Weapons of '*Maths*' Destruction:
Cybercrime, Cyberwarfare and Cyberdefence

How cybertechnology is defining our national and economic security.

1000100010101000110000001**EDWARD**0001000010000100010001
100010111110000**CHRISTIE**000010000100001000000001000010000
0010000001000000000100000000100000000001111110000001100000
00000111101110011111100000111**GOWNBOYS**0000100001000111
1110111000100101001100001000010000100000010100000011110
10110001000011**SUPERVISOR:DL**0010100010000001000001110000
0001011010001111100001110000000111000100000111110000001
0101110000111100100011111100000**SEPTEMBER2015**1100000000

Weapons of 'Maths' Destruction: Cybercrime, Cyberwarfare and Cyberdefence

Introduction:

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property." *President Obama*[1]

There are many examples that could be cited to defend this view, including recent attacks on the US defence aircraft design suppliers by China, Sony's corporate networks by Korea, retail and energy utility attacks by China, and financial institutions including JP Morgan by Russia.[2] This is not however a problem localised to the US. It is a global issue and widely regarded as one of the top three and increasingly the top one issue for governments and institutions to address.

It is however a very technical and complex issue to address which requires solutions from a unique combination of hard science (mathematicians, computer, data and behavioural scientists, and technical strategists) as well as soft science (economic, political and legislative policy experts).

The global economic cost of cybercrime is hard to measure but is estimated at over £260 billion, which some consider to be a significant underestimate although all agree that the number is unacceptably high and the trend is expected to continue to rise. The cost to the UK economy alone is estimated to be £20 billion per annum. There is also a high opportunity cost as it is estimated that the cost to institutions to defend against the losses being even higher is at least £300 billion.[3]

The economic cost of cyberwarfare could be unlimited.

This is however only part of the story. Governments and institutions are also actively looking at building '*offensive'* as well as '*defensive'* cyberstrategies. In August 2015, the UK Government announced plans to invest in a £2bn cyberspace military offensive capability, ten times the previous level of investment. The US has committed ten times this amount for many years, which is still dwarfed by the sums spent by China.[4]

Despite significant investment, governments and institutions are still unclear what the nature of the threats are, what tools and techniques to deploy to mitigate attacks, how to enforce measures of legislative action, and how to

[1] White House Policy Paper : Cybersecurity (Order Number 20)

[2] Heritage Foundation: Cyber Attacks on US Companies – Riley Walters 2014

[3] Symantec Research, McAfee Research 2014

[4] Sunday Times: 16/08/15 (Military Strategy Briefing) & Times 17/08/15

proactively identify and target strategies against the different types of *'cyberactivists'*.

This paper explores these issues in detail, outlining some of the methods used in cyberattacks and the potential countermeasures that could be adopted to mitigate against those attacks. To illustrate potential countermeasures, a case study of the financial industry is discussed as this has been one of the main targets of attack and despite being highlighted as one of the most secure areas of cyberspace, is still extremely vulnerable.[5]

The New Arms Race

Traditional warfare has often been determined by force. Military strategists use the term 'kinetic' which highlights the nature of the approach, notably combat. Outcomes are based on the successful deployment of force to overwhelm the opposing enemy. This has lead historically to what has been termed an 'arms race', which is defined as "the participation of two or more nation-states in apparently competitive or interactive increases in quantity or quality of war material and/or persons under arms".[6]

Examples of arms races are not new and have included nations' increase in naval forces, nuclear weapons, and biological weaponry. The escalation of the races have lead to the need for nations to agree treaties to control the levels of weapons, often driven as much by economic as political expediency.

These weapons were deployed in four domains: air, land, water and space. The key architects of the innovation were physicists, chemists and engineers. There are a number of characteristics of traditional weaponry, namely:

1. They are destructive to both parties warfare 'material' – including manpower, infrastructure, weaponry and natural resources.
2. They are blunt in application, and may frequently involve collateral damage or unintended consequences.
3. They are expensive to maintain, and require constant innovation to maintain supremacy.
4. They are generally bilateral, in that there is a high likelihood of retaliatory action and damage on both sides.
5. They are attributable, which means that it is generally easy to identify the identity, nature and capability of the attacker.
6. They are limited in scale and potentially slow to deploy, requiring physical proximity and localised intelligence.

Military strategists still tend to focus on kinetic supremacy, although the nature of this technology is evolving to reduce the dependency on humans in the chain of command and deployment. This is proving to have a number of ethical issues

[5] Cyberwar: Richard Clarke – Harvard University

[6] Arms Race : Alex Upton (Wikipedia)

raised, for example in the deployment of drones. Systematic analysis of conflict which focuses on the causes of war and conditions of peace conclude that the build up of traditional weapons by a nation is based “proportionally to the level of armaments of its’ rival and its’ level of grievance to that rival, and inversely proportional to its’ own level of armaments”.[7]

Modern warfare has however highlighted a fifth domain of military deployment, cyber, as an area of strategic importance. [8] Cyberwarfare is defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”.[9]

There is therefore a need for a *new* arms race to gain supremacy in the cyber domain, generally termed cyberspace. This race has a number of differences to the traditional arms race, namely:

1. It is extremely difficult to measure, monitor or control the capability of a rival’s *‘armaments’*.
2. It is asymmetrical, meaning that the force could be applied without the ability to counterattack.
3. It is precise, meaning that attacks can be designed to be targeted very accurately at for example a nations’ banks, energy supplies, military equipment, defences, hospitals, communications.
4. It does not require destruction of a nations’ physical assets or military ‘material’ to be effective.
5. It is potentially untraceable and unattributable.
6. It is relatively cheap to deploy, can be deployed at scale, and can also be pre-emptively designed years in advance of a planned attack.
7. It is ‘virtual’[10] and does not require significant physical resources, such as enriched uranium, which means a potentially level battlefield for all nations.
8. It is constantly evolving. New methods of attack and counterattack are constantly being designed, and the ‘innovation process’ is often in the hands of groups of individuals rather than large military ‘engines’.

The primary architects of the *new* arms race are mathematicians and computer scientists. Mathematics has taken over from physics as the enabler of the next generation of military weapons in their design and deployment. The latter part of the 20th century became obsessed with the reality or otherwise of ‘Weapons of *Mass* Destruction’.[11] The early part of the 21st century is now focused on the reality and potential danger of ‘Weapons of *Maths* Destruction’.

[7] Military Conflict Analysis: Lewis Fry Richardson (Wikipedia)

[8] Cyberwar: The Economist – 1 July 2010

[9] Cyberwar : Richard Clarke

[10] Defined as operating within a computer architecture rather than physical architecture - EC

[11] Numerous references since 1937 up to Iraq War – Weapons of Mass Destruction (Wikipedia)

There is however a bigger problem associated with *cyber* compared to *traditional* warfare. It doesn't just involve nation-states, but also other organizations, such as terrorist groups, companies, political or ideological extremist groups, 'hacktivists', who subversively use computers to promote a political agenda, and transnational criminal organisations. It is also not defined by geographic boundaries or national identities.

Furthermore, the identity and objectives of these cyberactivists are not always apparent, and it is easy to masquerade as each other.

The Cyberspace Battlefield

So what is cyberspace and why has it become an important battlefield?

The answer to that is easy. To adapt a phrase from Douglas Adams, "*Cyber*space is big. You won't believe how incredibly, mind bogglingly big it is"[12]. Furthermore, it is everywhere. Cyberspace is defined by the architecture of all our computer based technology: our computer programs and operating systems, the physical technical infrastructure, and the data stored on all of the computers. This technology is embedded in all of the personal, commercial, national and international infrastructure that we use. Our healthcare systems, banking systems, tax and central government systems, defence systems, communication systems, transport systems, entertainment systems, for example, all rely upon computer technologies.

In essence, cyberspace is <u>our</u> global computer '*macro*-network' which consists of '*micro*-networks' of internets and intranets[13]. Each of these networks consist of connected devices that can share data and perform computational applications. There are currently two trends in cyberspace that are defining the evolution of these networks, 'big data' and the 'Internet of Things'.

Big data refers to the trend in a massive increase in available data stored on these networks, which is growing at an estimated 60% per annum. 90% of the data that exists in the world today has been created in the last two years.[14] This data is both structured and unstructured and enables complex analysis to be performed on this data to reveal details about us, our governments and institutions that would not have been available historically. As this data gets applied in more complex and mission critical applications, the quality and security of this data will become more important. There is also more of it for criminals to mine and exploit, to design new and novel ways to attack.

[12] Douglas Adams: Hitchhikers Guide to the Galaxy

[13] Internet is defined as a network that is openly accessible externally. Intranets are closed internal networks, which may though be connected to internets via a secure authentication gateway.

[14] IDC Big Data Survey; SAS Analytics Big Data Research

The '*Internet of Things'* adds a second dimension to the evolution and importance of cyberspace. Cyberspace is getting even bigger as more and more devices are being added to the macro-network, ranging in such diverse applications as, for example, healthcare fitness bands, our televisions, fridges, car GPS monitors, and smartphones. Sensors and additional computer managed devices are being added at an exponential rate, so fast indeed that the internet needs to be redesigned to support the volume of new devices being added.[15]

The consequence of this trend is that the potential areas of attack have already proven to have penetrated into nearly every device and mission critical systems, from our cars' safety systems[16], bank accounts[17], airline defences[18], health records[19], logistics[20], food chain through to our national security. We are heavily reliant on the security, resilience and integrity of the macro-internet to safeguard modern society.

But contrary to popular belief, the internet is extremely vulnerable to attack.

There are at least five key areas of weaknesses that could be exploited[21], namely:

1. The Addressing System

Every device or web page attached to the internet has a unique 32-bit numeric based address to identify it. These are generally presented in human readable format as, for example, '180.14.196.1'. In practice, these are difficult to remember and therefore the internet was designed to enable users to associate more user friendly 'domain names' to map to these numbers, which is achieved by a mapping table called the *Domain Name System* (DNS).

When a user logs onto a web page, say his home page (eg. www.edwardc.com), the browser sends a message to the DNS to look up the unique address for that page. The DNS was not however designed with security included as it was intended to be a scalable, distributed system.[22] Whilst there are attempts to add security, it is possible for hackers to change the information in the DNS and redirect users to phony websites or affected devices. The security firm, Kapersky, released software that demonstrated the ease of attacking the DNS.

It is also possible to bombard the DNS to prevent it being able to operate efficiently, thereby bringing the internet to an effective stop. This is the basis of what is termed Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.

[15] Cisco & SAS Research Papers

[16] Tesla hacked (China 2014); Jeep Cherokee (July 2015)

[17] Barclays loses £1.3 million by cyberattacks – Sep 2013

[18] Chinese government accused of hacking into civilian aircraft by US Senate – Sep 2014

[19] Anthem healthcare insurance records hacked – Feb 2015

[20] Inventory scanners used by China to hack shipping and logistics firms – TrapX - Sep 14

[21] Cyber war – Richard Clarke

[22] Domain Name System Security Extensions - Wikipedia

2. The Connectivity Routing

Internet traffic is carried by Internet Service Providers (ISPs) in packets or blocks of data that carry labels such as 'to' and 'from'. There are multiple tiers of quality of providers and the security associated with each provider can vary. Typically an internet traffic journey can involve multiple ISPs, which requires a central router to manage the traffic across the internet. This is performed by a system called the Border Gateway Protocol (BGP). The BGP is the sorting station that determines where information packets should be sent.

BGP however is also a system that was not designed with security in mind and relies on trust, and information from ISPs on the addresses and routes that relate to it. This introduces a significant opportunity for hackers to redirect these packets to other sites and create significant disruption to the internet.

3. Open Access

The third key vulnerability is that most of the internet has been designed to be open, accessible and is mostly unencrypted. If a hacker 'snoops' in to internet traffic, it is possible to read all of the data packets on the internet. This could include password or instruction codes associated with applications or data. There are a number of snoop technologies readily available on the market, known as sniffers, and the internet has numerous companies who are available to train and configure these.[23] Many of these sniffers operate in real time and provide advanced visualisation methods to be able to process vast quantities of internet traffic data. Examples include:

Top 10 Sniffers for Hackers
Wireshark
TCPDump
Cain & Abel
Kismet
DSniff
NetStumbler
Ettercap
Ngrep
NTop
EtherApe

Whilst there have been attempts to improve the security of internet usage, due to the need for speed and cost efficiency, many sites only encrypt for initial authentication and then revert to an unencrypted web version. This introduces additional vulnerability as users can often be under the impression that the sites that they are using are more secure than they really are.

[23] Infosec institute publish a league table of the best tools available: Internet Geeks Reference

4. Propagation Efficiency

The internet is not designed to audit the contents or the intent of internet traffic. In part this is because of cost and the concern that an ISP will be seen to be too slow. ISPs frequently compete on performance speeds and therefore there is a disincentive to increase the associated security controls within the operating model of an ISP.

Hackers exploit this business and technical model weakness. It is therefore possible to rapidly transmit intentionally malicious traffic across the internet. This is known as malware, which includes the design of viruses that replicate from computer to computer, or worms that are not replicated but move across the networks attached to the internet based on vulnerabilities in the network security, with a specific malicious intent. Examples of malware include emails with embedded viruses or worms, known as *phishing*, phone call attacks to get personal information such as passwords, known as *vishing*, or virus attacks on mobile phone text systems, known as *smishing*.

5. Network Decentralisation

The internet is a single network, albeit with complex sub-networks, that is architected to be a decentralised design. There was a greater emphasis on ensuring that the decentralised design was not under the control of a single or collective authority, than there was on security. The original design of the internet was based on an assumption that there would be relatively few computers connected to the internet, new connections were from trusted and verified sources and encryption of the data links between computers was all that was needed.

With the internet rapidly running out of addresses[24], the original design principles are clearly being challenged. The function and nature of the internet is dramatically different from the original vision and the security weaknesses, lack of transparency, and technical complexity require attention.

Evidence of Attack

The vulnerabilities above are clearly worrying as is the ease by which tools can be located ‘on the internet’ to ‘attack the internet’. There is significant evidence of cyberattacks for espionage, financial crime, and sabotage purposes. Some examples of the extent of the attacks include:

- In December 2006, NASA’s cyberdefences were infiltrated by an unknown source. The hackers were looking for information on the propulsion and radio systems onboard their rockets, which could be used for both commercial and military gain.

[24] Currently over 4.3 billion addresses in use and a new standard for numbering is being introduced (iPV6)

- In April 2007, Estonia came under cyber attack in the wake of relocation of the Bronze Soldier of Tallinn. The largest part of the attacks were coming from Russia and from official servers of the authorities of Russia. In the attack, ministries, banks, and media were targeted.

- In 2010, the infamous Stuxnet worm was discovered which targeted the controllers associated with Iran's nuclear enrichment plant, Natanz. This was a very sophisticated worm that looked for specific industrial programmable logic controllers that it could then take over to destroy the plant and over-ride the monitoring and fail-safe systems.

- In November 2010, a group calling itself the Indian Cyber Army hacked into Pakistan's government sites as revenge against the Mumbai attacks. In retribution, on 4 December 2010, a group calling itself the *Pakistan Cyber Army* hacked the website of India's top investigating agency, the Central Bureau of Investigation.

- In May 2014, the personal records of 233 million ebay users were hacked including the information on the users physical addresses and identities. Responsibility was claimed by the Syrian Electronic Army.

- In July 2014, the health and financial records of 1.3 million US citizens were stolen.

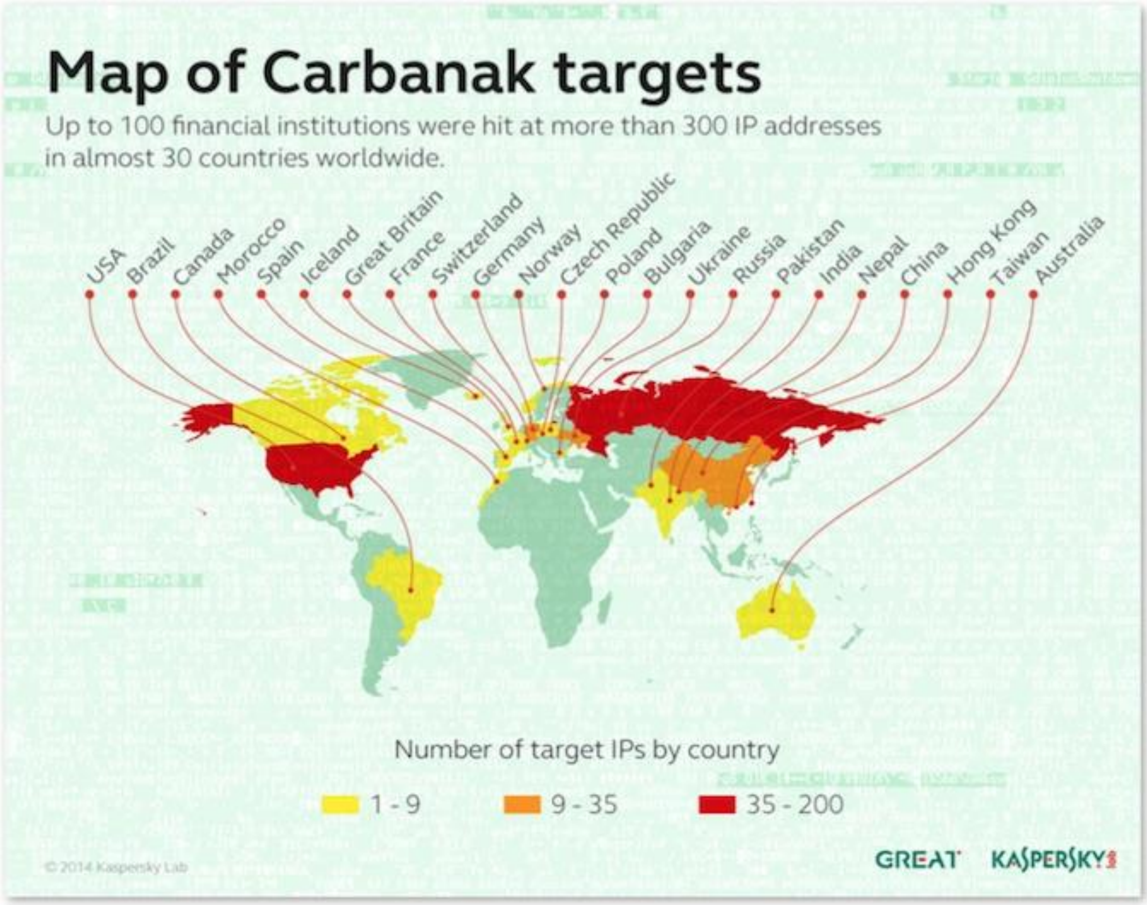
- In June 2014, the news aggregation website, Evernote, was taken out of business by a Distributed Denial of Service (DDoS) attack, and held to ransom to restore service.

- In February 2015, US National Intelligence Director blamed Iran for a cyber attack on Sands Casino in Las Vegas that stole confidential data and shut down many of the casino's operations.

- In June 2015, China is alleged to have attacked the Office of Personnel Management and stolen personal and professional details on 4.2 million American civilians.

- In August 2015, 1.2 million UK personal account details were hacked from an illicit dating website, Ashley Madison. This included 90 members of the UK government and has lead to serious concerns on the threat of blackmail.

- Since 2012, 100 banks in 30 countries were targeted and over $1billion was stolen by a team known as Carbanak. These attacks were directed at the internal networks of the financial institutions and were not localised to a particular type of technology, as outlined below.



Source: Kaspersky

- In August 2015, Carphone Warehouse was hacked and the personal and financial details of 2.4 million customers were stolen. This also had a direct regulatory and reputational risk to banks that provide insurance and credit facilities to the Carphone Warehouse customers.

Many cyberattacks are not revealed publicly due to the concern that institutions would lose the trust of their customers. It is clear that most institutions are targeted daily and it has been reported that 90% of FT500 companies have been subject to cyberattacks, with the remaining 10% unaware of where they are being attacked. According to GCHQ, over 80% of UK large companies were hacked in 2014.[25]

An additional problem is that many cyberattacks are targeting intellectual property, the theft of which is difficult to detect. The cybercriminals can sell secret information to the highest bidder or multiple bidders. Frequently the infiltrators are assets of governments seeking to obtain valuable information about other nations' weapons' programmes, satellite information and political data.[26] Imagine the economic impact of a countries' multi-billion pound secret fighter jet blueprint being released before production.

[25] GCHQ CyberReview reported by BBC News Jan 2015

[26] Cyberwar – Richard Clarke

Designing Effective Countermeasures:

Designing an effective solution to minimize the risk of cyberattacks relies on four key design principles[27]:

Principle 1: Technical Countermeasures

Technical countermeasures are based on the latest ‘state of the art’ hardware and software tools to prevent unauthorized access across the network. Firewalls are considered the first line of defence of this type of countermeasure, which are nodes in a network that set access rights for the users, type of data and services that can pass through gateways that ‘bridge’ sub-networks, as illustrated in the example below.

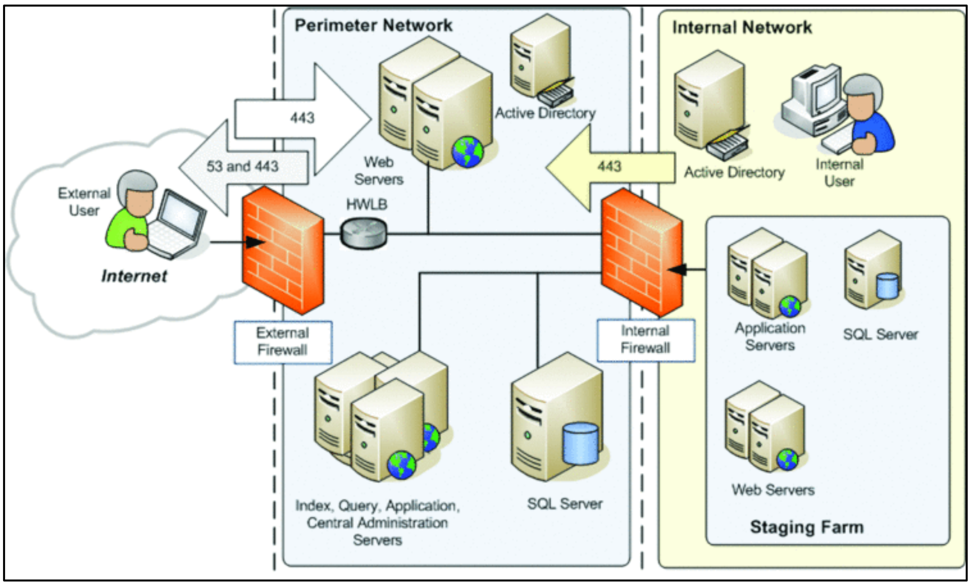


Figure: Example of a firewall configuration

Antivirus software, network monitoring tools and penetration testing are also technical countermeasures that are frequently deployed. Institutions need to ensure that they constantly update to protect against the latest variants of malware. Encryption, increased authentication methods such as biometrics, and ‘clean hosts’ can also be embedded within a network security design strategy.

Principle 2 – Economic Countermeasures

Ultimately, the economic countermeasures to defend against cyberattacks depend on the incentives associated with the attack. Espionage, theft of intellectual property, commercial sabotage all have a clear economic impact on individuals, institutions and governments. It is imperative that a punitive action can be taken to recover this lost value, although this is currently difficult to uphold on an international basis.

[27] Cyberwarfare and Cybercountermeasures – Wikipedia; Economics & Cyberpolicy - Crabbe

Policy makers have started to analyse the economic impacts of underinvestment in cyber security, applying many of the techniques of microeconomics that have been applied in areas such as environmental policy.[28] The economic impact of the internet is estimated to have contributed 3-4% of the GDP of developed economies. The economic importance of the internet is therefore a critical factor in the design of a national policy. Some have argued that the economic factors are more important to address than the technical countermeasures.[29]

The imposition of sanctions by the US Government on North Korea following the Sony cyberattack indicates the serious nature by which economic conditions can be introduced following a cyber attack.

Principle 3 – Legal Countermeasures

This is one of the most interesting and complex areas to investigate. Most laws are national in nature and there has not been a strong desire to get universal support to develop an internationally rigorous legal framework against cyberattackers. This may also be because many of the governments are condoning, if not actively driving, the cyberactivity.

Corporations and individuals that are prone to cyberattacks do have legal countermeasures to combat the hackers, which includes legislation on computer crime, identity theft, copyright protection, data theft, access prevention and malware dissemination. These tend to be nationally applied in different variants of strength depending on the country.

There appears to be a rising tension when this issue is considered internationally. The US considered, for example, that the recent Sony attack was an attack on the government of the USA and would consider reinstating North Korea as a global terrorist target. Pursuant to Article 51 of the UN Charter and customary international law, if the malicious cyber operation against Sony had constituted a "use of force" rising to the level of an "armed attack," the United States would have been entitled to respond forcefully, whether by kinetic or cyber means. This would also have enabled the United States to seek the credibility of the United Nations legal framework to support any actions taken.

Principle 4 - Behavioural Countermeasures

Behavioural countermeasures can also be an important area to combat cybercrime. At the simplest level, public awareness and training is key. Bank fraud, for example, that originated by customers responding to fake emails is a typical example. The fault here frequently lies with the banks who have not educated customers that they would never contact them by email. Addressing this weakness would have a significant reduction on daily fraud events that cost banks significant costs to remediate.[30] Other simple areas include awareness of the need

[28] An overview of the economics of cybersecurity & cyberpolicy – J Cordes

[29] McKinsey – Measuring the Net's Growth Dividend

[30] Neural Insights – Fraud & Behavioural Analytics

to maintain effective password standards, telephone network response traps and malware avoidance techniques.

More advanced analytics on customer behaviour, fraud detection patterns, and biometrics are also a key tool to either minimize the risk of cyberattack, or maximize the detection rate and thereby mitigate the impact after an attack.

Financial Services – An Industry Example Under Attack

Banking is about trust and it is a fundamental requirement that banks maintain the trust of the customers to prevent losing those customers. Recent examples, such as the run on Northern Rock, demonstrate that this is still a fundamental requirement of banking. Cyberattacks, whether real or perceived, are a perfect tool to erode trust.

Traditionally, banking consisted of a well defined branch network which provided an effective physical infrastructure to safeguard customer assets. Stealing from a bank generally involved forced entry, arms and insider access or information. Over time, banks gradually added call centres then on-line banking to enable customers to have greater convenience in how they communicated with banks. These were known as the channels of access. Fundamentally, they were still based on integrating with the same underlying physical infrastructure of the traditional bank.

Modern banking however has changed based on customer expectations of greater personalisation, faster access, streamlined and innovative channel access, and near zero transaction costs. This has enabled digital and mobile banks to emerge as challengers to the traditional banks, and presented a new type of business model that banks have needed to address. In short, for many banking is now something you do rather than somewhere you go.[31]

The structure of a modern bank is essentially a large computer network that manages the integrity and security of data. Functions within a bank, such as payments, are essentially utilities that transfer data between banks and institutions. Unfortunately as the expectations of real-time digital and mobile banking evolve, the risks to the integrity of the data and the networks rise dramatically.

This is a perfect environment for cyberattacks.

As an example, the UK Faster Payments Scheme has introduced instantaneous payments between parties. This means that the opportunity to validate the transactions is much reduced and leads to a higher incidence of fraud. There are additional steps that are being introduced to, for example, increase the levels of authentication but many of these are proving to be too cumbersome for customers to want to adopt. New devices such as Apple Pay bring convenience

[31] SAP Global Forum 2015 Paper - Rise of Challenger Banks – Neural Insights

but the risks have had to be contained by setting financial upper limits on sizes of transactions, currently set at £20 per transaction. As has been demonstrated historically though, cyber attacks frequently occur at large volume of small transaction value.

All banks are required by law to have effective financial crime, systems controls, fraud detection and network resilience infrastructure in place. There are a number of industry standards that have emerged to provide a 'best-practice' solution in this area, many of which are also the industry standard for government networks and applicable across multiple industries. At the time of writing, the leaders are as follows:

Top 10 Detection Tools[32]
Actimise
Bankware.NET
FICO Falcon
Alaric Fractals
FiServe
NetReveal
Oracle Bharosa
Patriot Officer
SAS
Entrust

In addition to the technical countermeasures listed above, banks also employ behavioural analytics to identify vulnerabilities in operation. To be effective, the data that is used to understand customer activity is frequently shared between banks. As an example, online applications for loans or insurance at different institutions under different names that would have similar data attributes such as size of loan, telephone numbers, variations in claimed insurance details, or address similarities would all trigger fraud analysis.

At an individual level though banks are still at a significant disadvantage. The primary attacks against them have exploited known vulnerabilities in the original design of software, known as *zero day* attacks, DDoS against mobile and ATM networks, phishing and variants. They have proven to be successful, and cost the UK banks alone £700 million per annum to maintain the current level of marginally effective cybersecurity infrastructure.[33] In the event of an attack, banks have been pro-active in reimbursing the customers any sums lost as they do not want to lose the trust of that customer, or breach their legal requirements set by the Financial Conduct Authority.

[32] Capterra Top Fraud Software 2015

[33] British Bankers Association – Cybersecurity Resilience & Costs Feb 2015

At an industry level, however, the issues are more alarming. In January 2015, the Bank of England warned the UK banks that there were "ever-present, ever-evolving threats from hackers and cybercriminals, and should expect that attempts to penetrate their networks would be successful". Furthermore they added that a successful attack on a bank today could not only result in the corruption or loss of data held in the bank's systems, but also "a complete loss of systems, disrupting a firm's capacity to operate".[34]

Governments already have the capability to cyberattack other nations' banking systems. This was considered as a pre-emptive action by the Bush administration ahead of attacking Iraq, and has been shown to be effective in attacks by activists against Estonia and Ukraine, and disabling banking systems in US, Russia and India. It is also known that the Chinese army's cyberforce have a specialised financial industry attack forum in the event of a major escalation. The technology to attack has to be assumed to be available to the broad range of cyber activists, not just governments.[35]

There is therefore a question on how to protect the financial services industry from attack. One potential answer exploits technology that was originally designed to protect the assets of criminals. The technology is based on a technique that enabled 'value' to be transferred between parties on an anonymous basis and without the need for a central 'controlling banking party'. This was originally devised by Satoshi Nakamoto as a basis for a cryptocurrency that would emerge as Bitcoin.[36]

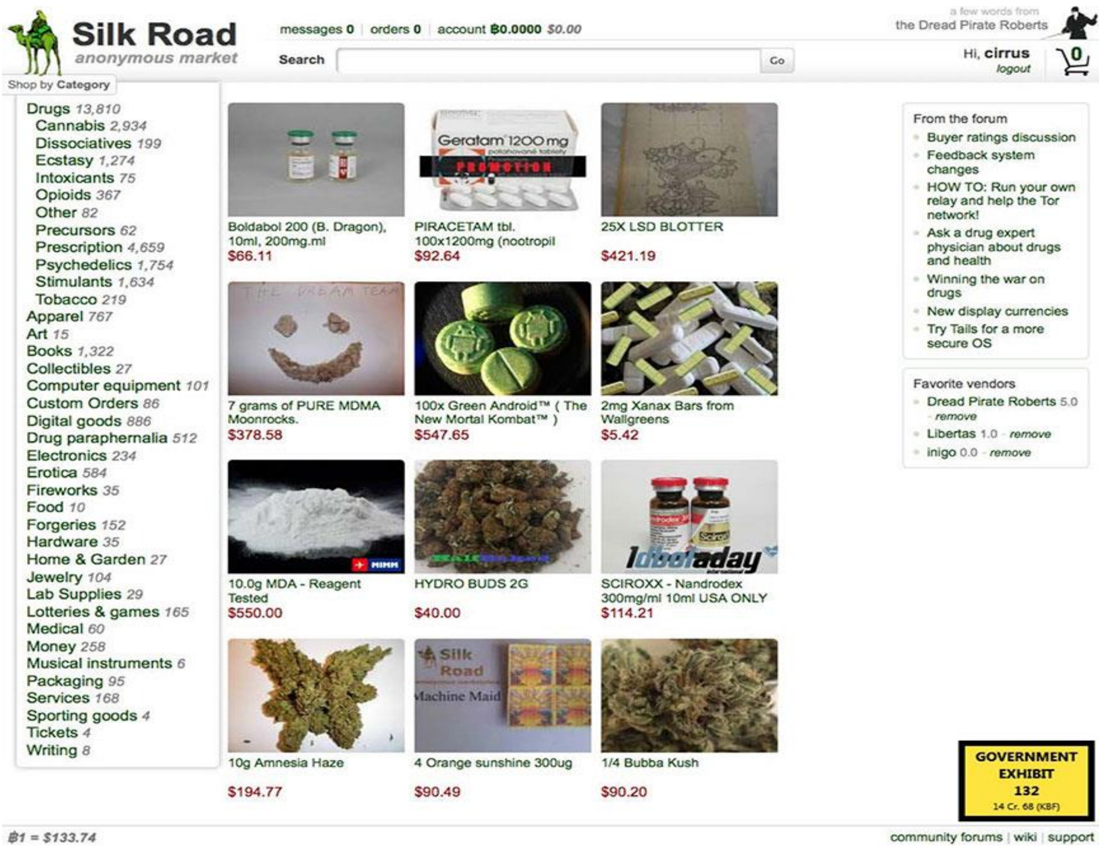
The identity of Nakamoto is unclear and is thought to be a group rather than an individual. The identity of the author of the paper is being held in secret as it is likely that they would be arrested for the initial implementation of Bitcoin. An anonymous currency that parties would accept as a 'fiat currency', one that does not require an underlying asset to benchmark value, and does not require a centralised trusted party is an ideal currency for illegal activities. Unfortunately that was how it rose to prominence, notably on Silk Road where Bitcoins were the accepted currency to purchase drugs, arms, order assassinations, and many other forms of criminal activity.[37]

[34] Andrew Gracie – Bank of England Executive Director – Jan 15

[35] Cyber War – Richard Clarke

[36] P2P e-coin strategy – Satoshi Nakamoto 2008

[37] See silk road extract image from government case



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.0000 $0.00

Search

Go

a few words from
the Dread Pirate Roberts

Hi, cirrus
logout

0

Shop by Category

Drugs	13,810
Cannabis	2,934
Dissociatives	199
Ecstasy	1,274
Intoxicants	75
Opioids	367
Other	82
Precursors	62
Prescription	4,659
Psychedelics	1,754
Stimulants	1,634
Tobacco	219
Apparel	767
Art	15
Books	1,322
Collectibles	27
Computer equipment	101
Custom Orders	86
Digital goods	886
Drug paraphernalia	512
Electronics	234
Erotica	584
Fireworks	35
Food	10
Forgeries	152
Hardware	35
Home & Garden	27
Jewelry	104
Lab Supplies	29
Lotteries & games	165
Medical	60
Money	258
Musical instruments	6
Packaging	95
Services	168
Sporting goods	4
Tickets	4
Writing	8

Boldabol 200 (B. Dragon), 10ml, 200mg.ml	$66.11
PIRACETAM tbl. 100x1200mg (nootropil	$92.64
25X LSD BLOTTER	$421.19
7 grams of PURE MDMA Moonrocks.	$378.58
100x Green Android™ (The New Mortal Kombat™)	$547.65
2mg Xanax Bars from Wallgreens	$5.42
10.0g MDA - Reagent Tested	$550.00
HYDRO BUDS 2G	$40.00
SCIROXX - Nandrodex 300mg/ml 10ml USA ONLY	$114.21
10g Amnesia Haze	$194.77
4 Orange sunshine 300ug	$90.49
1/4 Bubba Kush	$90.20

From the forum
- Buyer ratings discussion
- Feedback system changes
- HOW TO: Run your own relay and help the Tor network!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS

Favorite vendors
- Dread Pirate Roberts 5.0 - remove
- Libertas 1.0 - remove
- inigo 0.0 - remove

GOVERNMENT EXHIBIT 132 14 Cr. 68 (KBF)

฿1 = $133.74

community forums | wiki | support

Figure: Extract from Silk Road Website

The key aspects of a crypto currency require a secure environment that maintains the integrity and agreed value of the underlying currency, is transparent in terms of ownership of currency without giving the identity of the owner away, avoids the ability for parties to multiple spend the same currency, and is resilient.

Bitcoin, and a number of other 30+ crypto-currency variants achieve these goals by having multiple ledgers (or copies of the data) that are all aligned, not owned by one single institution thereby increasing resilience, and rely on a technique called block chain technology to validate the integrity of the data. A block chain is a distributed (held on all ledgers simultaneously) set of data records that show the change in ownership of the currency and are extremely hardened to tampering or theft, even by the owners of the nodes of the central ledgers.[38] It is recorded chronologically and uses a cryptographic key to ensure that the integrity of the timeline of the transactions is always maintained. Furthermore it is stored on every computer (or 'node') in the network (the ledgers), and lists the sender, receiver, value and approximate time of every value transfer, all verified and anonymised.[39]

Furthermore as the data is openly transparent to all members of the network, albeit the individual owners of each piece of the data are not known, there is no incentive to 'sniff' the data for cyberattack.

[38] Cryptocurrency – Vigna & Casey

[39] Alphr – Blockchain Technology 2015

At its' simplest level, block chains work as follows:

1. Initial 'units' of currency are created.

   In the case of Bitcoin, these are created by assigning the notion of computing power to solve a puzzle as an indicative 'commit' to assign an agreed value to a unit of currency. The total volume of currency to be created in the global 'cyber economy' is pre-set to avoid artificial volatility or value erosion.

2. Each member of the cyber economy has a unique 'wallet' or address, which is the central holder of the value held by that individual.

3. The address and value of all wallets is replicated across the ledgers on every node in the network, significantly building in a resilient record of the cyber financial system that has been created.

4. When a transaction takes place, the two parties in the transaction broadcast their transaction to the whole network, complete with a unique individual private key that they each hold, and the underlying value.

5. A validation of this transaction is based on two complex mathematical functions on these 3 inputs (2 keys and the value) that create a new and unique validation code that is associated with the transaction. The two functions are common functions used and validated in advanced cryptography.[40] This validation is performed by other computers on the network and a digital 'signature' is applied to confirm the legal transfer of value.

6. The digital signature is attached as a new block chain of evidence of value change to both parties in the transaction. This enables a chronological sequence to be maintained in the ledger. It is (practically) impossible to reverse engineer the digital signatures and adjust the transactions to commit theft or fraud.

7. Finally, the confirmed block chains are synchronised across the network, ensuring that the individual ledgers all maintain the ability to continue to manage and validate future transactions.

The advantages of the use of block chain technology enable any data to be made significantly more complex to attack. This may have a number of additional novel application including managing the integrity of electronic voting, insurance and legal contracts, and any other mission critical data.

As there is therefore not a central banking node to attack, and the resilience of the data is maximized across a network, this is proposed as a potential to avoid a central attack to a financial system. Individual governments and banks could

[40] The functions are called hash functions and Merkle functions but are outside the scope of this essay

replicate their financial systems across a global network, which would mean individual localised attacks to utilities, for example, would not bring down an entire financial system.

Conclusion:

The primary role of a government is to secure the safety and stability of its people and its financial assets. There is a proven link between the financial stability of an economy and the order of rule of a country. Recent examples of the Arab spring rising, riots in Greece and the Kuwaiti oil company attacks highlight the issues that arise when the economic stability of a country is threatened. Governments have recognised this threat and many have initiated both attack and defence strategies to support their financial infrastructure. Cyber is considered by many governments to be the number one priority against terrorism.

In summary, this paper has highlighted the significant threat to the world by the increasing threat in cybercrime, and a number of the techniques used to attack and defend cyberspace. It has proposed a potential and elegant solution to create a globally integrated, fully transparent and resilient blockchain-based architecture for all financial transactions.

Key References:

Clarke, R.:	Cyberwar
Cordes, J.:	An overview of the economics of Cybersecurity & Cyberpolicy
Goodman, M.:	Future Crimes
Singer & Friedman:	Cybersecurity & Cyberwar
McKinsey:	Measuring the Net's Growth Dividend
The Economist:	Cyberwar (1st July 2010)
Vigna & Casey:	Cryptocurrency
Nakamoto, S:	P2P e-coin strategy (2008)
IDC:	Big Data Survey
SAS:	Analytics & Big Data
White House Policy Paper:	Cybersecurity (Order Number 20)
Heritage Foundation:	Cyber Attacks on US Companies – Riley Walters 2014
Neural Insights:	Challenger Banks, Fraud & Financial Crime
Wikipedia:	Arms Race
Wikipedia:	Military Conflict Analysis (Richardson)
Wikipedia:	Cyberwarfare & Cybercountermeasures
Wikipedia:	Economics & Cyberpolicy