Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA

Wayne Harrop and Ashley Matteson

Received (in revised form): 16th August, 2013

Centre for Disaster Management, Coventry University, Priory Street, Coventry CV1 5FB, UK
Tel: +44 (0) 207 688 7689
E-mail: w.harrop@coventry.ac.uk; E-mail: ashmatteson@hotmail.com

Wayne Harrop *is Director of the Centre for Disaster Management at the University of Coventry. He has developed a hybrid career as an academic and practitioner, winning three international industry accolades and contributing to funded research projects worldwide. Mr Harrop is part of a national cyber-security advisory cell led by the Bank of England. Mr Harrop co-directs the International Risk, Resilience and Response Centre (a UK–US partnership), which has successfully delivered international briefings on homeland security, disaster impacts, national infrastructure and cyber security. Mr Harrop is a co-opted expert on the BSI committee that drafted BS25999 and currently sits on the Advisory Council for City Security and Resilience Network.*

Ashley Matteson *currently serves as a steering group member and cyber security adviser to the International Risk, Resilience and Response Centre (IRRRC), chaired jointly by Coventry University in the UK and Texas A&M University Engineering Extension in the USA. Mr. Matteson has completed and become certified in all foundation and capability based Information Technology Infrastructure Library (ITIL) v3 courses. His ITIL training has added to an extensive background in IT and business with a bachelor's degree in IT and a master's in business administration. Mr. Matteson's unique background and experience has made him a sought-after author and lecturer on cloud computing and cyber security topics. He enjoys raising public awareness on how to be safe online though these opportunities and through his work with the IRRRC.*

Wayne Harrop

Ashley Matteson

ABSTRACT

This paper presents cyber resilience as key strand of national security. It establishes the importance of critical national infrastructure protection and the growing vicarious nature of remote, well-planned, and well executed cyber attacks on critical infrastructures. Examples of well-known historical cyber attacks are presented, and the emergence of the 'internet of things' as one of the cyber vulnerability issues yet to be tackled is explored. The paper identifies key steps being undertaken by those responsible for detecting, deterring, and disrupting cyber attacks on critical national infrastructure in the United Kingdom and the USA.

Keywords: national security, cyber-attacks, cyber security, DDoS, CNI, CIKR, IoT, US Cyber Security Act 2012

INTRODUCTION

Imagine a future world held to ransom by the demands of a hidden unnamed force

Journal of Business Continuity & Emergency Planning
Vol. 7 No. 2, pp. 149–163

1749–9216

lurking behind computer screens and operating in murky shadows. Imagine the same forces causing indiscriminate and lasting harm in an ever-increasing technologically dependent world. A world where a private GPS or home smart meter could be hacked and reprogrammed remotely without permission or knowledge; where financial systems might unexpectedly suffer malicious downtime, where ICT systems are hacked to steal highly confidential information or intellectual property; where power grids are interfered with, water treatment plants remotely breached and attacked by digital terrorists and cyber activists and public transportation networks (ICT systems) targeted to cause maximum chaos during peak travel periods. Maybe this all sounds like another Hollywood blockbuster movie. However, consider the alternative that it is a real prospect. If so, what can be done to safeguard the basic way of life? In particular, what is being done by countries like the UK and USA to safeguard the security people have come to expect and enjoy but may take for granted?

The nature of cyber space and everyone's growing reliance upon it is constantly changing and the way advanced users operate in a modern decentralised cyberspace environment provides good cover and anonymity for an intelligent foe, making the attribution of any cyber-attack very difficult to pinpoint. One thing is certain, cyber-attacks are growing at an alarming rate worldwide and this includes both the UK and the USA. The threat is especially focused and targeted towards government systems, business and commerce. The public might get caught up in the crossfire where the threat infiltrates what they rely upon to sustain their daily activities. Recent examples include attacks on Barclays and Santander banks. "Barclays bank [was attacked] using a remotely-controlled KVM (keyboard-video-mouse) device and 3G routers. [The attack was] described by police in the United Kingdom as being a "Mr Big" of UK cybercrime. [The attackers] are said to have stolen £1.3 million ($2 million) from Barclays bank, before being caught."[1] In addition to the Barclays attack, Santander also recently foiled a cyber plot of a similar nature. Whatever the motive, cyber security is a very hot topic. There are several critical questions that must be answered in relation to cyber security to ensure the protection and integrity of systems and data. How prepared are the UK and USA for sustained and targeted attacks on their respective essential services delivered to the public through critical national infrastructure (CNI) and critical information infrastructures? Who is taking the lead on protecting national security on the public's behalf?

One certainty exists, cyber security concerns are becoming more apparent every day and the issue is likely to grow as a real and present challenge to the smooth functioning of any modern Western economy. The USA recognises cyberspace as a fifth domain of its own national security agenda in tandem with pre-existing domains such as land, sea, air and space. As such, the US government established the United States Cyber Command (USCYBERCOM) in 2009 to recognise that fact and organise a body under the US Department of Defense (DoD) to address cyber issues. On 22nd February, 2013 at the 4th Annual Cyber Security Conference in Washington DC, US Air Force Major General Brett T. Williams, Director of Operations at US Cyber Command: said 'part of Cybercom's mission is to help in defending the homeland, especially against cyber-attacks and other activities in cyberspace that could affect national security'.[1] There are strong and compelling reasons why it is important to protect CNI from cyber-attacks, but there

is also an ill-defined enemy behind the emerging trend of cyber-attacks. The enemy could vary and understanding their evolving capabilities and organisational limits is crucial to fending off cyber-attacks orchestrated by a range of possible foes, such as state sponsored attackers, hackers, anarchists and criminal gangs. Recently, former US Secretary of Defense, Leon Panetta, stated: 'A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11, such a destructive cyber terrorist attack could paralyze the nation'.[2]

The DoD is believed to be probed millions of times a day by malicious cyber actors. By September 2011, DoD had identified over 70 million cumulative malware threats against its own networks. In the last few years, malicious actors have launched cyber-attacks against America's nuclear infrastructure, advanced military weapons systems, water treatment facilities, credit card companies, financial institutions and the NASDAQ stock exchange.[3]

THE INTERNET OF THINGS

The world is entering a new future reality where nearly anything that can be on the internet will be.

> 'Internet of Things (IoT) is an integrated part of Future Internet including existing and evolving Internet and network developments and could be conceptually defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network'.[4]

With the growth of the IoT, consumers should be cognisant that as homes become increasingly connected to smart and wireless devices and sensors, the national infrastructure extends its reach. Indeed in the home of the future, there will be improved access to remote digital content (such as cloud and streaming media content); service providers will monitor household energy consumption; and household appliance will be smart and networked.

> 'Many people think of the Internet of Things as some magic web of connected devices that will communicate with each other and act together, but the reality is probably closer to the vertical segmentation we already have in our lives. So while we might have an Internet of electricity that combines elements of the smart grid with our thermostats, we may have to buy some kind of device that we plug our appliances into to connect them to the Internet of electricity'.[5]

The additional devices might be simple routers or other networking equipment that connect together the devices in the home so they can communicate with each other as well as provide streaming services, such as weather forecasting and internet radio broadcasts. Although IoT brings much convenience to the consumer, it could also introduce great vulnerability and must be a part of future cyber security strategies. As many of IoT devices are used to manage power usage they often feed the smart utility grids operated by power companies. As such, the best approach to securing IoT devices against cyber attack is by protecting the smart grids to which they are connected, while employing basic internet security in the home networks to which they are connected, such as firewalls and routers that only allow expected traffic to the connected devices (streaming

radio feeds, weather forecasts, outgoing data streams to the smart grid reporting usage, etc). Much of the areas discussed above have some direct or indirect relationship to CNI.

THE UK APPROACH TO CYBER SECURITY

In the UK, the Centre for the Protection of Critical National Infrastructure (CPNI) defines CNI as: 'Those facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the United Kingdom depends and which ensure the country continues to function socially and economically'.[6]

There is a compelling need to better understand, protect and maintain critical assets and information infrastructures against cyber threats, especially in a world where 80 per cent of private sector industries operate national assets as part of their core business. There is limited consumer and end-user understanding or technical skills to counter the growing cyber threats. In many cases in the corporate world, a weakness is clearly found where organisations have porous controls around intrusion detection and monitoring, incident response or computing forensics. Cyber issues can of course be as a result of internal and external sources to any organisation or system, requiring organisations to look within as well as to the exterior interface with the world at large.

As organisations look both internally and externally they are better able to create a robust cyber security posture to combat would-be attackers from whatever vector the attackers may originate.

An excellent example of a threat presented by an external source but accepted or introduced from an internal source is a successful spear phishing attempt. Recently (as of September 2013) the CPNI released new guidance to educate the public on this topic called 'Spear Phishing: Understanding the Threat'. The CPNI guidance explains Spear Phishing is 'a targeted form of email deception that results in exploitation or compromise of individual devices and organisational networks'.[8] The CPNI guidance explains how Spear Phishing attacks work, the likelihood of being targeted and the steps an organisation can take to manage the business risks. In addition the European Union Agency for Network and Information Security (ENISA) has identified and published the first and most comprehensive Cyber Threat Landscape analysis of 2012, summarising over 120 threat reports. The report lists the top ten threats identified by ENISA and their trends, and concludes that drive-by exploits in emerging technology areas have become the top web threat. The areas considered by ENISA when generating the list include mobile computing, social media/technology, critical infrastructure, trust infrastructures, cloud, and big data. The identified top ten threats mentioned above are:

1. Drive-by exploits (malicious code injects to exploit web browser vulnerabilities);
2. Worms/trojans;
3. Code injection attacks;
4. Exploit kits (ready to use software package to automate cybercrime);
5. Botnets (hijacked computers that are remotely controlled);
6. (Distributed) Denial of Service attacks (DDoS/DoS);
7. Phishing (fraud mails and websites);
8. Compromising confidential information (data breaches);
9. Rogueware/Scareware;
10. Spam[9].

The issue of cyber security is so relevant and topical for the British government it developed and published the National

Security Strategy in 2010, which essentially describes how — 'in an age of uncertainty — the UK needs the structures in place to allow it to react quickly and effectively to new and evolving threats to UK security'. The National Security Strategy identifies 15 priority risk types; one of the top four risks identified includes the need to safeguard against 'hostile attacks upon UK Cyber Space'[7] in line with national emergencies, such a serious pandemic flu outbreak(s).

The UK and the USA are responding to an ever-shifting landscape, and engineered and well-thought-out cyber attack capabilities. Organisations are waking up to the growing calls to stem the consequences of cyber-attacks, but they also need to make the right decisions and understand the trade-off between performance, cost and risk as a sustainable business model. Effective resilience requires an understanding and broader attunement to infrastructure assurance, within organisations and the future direction the organisation and its competitors and customers are moving toward. The modern organisation will need to be able to better anticipate and forecast cyber risks and vulnerabilities connected to new and emerging ICT trends, such as the explosion in smartphone usage, the shaping forces behind the digitisation of commerce and society, and connect this understanding to the security investments and planning of expenditures over asset life cycles.

In response to the rise in cyber threats, a new UK Government Communication Headquarters (GCHQ) Security Operations Centre was established in 2009 and declared in full operation as of March 2010. Its mission is to provide an opportunity for businesses and organisations to report instances of cyber-attacks with the intention of building a knowledge base from which to prevent future attacks. According to BBC reports of this open exchange between government and industry, 'this should give the government early-warning of cyber-attacks that could bring down critical national infrastructure. In return, the commercial sector can expect expertise on-tap'.[8]

In addition to GCHQ's Security Operations Centre, Francis Maude, Minister for the Cabinet Office, in March 2013 developed the new Cyber Information Sharing Partnership (CISP), previously called Project Auburn. CISP started in February 2011, when the Prime Minister met with the 'captains of industry' to discuss cyber security and attacks. Both industry and government agreed that faster situational awareness was required in light of the severity and rapidly increasing pace of cyber-attacks against UK interests and industry. At the CISP launch, Maude stated:

> 'We know that cyber-attacks are happening on an industrial scale and businesses are by far the biggest victims of cyber-crime in terms of industrial espionage and intellectual property theft with losses to the UK economy running into the billions of pounds annually'.[9]

The CISP will 'introduce a secure virtual 'collaboration environment', where government and industry partners can exchange information on threats and vulnerabilities in real time. The CISP will be complemented by a 'fusion cell', which will be supported on the government side by the Security Service, GCHQ and the National Crime Agency and by industry analysts from a variety of sectors. They will work together to produce an enhanced picture of cyber threats facing the UK for the benefit of all partners'.[9]

The CISP is being driven principally by the Centre for the Protection of National

Table 1: CPNI cyber security guidance aimed at organisations in the UK

Critical control 1	Inventory of authorised and unauthorised devices
Critical control 2	Inventory of authorised and unauthorised software
Critical control 3	Secure configurations for hardware and software
Critical control 4	Continuous vulnerability assessment and remediation
Critical control 5	Malware defences
Critical control 6	Application software security
Critical control 7	Wireless device control
Critical control 8	Data recovery capability
Critical control 9	Security skills assessment and appropriate training to fill gaps
Critical control 10	Secure configurations for network devices
Critical control 11	Limitation and control of network ports, protocols and services
Critical control 12	Controlled use of administrative privileges
Critical control 13	Boundary defence
Critical control 14	Maintenance, monitoring and analysis of security audit logs
Critical control 15	Controlled access based on the need to know
Critical control 16	Account monitoring and control
Critical control 17	Data loss prevention
Critical control 18	Incident response capability
Critical control 19	Secure network engineering
Critical control 20	Penetration tests and red team exercises

Infrastructure (CPNI), the Department for Business Innovation and Skills (BIS) and GCHQ. The Cyber Intelligence Fusion Cell will promote information sharing between industry sectors and enrich intelligence using multiple sources. The Fusion Cell will work closely with a number of partners from defence and finance sectors supported by a few UK government agencies with a stake in national cyber security.

The Fusion Cell will monitor cyberspace via a giant screen showing where in the UK cyber-attacks by foreign states and criminals are emerging. The information will be shared among up to 160 top British companies under the CISP. The Fusion Cell will comprise about ten officers from MI5, GCHQ and MI6, as well as handpicked specialists from some of Britain's biggest companies.[10]

The UK government is responding because cyber security is such a serious issue, where cyber-related fraud and intellectual property theft alone is estimated to cost the UK's economy £27bn per year. This mid-range financial estimate was identified by the UK government in 2011 and then represented a breakdown of £21bn of costs to businesses, £2.2bn to government and £3.1bn to citizens.[11] Similarly, a report by the US National Counterintelligence Executive has also described a persistent, widespread campaign by foreign nation states to steal intellectual property and trade secrets from US companies.

'Chinese actors', it found, 'are the world's most active and persistent perpetrators of economic espionage'.[3] A recent study conducted by Norton, an internet security company, estimates that, during a year, cybercrimes — including identity theft and online scams — cost the USA $140bn in cash and lost time. It found the $388bn global cost of cybercrime to be greater than the black market for marijuana, cocaine and heroin combined.[12] Although the finger has traditionally tended to point towards the Chinese government or rogue groups in China, the

scale of the problem is growing elsewhere in the world, with reports of rising cyber threats and capabilities emerging from India, the Middle East and Eastern Europe.

Mandiant, private security firm, the US recently identified the headquarters of Unit 61398, a People's Liberation Army grouping suspected of waging cyber warfare. The study revealed that 150 highly sophisticated cyber-attacks against targets in the USA had originated from inside. Unit 61398 looks like any other 12-storey tower on the outskirts of Shanghai's Pudong.[13] Governments are aware of a number of hacking hotspots around the globe, but are often reluctant to openly point the finger at countries, mainly for diplomatic and trade reasons.

Nonetheless, the hidden scale of cyber-related crime is enormous and growing significantly, especially where organisations are reluctant to discuss their status as a target by a stream of well-networked savvy opponents who can collectively pool ideas and design, customise and deploy increasingly cunning and resourceful methods through cyberspace. A drive for better digital literacy in children will bring both opportunities and threats to the future of cyberspace interactions. Educating the end user seems sensible, but the rate at which technology and software changes makes it hard to maintain.

ICT investments are increasingly driving the delivery and monitoring of critical infrastructure with networked apparatus and this leaves the door wide open to cyber-attacks, such as phishing, man in the middle browser attacks, malware, Trojans, worms, root-kits, distributed denial of service (DDoS) and increasingly evolved and well-planned no-notice attacks, such as 'zero day' attacks, one of the biggest emerging concerns.[14] In the face of such security challenges, organisations are scrambling to improve cyber incident management and intrusion detection and deploy plausible decoys such as honey nets and honey pots. Absolute reliance on the constant availability of CNI to fuel basic needs presents a serious and increasing challenge that requires better stakeholder coordination and improved understanding of this fast-moving, ill-defined problem.

The CPNI is one source that provides detailed public guidance aimed at advising organisations in the UK on how better to understand and manage their own current cyber security arrangements. The CPNI recommends a total of 20 specific controls (with sub-controls) spanning across various technical measures and activities,[15] with the primary goal of helping UK organisations prioritise their efforts to defend against the current most common and damaging computer and network attacks (see Table 1).

The need for clear guidance is most relevant where organisations are scrambling to improve their own cyber situational awareness. One crucial area not evident in the CPNI's 20 controls listed in Table 1 (and seldom in the minds of many company executives) is the need for integrated business continuity arrangements, specifically addressing the resilience and backup arrangements for critical ICT infrastructure and information resources. This is especially important if critical ICT systems are compromised and taken offline by a determined attacker. Clearly, conducting a business impact analysis as part of a continuity process should add value to cyber priorities by informing on 'defined criticality' and 'recovery times' for any organisation's critical infrastructure. Further to the above, linking cyber resilience into the organisation's (and its critical suppliers and contractors) policies and strategic risk registers will place the issue at the heart of governance procedures and firmly across a broad range of stakeholder agendas.

In addition to the guidance to industry

from the CPNI, the British government is also behind the Communications Electronic Security Group (CESG) Cyber Incident Response Scheme, launched in November 2012, which provides access to companies certified to respond to the consequences of cyber-attacks. This scheme builds upon the Cabinet Office '10 Steps to Cyber Security', which was launched in September 2012. It is aimed at business leaders, describing the cyber security threat and providing advice on the basic measures to increase cyber security within their organisations. CESG's aim is to 'protect the vital interests of the UK by providing policy and assistance on the security of communications and electronic data, working in partnership with industry and academia'.[16]

As hacking and cyber-attacks against the defence sector are particularly concerning, the UK government has established the Defence Cyber Protection Partnership (DCPP). The DCPP aims to meet the emerging threat to the UK defence supply chain by increasing awareness of cyber risks, sharing threat intelligence and defining risk-driven approaches to applying cyber security standards. The DCPP currently partners the CPNI, GCHQ, the Ministry of Defence and nine companies: BAE Systems, BT, Cassidian, CGI, Hewlett Packard, Lockheed Martin, Rolls-Royce, Selex ES and Thales UK.[17]

Lessons from cyber attacks

From the serious attacks on the Estonian government network, it is already known that disruption to national infrastructure and vital resources can have a profound and cascading impact, seriously challenging essential and basic public services. Maintaining the safe and efficient use of internet-enabled and networked services such as communications, energy, finance, food, government, health, transport and water supplies presents governments and stakeholders with a stark challenge in the face of increasing levels of sophisticated cyber-attackers and hackers. For the most part, CNI is tightly coupled and connected, with little or no slack (designated redundancy), and it is spread across complex geo-spatial and multi-dimensional boundaries with critical node points or hierarchical controlling systems, such as SCADA systems, across the UK. The threats posed to national interests has brought together stakeholders such as the Metropolitan Police, GCHQ, CPNI and the Cabinet Office to ensure cyber initiatives are coordinated in line with national risk assessments and the National Risk Register.

THE US APPROACH TO CYBER SECURITY

After the 2007 DDOS on Estonia and other cyber-attacks that followed, it was clear that action was needed to secure the USA's critical infrastructure against cyber-attack. In January 2008, President Bush signed the National Security Presidential Directive 54/ Homeland Security Presidential Directive 23, Comprehensive National Cybersecurity Initiative (CNCI), which was initially classified until March 2010, when President Barack Obama released public information about CNCI and its main recommendations. 'President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter'.[18] President Obama used CNCI as part of an in-depth cyberspace policy review that he commissioned to assess US readiness to withstand cyber attacks. When the review had concluded, President Obama reviewed the results and released a plan using the CNCI goals to secure the USA digital infrastructure.

CNCI's main goals are as follows:

- To establish a frontline of defence against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats and events within the federal government — and ultimately with state, local and tribal governments and private sector partners — and the ability to act quickly to reduce current vulnerabilities and prevent intrusions.[18]
- To defend against the full spectrum of threats by enhancing US counterintelligence capabilities and increasing the security of the supply chain for important information technologies.[18]
- To strengthen the future cyber security environment by expanding cyber education, coordinating and redirecting research and development efforts across the federal government and working to define and develop strategies to deter hostile or malicious activity in cyberspace.[18]

In addition to CNCI, the US government has recognised the cyber threat to national security by creating USCYBERCOM, which was mentioned briefly earlier. Through USCYBERCOM, the USA is fighting cyber terrorism, both in the public (US military) and private (home and business) sectors.

The US government also recognises that emergency response and readiness teams are needed to assist when an attack takes place, or in advance of it to stop or mitigate the potential effects of the attack. As such, the US Computer Emergency Readiness Team (USCERT) maintains a website to help the less technical savvy as well as expert information technology professionals. 'USCERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans'.[19] USCERT provides users with specific instructions on how to protect their computer systems and networks from attack by making readers aware of the newest software patches available to protect information systems that access the internet. In addition, USCERT provides a large library of articles and discussions on cyber security-related content to educate readers on the newest threats and related trends and how to defend against them. The organisation also gives users helpful tips offering best practices and advice on security issues of interest to the general public. Its last and likely most recognised role is to provide security alerts and vulnerability bulletins, also providing viewers with the links to download patches to mitigate vulnerabilities.

While USCERT, USCYBERCOM and CNCI have been in existence for a few years, the job of cyber security is far from finished. President Barack Obama recently signed a presidental executive order requiring the USA to step up its cyber security to improve its resilience against attacks on critical infrastructure. The Improving Critical Infrastructure Cybersecurity Executive Order (EO) was signed on 12th February, 2013. 'The EO tasks the National Institute of Standards and Technology (NIST), within the Department of Commerce, to develop a baseline Cybersecurity Framework that sector-specific agencies would rely upon to establish a voluntary critical infrastructure cybersecurity program'.[20]

Cyber threats: Weapons of mass disruption

The modern computer virus is rapidly evolving and becoming capable of causing massive disruption to critical infrastructure and vital resources. Project Aurora in the USA was a controlled demonstration on

how a virtual breach could afford control over a critical industrial control system. The system was tampered with in such a way that it caused rapid physical malfunction and failure to occur despite fairly robust security measures being in place. The fear is that a sustained and well-targeted campaign of cyber-attacks could easily cause mass disruption to daily functioning across government industry and commerce (as occurred in Estonia to a smaller degree).

Table 2: The 16 CIKR sectors in the USA

Chemical sector
Communications sector
Dams sector
Emergency services sector
Financial services sector
Government facilities sector
Information technology sector
Transportation systems sector
Commercial facilities sector
Critical manufacturing sector
Defence industrial base sector
Energy sector
Food and agriculture sector
Healthcare and public health sector
Nuclear reactors, materials and waste sector
Water and wastewater systems sector

The impact of the Stuxnet virus on industrial control systems

Maintaining effective cyber security capabilities in complex distributed infrastructures requires extended vigilance and situational awareness in a changing cyber landscape. Stuxnet introduced a need to change the way that organisations and anti-virus providers managed threats from cyberspace. Stuxnet had a very effective strategy for the covert monitoring of specific targeted facilities. 'The United States of America, Department of Homeland Security said that this "highly complex" computer worm was the "first of its kind". Stuxnet's potential to damage CNI caused "worldwide alarm", according to the *Financial Times*, and has been called a "paradigm shift" by the European Network and Information Security Agency'.[21] Stuxnet deployed a sophisticated code that had an intelligent control interface allowing for extensive and refined damage capabilities in networked components. Iran was reportedly the intended target due to its own controversial nuclear development programme. Symantec Corporation stated that 'the Iranian organisations were involved in "normal" industrial projects. These conclusions are based on intercepted data that Stuxnet transmitted to its command and control server'.[21] Analysts suggest that Stuxnet was specifically designed to target the reliability of Siemens components, controlling the rate at which nuclear centrifuges could safely spin in Iranian nuclear plants. 'Tehran confirmed in September 2010 that Stuxnet had infected about 30,000 IP addresses in Iran. The high infection rate increases the probability that Iranian centrifuge facilities may have been affected, but is not in itself proof that they were'.[21]

The impact of the Flame virus on critical information infrastructure

Flame was detected in May 2012 and it was believed to essentially exhibit cyber-espionage capabilities. The virus was believed to have been around for two years prior to its discovery. The Middle East including Israel, Syria and Iran became particularly vulnerable. Flame had the ability to remotely control and pass information from webcams; it could take and remotely send screenshots from infected computers; and control microphones, switching them on and off as required in any infected computing devices. In addition to webcam control, it

Table 3: The nine CNI sectors in the UK

Communications
Emergency services
Energy
Financial services
Food
Government
Health
Transport
Water

could also record all network connections on the infected machine, gather basic systems data, search and steal files based on name or contextual window searches and it scan for and use locally connected Bluetooth devices. Flame allegedly had 20 times the code of Stuxnet according to Russian anti-virus provider, Kaspersky.

The United Nations' International, The International Telecommunications Union of the United Nations said:

> 'Flame is a suite of tools for professional cyber-espionage. It is an example of powerful cyber weapons that are a rising international problem. People's lives could be seriously affected by such weapons if personal data is stolen, or if critical infrastructure is threatened through connections to the Internet'.[22]

The threats are getting worse each day so the defences must keep pace with them by constant virus definition updates and patches. This is why keeping on top of vulnerability patching of personal and business computers and devices should be top on every internet user's mind. Cyber threats exist because there is a time gap between recognising the changing nature of the threat landscape and concerted action to limit the impacts of a potential targeted attack.

CLASSIFICATION OF CNI IN THE USA AND UK

Both the USA and UK face similar cyber threats at home and from foreign sources. There are, however, some crucial differences observed around what is considered critical infrastructure and, secondly, which agencies at a national level have an active responsibility for nationwide cyber security. Much of these differences are reflected in the legal processes and structural design and functioning of each country's own government.

In 2008, the US Department of Homeland Security identified 17 critical infrastructure and key resources (CIKR) sectors. These CIKR sectors were recognised under the US National Infrastructure Protection Plan and CIKR sectors were mapped against 15 existing US emergency support functions.[23]

Since 2008, the Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience has advanced to include a national policy to strengthen and maintain secure, functioning and resilient critical infrastructure. This directive now supersedes the pre-existing Homeland Security Presidential Directive 7. PPD-21 now identifies 16 critical infrastructure sectors, as shown in Table 2.[24]

The UK addresses the scope of critical infrastructure and applies a different approach (although there is much overlap) to the USA. In essence, the UK's national infrastructure is currently categorised into only nine sectors by the CPNI (see Table 3).

There are some cross-sector themes such as technology wherein infrastructure may support the delivery of essential services across a number of sectors.

The National Cyber Security Strategy Cabinet Office has four main strategic objectives:

- making the UK one of the most secure

places in the world to do business in cyberspace;
- making the UK more resilient to cyber-attack and better able to protect its interests in cyberspace;
- helping shape an open, vibrant and stable cyberspace that supports open societies;
- building the UK's cyber security knowledge, skills and capability.

A significant proportion of funding (£650m over five years) has already been given to organisations such as GCHQ by the British government to improve the detection of cyber-attacks on the UK's interests. The funding will help transform the UK's situational awareness in cyberspace. A series of investments will see GCHQ and partners further increase the ability to respond to a diversified range of cyber threats and to protect the UK's national and economic security interests.[25]

The US approach has been similar to using agencies such as GCHQ to begin to confront cyber-related challenges. The National Security Agency and the Department of Homeland Security work very closely together to fight cyber-attacks, especially when they are directed toward those critical infrastructure areas defined in PPD-21 and other related legislation. Presidents George Bush and Barack Obama have placed a high priority on securing cyberspace so it is safe for all Americans and world users. Every year, for the past three years, some form of cyber security bill has been introduced and every year for the past three years civil liberties organisations such as the American Civil Liberties Union and the Electronic Frontier Foundation have fought hard for privacy.[26]

More recently in the USA, a legislative bill known as the Cybersecurity Act 2012 was introduced by Senators Joseph Lieberman (ICT) and Susan Collins (RME). This legislation would have allowed for better critical infrastructure protection, but at the cost of privacy rights. The bill, if passed, would have allowed for collection and monitoring any electronic transmission that contained certain keywords that would appear to be planning to cause harm to the USA's critical infrastructure. The proposed Cybersecurity Act 2012 was defeated in the US Senate. There were serious concerns about public privacy rights and it was felt by some detractors to be too restrictive and burdensome on businesses. The proposed act would have allowed private corporations to voluntarily share suspicious online activities with the intelligence and law enforcement communities. Despite the Cybersecurity Act 2012 not being passed into law and to ensure that the critical infrastructures were still protected from cyber-attack, in February 2013, President Obama signed an executive order titled Improving Critical Infrastructure Cybersecurity. It appears the debate on cyber security will continue as the rate of cyber intrusion, disruption, espionage and destructive attacks will increase worldwide.

The release of sensitive information about the National Security Agency's clandestine mass surveillance programme called 'PRISM' has added another dimension to cyber security protection measure discussions and divided public opinion about electronic surveillance and the security of cyberspace. The release of restricted information by Edward Snowden to the *Washington Post* and *Guardian* newspapers has caused great debate about civil rights, checks and balances and approaches used by the US and UK intelligence communities in pursuit of keeping their own citizens safe from harm. The dimensions of cyber security, and who is sourcing information on whom, will become far more complex and interesting as time goes by, as

will the way US and UK government leaders balance personal liberties and human rights with national security.

CONCLUSION

This paper has identified how critical infrastructure is pivotal to the smooth running of daily life. As everyone continues to become more dependent on critical infrastructure in a growing cyber-enabled era, the threats and vulnerabilities are likely to grow and change faster than people can perhaps appreciate or collectively respond. The nature of surveillance for national security is also likely to stray into the debate with civil libertarians.

The perpetrators behind foreign cyber-attacks are not always easy to determine and the motives behind attacks can vary significantly. As attack surfaces (eg via mobile-enabled devices such as 'bring your own device') change, there is a continued requirement for much better situational awareness and planning at all levels, ranging from home PC users to corporate enterprises. The nature of the threats ranging from disruptive, criminal and destructive cyber-attacks requires greater research and cooperation between industry, commerce, infrastructure owners, infrastructure operators and government(s). This process of partnership has begun to take shape in the UK and USA with developments such as the USA's Comprehensive National Cybersecurity Initiative (CSCI) and the UK's Cyber Information Sharing Partnership (CISP) at nationally coordinated levels.

The approaches and methods used to manage cyber threats at a national level in the UK and USA differ most notably in defining the scope of each country's respective CNI sectors. Government agencies in both the USA and UK have acknowledged the issues concerning cyber threats, but there is still much more work to be done and the success of any strategy is dependent upon applying effective foresight and controls based on understanding the landscape of cyber and future developments.

Additionally, when comparing the UK and US approaches, it is evident that both countries recognise that their critical infrastructure is vulnerable and that the government must assist in protecting against cyber-attacks. Both countries recognise that standards are needed to help businesses and organisations to adapt their processes to accommodate a security posture that would better protect them from cyber-attacks. Legislation is another option (such as the recent failed Cyber Security Bill 2012), but this is not without considerable opposition emanating most notably from civil liberties groups. It is possible that the capabilities of a defensive posture against aggressive cyber-attacks will move towards a more offensive posture involving attacking the adversary under clear standing orders, being empowered to execute those orders immediately upon discovery of the threat or in anticipation of it, thereby making the strategy more effectively aligned to cyber warfare than cyber resilience. It is also clear that most nations engage in some form of heightened surveillance and cyber espionage, whether they admit it or not.

References

(1) Dunn, J. (2013) Tech World (Internet) 'Barclays Bank KVM attack plotted by UK cybercrime's "Mr Big", claim police', available at: http://news.techworld.com/security/3470224/barclays-bank-kvm-attack-plotted-by-uk-cybercrimes-mr-big-claim-police/, (accessed 31 March, 2014)

(2) Williams, M. G. B. T. (2013) 'Armed Forces Communication and Electronics Association (AFCEA) Conference Proceedings from the 4th Annual Cyber Security Symposium', Cybersecurity Symposium 2013, Washington DC.

(3) Garamone, J. (2012) 'Panetta Spells Out DOD Roles in Cyberdefense', American Forces Press Service, available at: http://www.defense.gov/news/newsarticle.aspx?id=118187 (accessed 17th May, 2013).
(4) United States of America National Senate, Democratic Policy and Communications Centre (2012) 'Myth vs. Fact: The Cybersecurity Act of 2012', available at: http://www.dpc.senate.gov/docs/fs-112-2-179.pdf (accessed 17th May, 2013).
(5) Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., et al. (2009) 'Internet of things strategic research roadmap', Internet of Things: Global Technological and Societal Trends, p. 9.
(6) Higginbotham, S. (2013) 'CES 2013: Connected devices and the Internet of Things,' *Bloomberg Businessweek Technology*, 3rd January.
(7) Centre for the Protection of National Infrastructure, UK Government (2013) 'The National Infrastructure', available at: http://www.cpni.gov.uk/about/cni/ (accessed 17th May, 2013).
(8) Centre for the Protection of National Infrastructure UK Government (2013) 'Spear Phishing', available at: http://www.cpni.gov.uk/documents/publications/2013/2013053-spear-phishing-understanding-the-threat.pdf?epslanguage=en-gb (accessed 25th September, 2013).
(9) European Union Agency for Network and Information Security (2013) 'New report on top trends in the first Cyber Threat Landscape by EU's cyber Agency ENISA', available from: http://www.enisa.europa.eu/media/press-releases/new-report-on-top-trends-in-the-first-cyber-threat-landscape-by-eu2019s-cyber-agency-enisa (accessed 25th September, 2013).
(10) Gov.UK (2013) 'Inside Government. The national security strategy — a strong Britain in an age of uncertainty', available at: https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty (accessed 25th July, 2013).
(11) Watts, S. (2011) 'Proposal for cyber war rules of engagement', available at: http://news.bbc.co.uk/1/hi/programmes/newsnight/9386445.stm (accessed 5th March, 2013).
(12) Gov.UK (2013) 'Inside Government. Government launches information sharing partnership on cyber security', available at: https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security (accessed 25th July, 2013).
(13) Sky News (2013) 'Cyber Threat: Spies and Big Firms Join Forces', available at: http://news.sky.com/story/1070111/cyber-threat-spies-and-big-firms-join-forces (accessed 25th July, 2013).
(14) BBC News (2011) 'UK cybercrime costs £27bn a year', available at: http://www.bbc.co.uk/news/uk-politics-12492309 (accessed 17th May, 2013).
(15) Symantec Corp. (2011) 'Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually', Press Release, available at: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (accessed 17th May, 2013).
(16) Harris, P. (2013) 'Chinese army hackers are the tip of the cyber warfare iceberg', available at: http://www.guardian.co.uk/technology/2013/feb/23/mandiant-unit-61398-china-hacking (accessed 25th July, 2013).
(17) Ponemon Institute (2012) 'A Study of Retail Banks & DDoS Attacks Report', available at: http://www.corero.com/resources/files/analyst-reports/CNS_Report_Ponemon_Jan13.pdf (accessed 17th May, 2013).
(18) Centre for the Protection of National Infrastructure, UK Government (2013) 'Top 20 critical security controls for cyber defence', available at: http://www.cpni.gov.uk/advice/cyber/Critical-controls/ (accessed 17th May, 2013).

(19) CESG (2013) 'The National Technical Authority for Information Assurance', available at: http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx (accessed 25th July, 2013).
(20) Gov.UK (2013) 'Inside Government. Defence Partnership tackles cyber security risks', available at: https://www.gov.uk/government/news/defence-partnership-tackles-cyber-security-risks (accessed 25th July, 2013).
(21) National Security Council, US Government (2009) 'The Comprehensive National Cybersecurity Initiative', available at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 17th May, 2013).
(22) US-CERT (2013) 'United States Computer Emergency Readiness Team', available at: http://www.us-cert.gov/ (accessed 3rd April, 2013).
(23) Daubert, T. D., Roth, A., Bertoson, T. R. and Blair, A. (2013) 'United States: President Obama's Cybersecurity Executive Order to Impact a Wide Range of Business and Industry', available at: http://www.mondaq.com/unitedstates/x/222598/Data+Protection+Privacy/President+Obamas+Cybersecurity+Executive+Order+To+Impact+A+Wide+Range+Of+Business+And+Industry (accessed 3rd April, 2013).
(24) Barzashka, I. (2013) 'Are cyber-weapons effective?', *RUSI Journal*, Vol. 158, No. 2, pp. 48–56.
(25) International Telecommunications Union of the United Nations (2012) 'FAQs on FLAME', available at: http://www.itu.int/cybersecurity/Articles/FAQs_on_FLAME.pdf (accessed 17th May, 2013).
(26) Federal Emergency Management Agency (2008) 'Critical Infrastructure and Key Resources Support Annex', available at: http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf (accessed 17th May, 2013).
(27) Department of Homeland Security (2013) 'Critical Infrastructure Sectors', available at: http://www.dhs.gov/critical-infrastructure-sectors (accessed 17th May, 2013).
(28) Cabinet Office, UK Government (2012) 'The UK Cyber Security Strategy: Report on progress — Forward Plans', available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83757/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf (accessed 17th May, 2013).
(29) Jaycox, M. M. (2012) 'The Cybersecurity Act was a surveillance bill in disguise', available at: http://www.guardian.co.uk/commentisfree/2012/aug/02/cybersecurity-act-surveillance-bill-disguise (accessed 17th May, 2013).