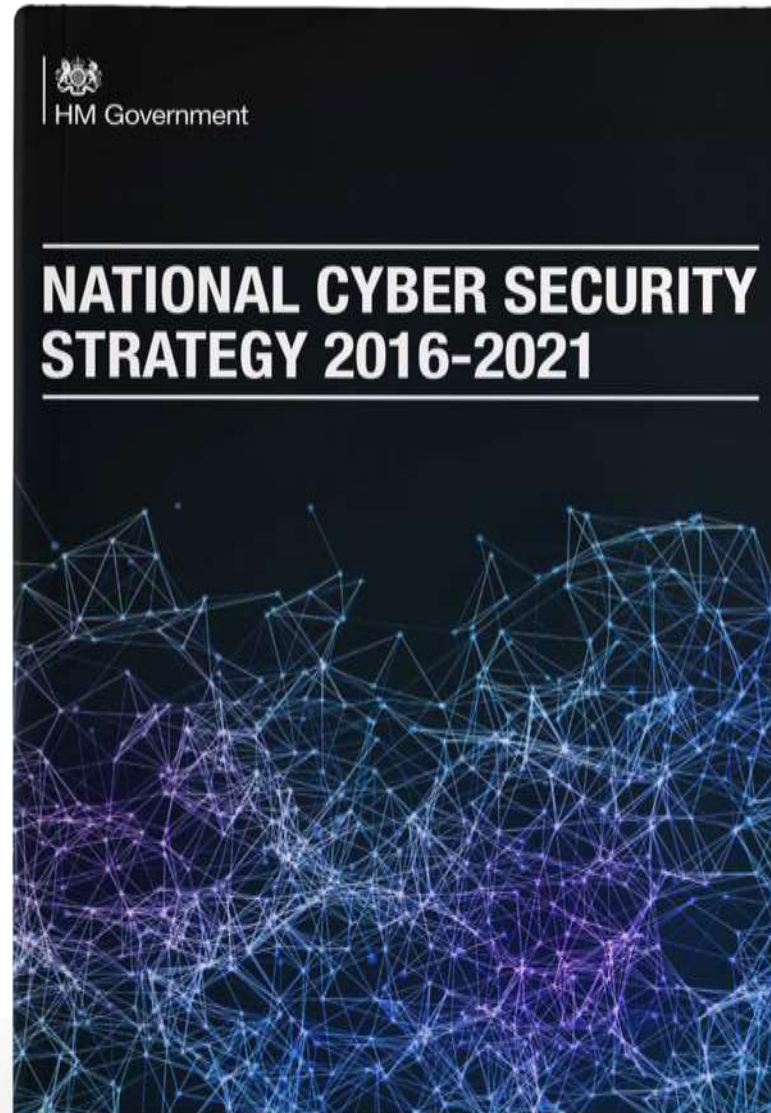
a part of GCHQ

CPNI

Centre for the Protection
of National Infrastructure



SHARING IS
STRATEGIC



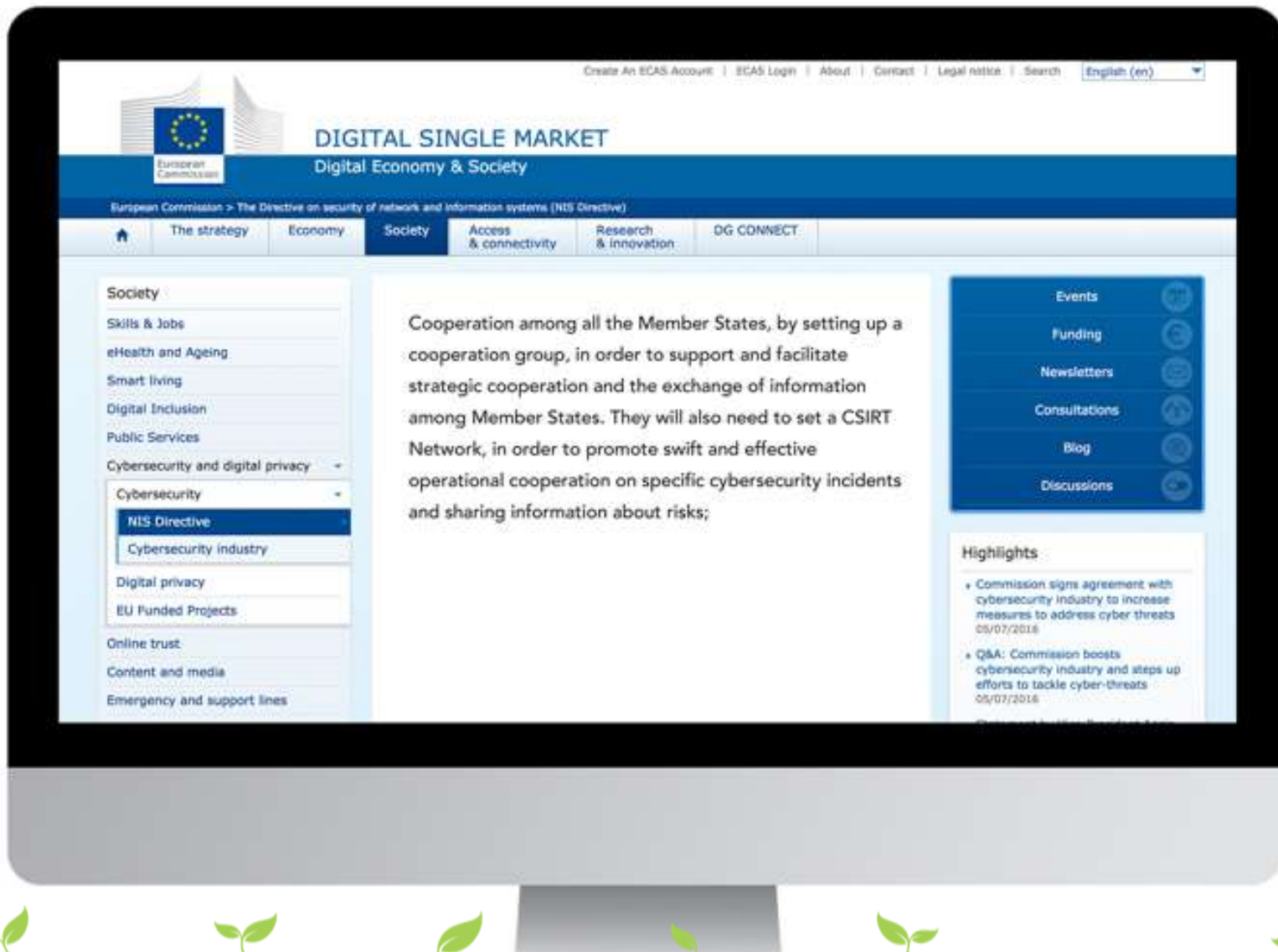
SHARING IN THE US



FINANCIAL | **ISAC**
SERVICES



EUROPE NISD



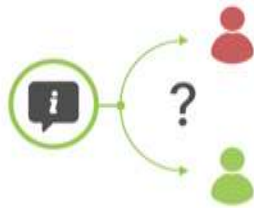
DIB – MANDATORY SHARING



WHERE INFORMATION GOES TO DIE



CHALLENGES



NOT SURE WHO TO TRUST
WITH YOUR INFORMATION



WAITING FOR OTHERS TO
SHARE PUBLICLY IS SLOW



NO EASY WAY FOR THIS
INFORMATION TO BE SHARED



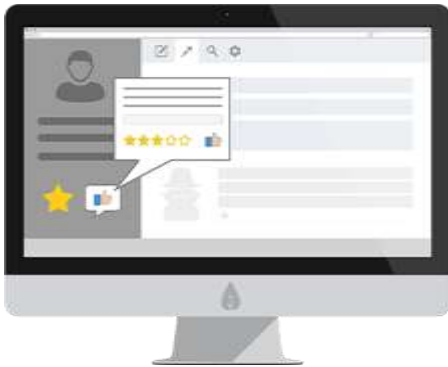
NOT SURE WHOSE
INFORMATION YOU CAN TRUST



PUBLIC DISCLOSURE DOES
NOT ALWAYS HAPPEN



FEATURES



COMMUNITY



ANONYMITY



INFORMATION
HANDLING



INCIDENT REPORTING





SECURE PLATFORM MAINTAINED
BY TRUSTED PARTY



QUICK AND EFFICIENT SHARING
THROUGH STRUCTURED DATA



USE INDUSTRY-RECOGNIZED TRAFFIC
LIGHT PROTOCOL
(TLP) TO CONTROL SHARING



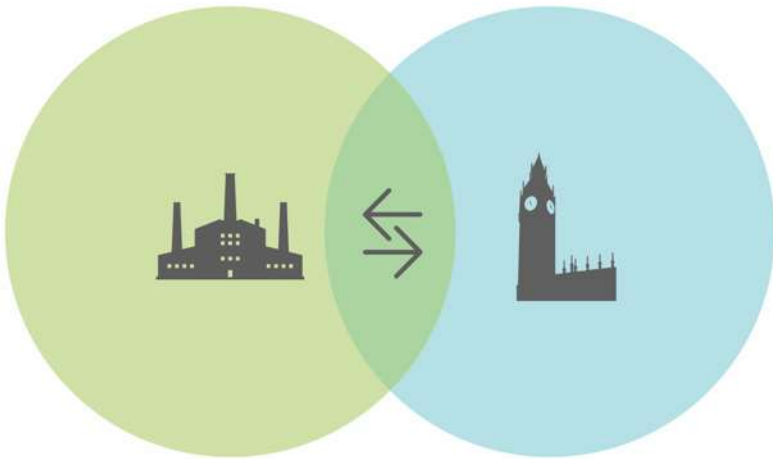
TERMS & CONDITIONS
THAT ALL MEMBERS
MUST AGREE TO



NEW MEMBERS ARE REVIEWED
BEFORE JOINING TO
MAINTAIN TRUST



OVERSIGHT...



FUSION CELL



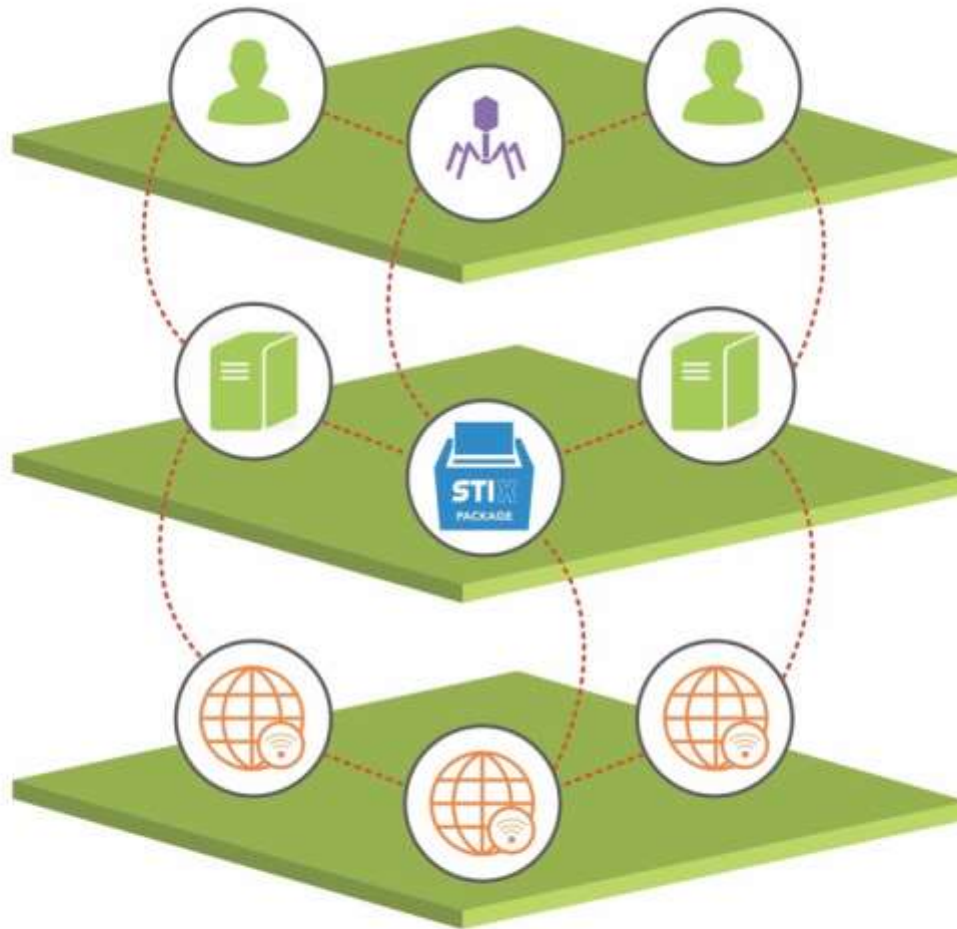
ANALYSE PATTERNS
ACROSS ALL SECTORS,
PROVIDE CONTEXT



GLOBAL DEMAND



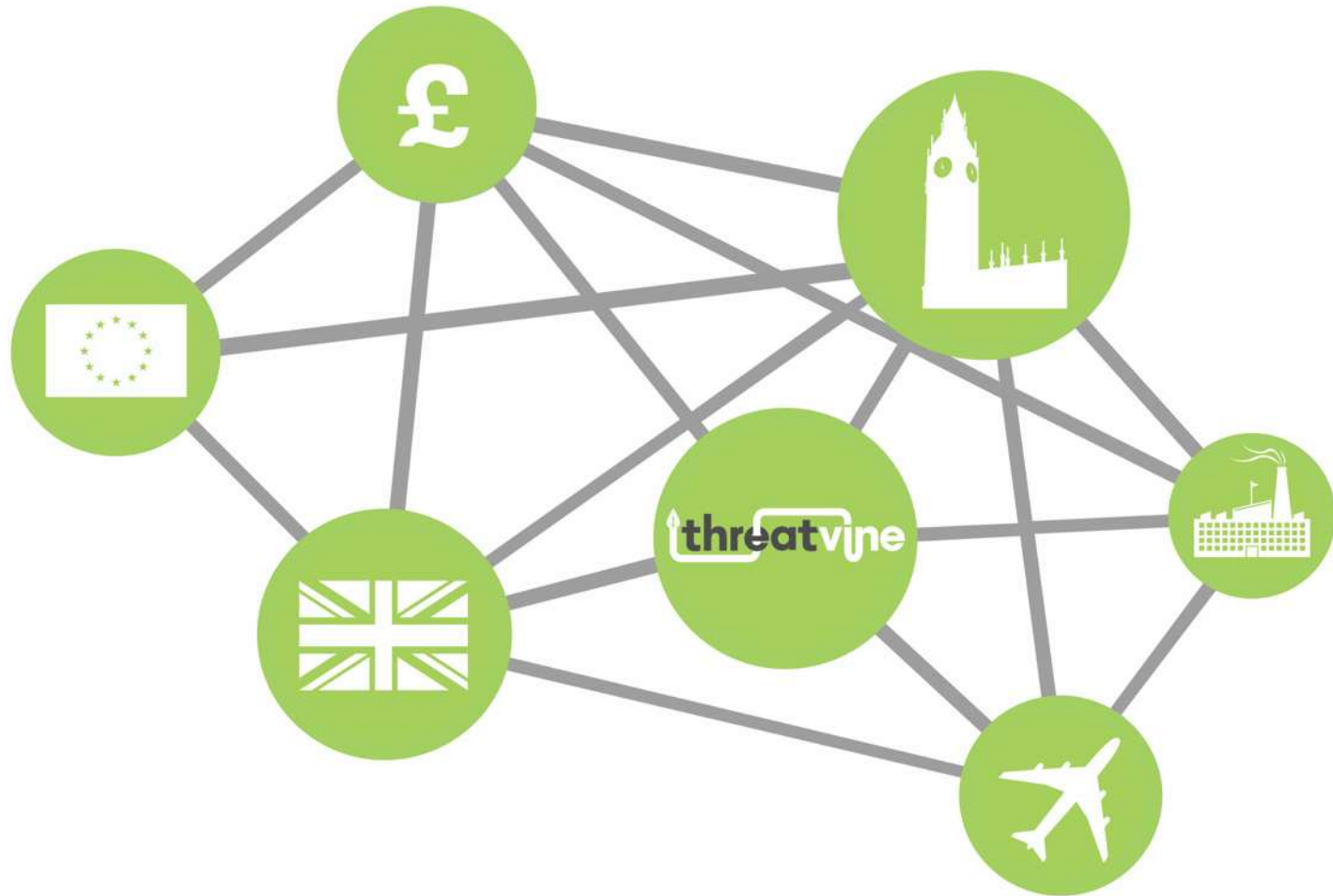
SHARING GOES DEEP



GLOBAL ALLIANCES



BORDERLESS OR SOVEREIGN?



HUB vs FEDERATION

- Centralised model - trusted authority
- National level collaboration
- Challenge: collaboration across boundaries



- Federated model
- Control who, what
- Protect data sovereignty

PLAY BY THE RULES



Secure Government and military communications nationally and trans-nationally





Secure Information Sharing

Cyber-security information sharing platform
designed for secure cross-organisational
collaboration and collaborative
intelligence analysis.





Participate | Collaborate | Innovate

