Cyber Threat Intelligence

An analysis of an intelligence led, threat centric, approach to Cyber Security strategy within the UK Banking and Payment Services sector

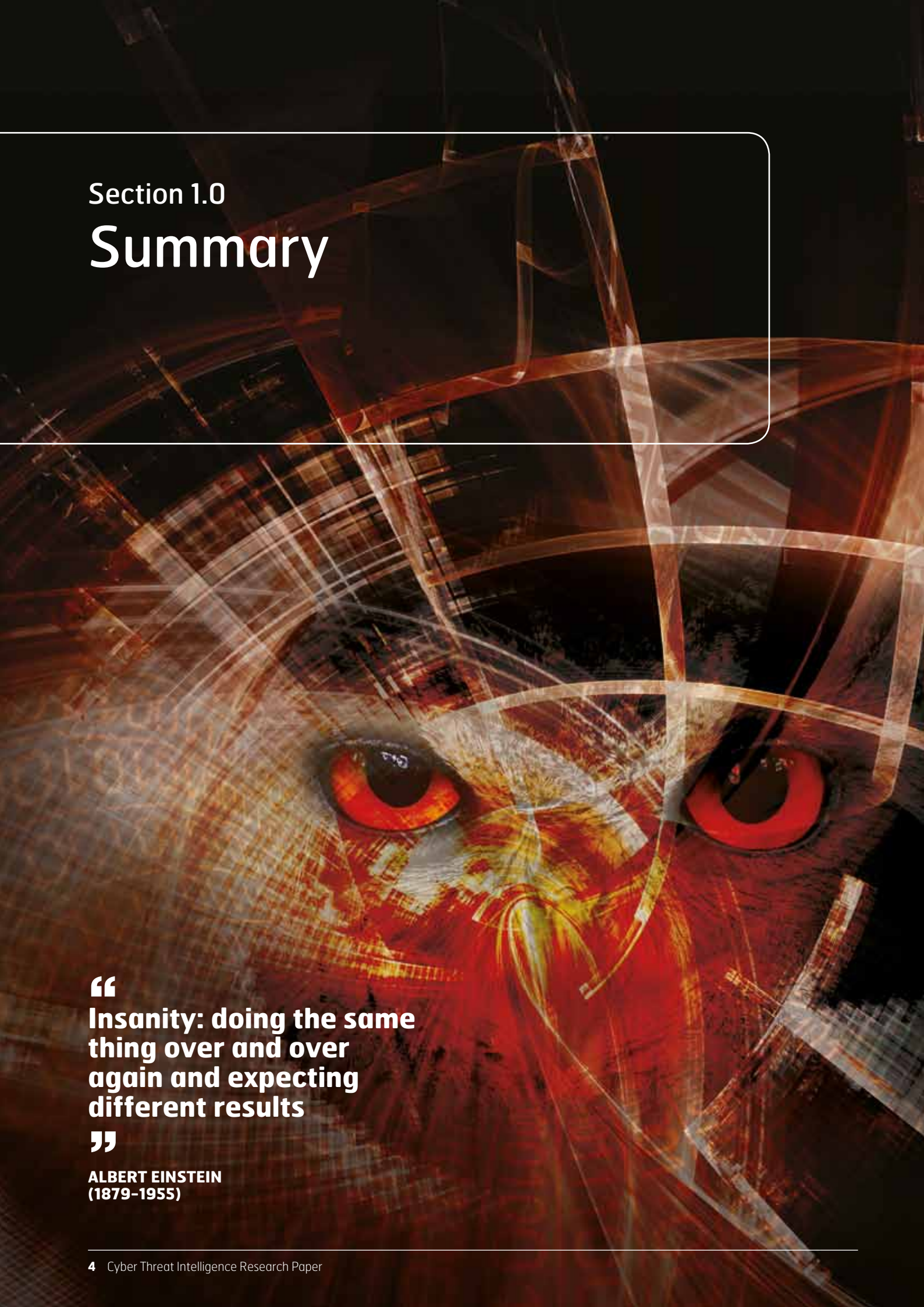
A Research Whitepaper

Contents

Version 1.1

This report is divided into four sections:

A further separate appendix is also available:



Section 1.0

Summary

“Insanity: doing the same thing over and over again and expecting different results”

ALBERT EINSTEIN (1879–1955)

Banking and Payment Services represents one of several high priority targets for Computer Network Attacks (CNA). CNA has arguably become the most prevalent medium of the threat to confidentiality, integrity and availability of retail, corporate and investment banking. It also represents a strategic threat to the payment systems and services that constitute the cortex of a hyper-connected and interdependent financial system.

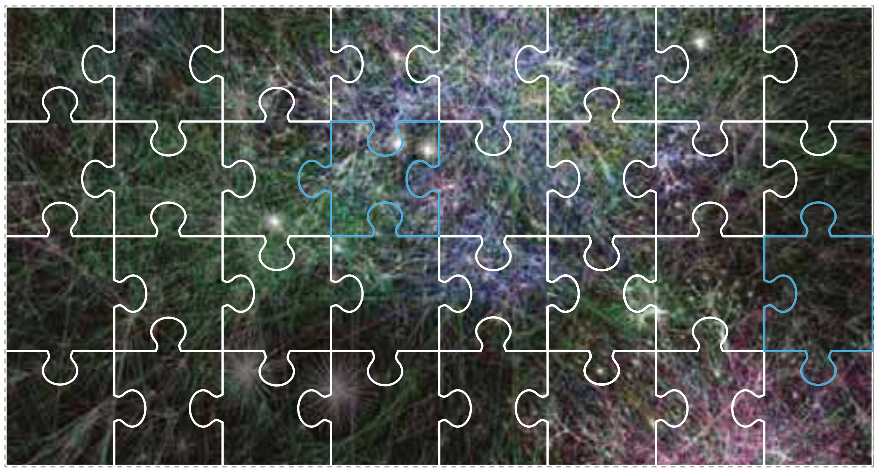
Further investment in technological defences is no longer proving effective against high end CNA threats. These highly organised, sophisticated and networked attacks are the variants that repeatedly penetrate Computer Network Defences (CND). The consequences of these attacks are evolving from simply intrusive, to disruptive and eventually destructive as the value of CND erodes from porous to inverted and eventually to virtual. Technological hardware and software defences remain the bedrock of effective cyber security strategy, mitigating the majority of less sophisticated attacks. However, a cyber security strategy founded on these measures alone will not be effective in the future.

This paper advocates the creation of a collaborative and federated cyber threat intelligence capability as the capstone to an effective cyber security strategy. This would improve the protection of retail, corporate and investment banking networks by allowing security managers to prioritise vulnerability patching. It would operate within existing information sharing forums as well as national and international governance initiatives to achieve a level of cyber security that cannot be achieved by any single institution alone.

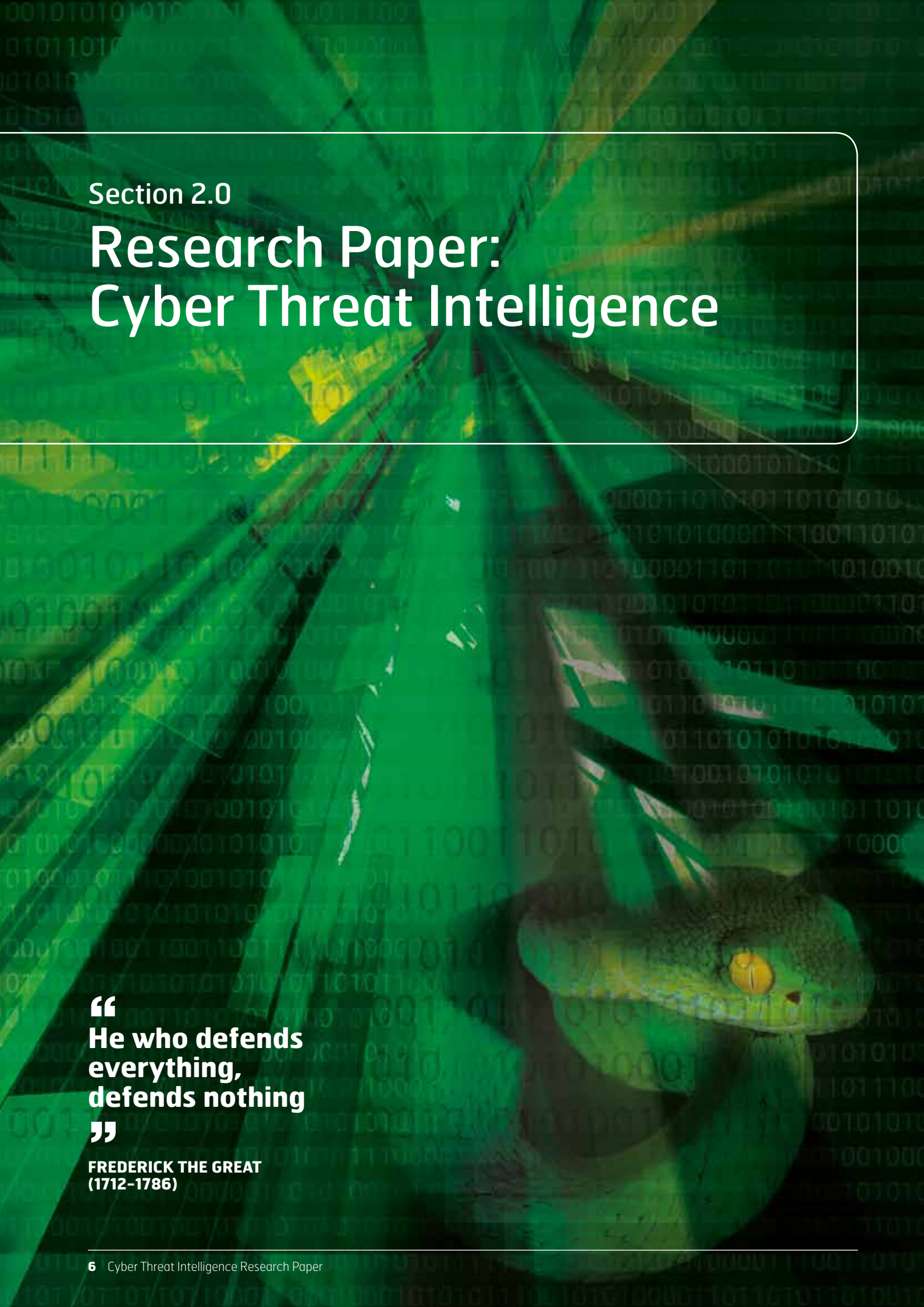
The aggregation of attack, anomalous and decline data reports, into a single secure environment that affords anonymity to all contributing financial institutions would, for the first time, achieve a Common Operating Picture (COP) of all CNA attacks and anomalous data across all areas of Banking and Payment Services. Separating data submissions into retail, corporate and investment profiles would allow a detailed Electronic Pattern of Life (EPoL) of CNA to be discerned for each form of CNA target. Moreover, creation of "big data" in these variants would also allow Electronic Finger Printing (EFP) of CNA Techniques, Tactics and Procedures (TTPs) offering potential collateral benefits by aligning corporate security education and training to the most damaging and prevalent attacks and informing the design or refinement of future CND architecture.

This initiative builds upon the lessons identified from the Banking and Payment Services initiative to combat fraud and the design and evolution of the Financial Intelligence Sharing Service (FISS). The ownership of both the function and data of this entity remains under the full control of contributing institutions.

A Banking and Payment Services Cyber Threat Intelligence (CTI) capability will also provide a docking point for law enforcement and the regulator without the reputational risk associated with current single institutional bi-lateral arrangements. A collaborative and federated capability also represents the most cost effective arrangement to increase the effectiveness and efficiency of existing cyber security measures.



The potential to achieve understanding of a novel and complex problem is optimised by seeing the whole problem, whether at the centre or the edge of the issue.



Section 2.0

Research Paper: Cyber Threat Intelligence

“He who defends everything, defends nothing”

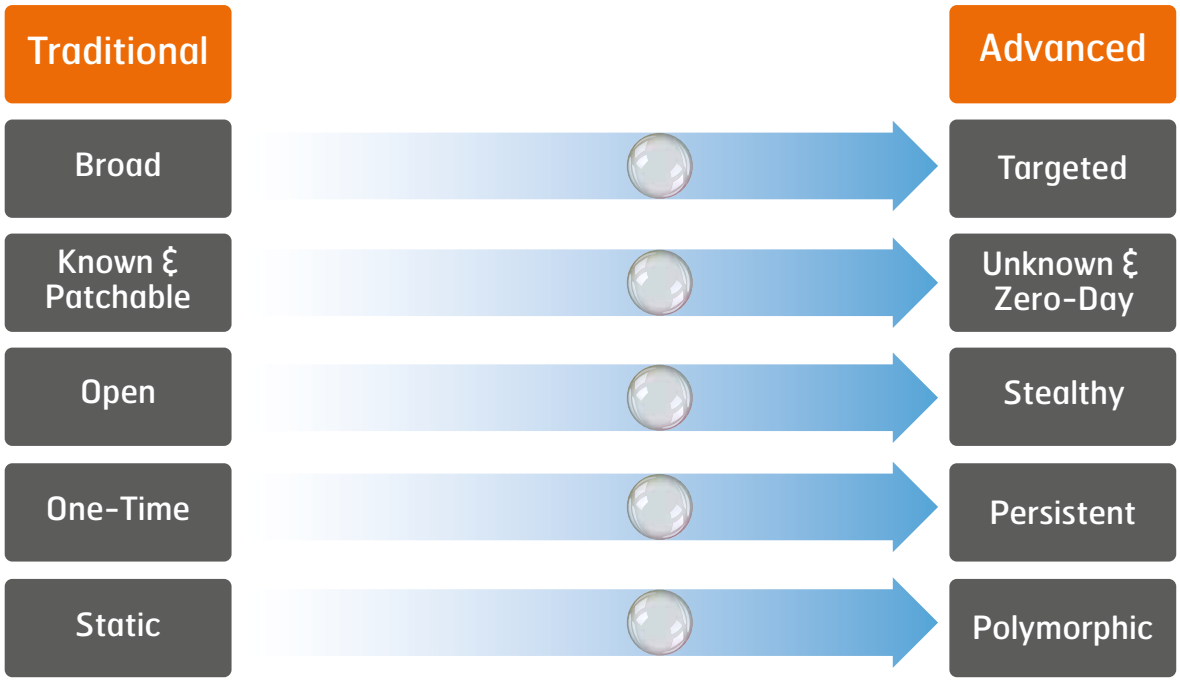
FREDERICK THE GREAT (1712-1786)

For decades cyber security has predominantly constituted the software and hardware controls of Computer Network Defence (CND). CND is maintained and enhanced by regular improvements and software "patching", collectively known as cyber hygiene.

This "technology led" approach to cyber security has focused on "target hardening" aspiring to create a strong perimeter of interlocking hardware and software defences to make illegitimate intrusion complex and difficult. This approach has, in the past, achieved mitigation, but not deterrence, of the majority of cyber attacks against financial institutions, variously estimated at 88-89% of attacks[1].

However, these attacks, those that have been stopped, are not the threats that cause the damage. Although Computer Network Defence and rigorous cyber hygiene remains fundamental to any cyber security strategy, it no longer constituents a complete response to the Computer Network Attack (CNA) threat.

An "intelligence led" strategy is now required to counter the agile and innovative industrialisation of cyber attack techniques, malware and exploit kits[2]. The increasing threat of cyber network attack entities originates from the cascade of increasingly sophisticated applications used by both organised criminal and state sponsored, or enabled, cyber attack capabilities. This has led to the commoditisation of cyber attack capabilities into hacker tool kits that are commercially traded on the dark web. Cyber attackers are also exploiting publicly available information, including social media, to target carefully crafted phishing attacks against financial management institution staff, customers and companies in their supply chain, in order to circumvent network cyber defences.

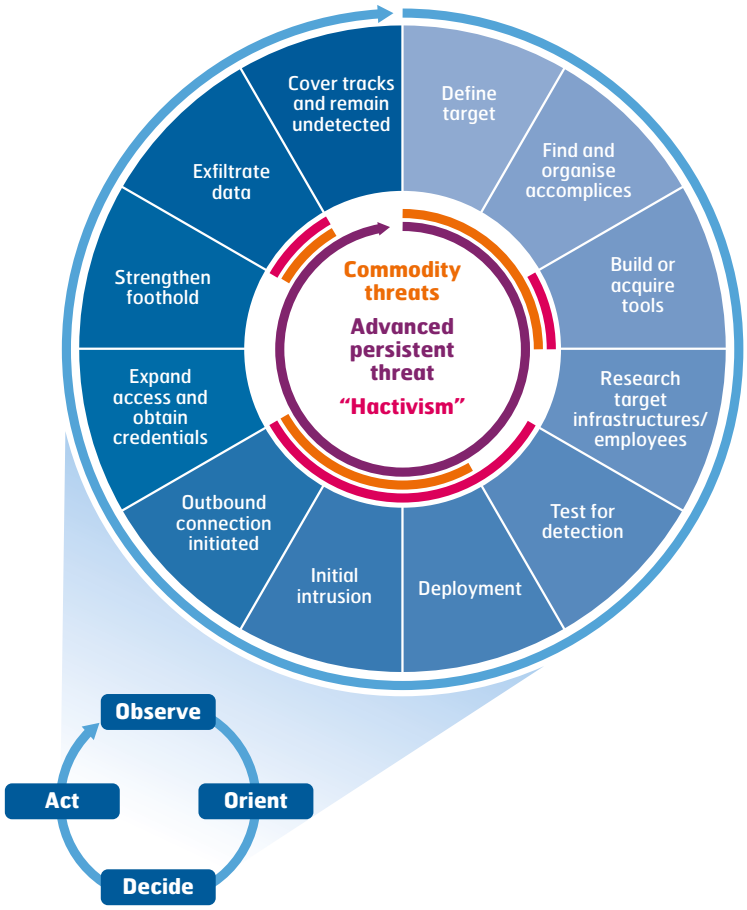


The characteristics and nature of the transformation in the malware threat

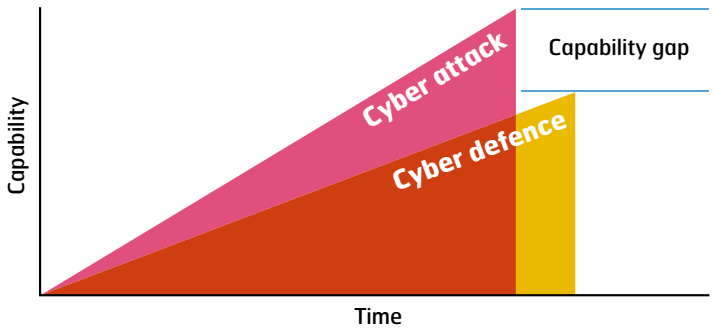
1 Online Trust Alliance and RSA. US Senate and UK Government reporting places the figure at 80%.

2 Kaspersky Security Bulletin 2013. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf IBM Cyber Security Intelligence Index. http://www-935.ibm.com/services/uk/en/security/infographic/cybersecurityindex.html Verizon Data breach Investigations report 2013. http://www.verizonenterprise.com/DBIR/2013/

The threat of Cyber Network Attack (CNA) is developing and operating faster than Computer Network Defences (CND) can respond. The increased CNA threat is outpacing traditional technology led, target-centric, approaches to cyber security strategy. The cyber threat spectrum is becoming a more challenging operating environment, in which adversary attack capability[3], intent and opportunity[4] are all increasing.



The agility and processes of cyber network attack methodologies



The strategic imbalance of cyber network attack against cyber network defence

If it has not already occurred then very soon a capability gap will exist that allows cyber network attacks to penetrate financial institutions and payments systems at unprecedented levels, threatening confidentiality, integrity and availability[5]. The Banking and Payment Services sector is now exposed to a variety of actors and capabilities, some of whom operate below the detection capability[6] of even advanced cyber network defences and surveillance of any single organisation or institution[7].

3 Currently Intrusive and Disruptive, but potentially the "Internet of things" or machine to machine communication will facilitate further Destructive attacks. (RSA)

4 The growth of mobile platforms in the UK Banking and Payment Services retail, corporate and investment banking landscapes considerably complicates an already complex threat environment.

5 RSA define the protection afforded by traditional CND as porous (2007), inverted (2013) and virtual by 2020. (https://www.youtube.com/watch?v=R31Ez1XJEeI)

6 Verizon term this "low and slow" to describe advanced persistent threats with a low digital forensic signature.

7 This has been a key feature of the recent UK Banking and Payment Services exercise, Waking Shark II. http://www.bankofengland.co.uk/financialstability/Banking and Payment Servicesc/Documents/wakingshark2report.pdf

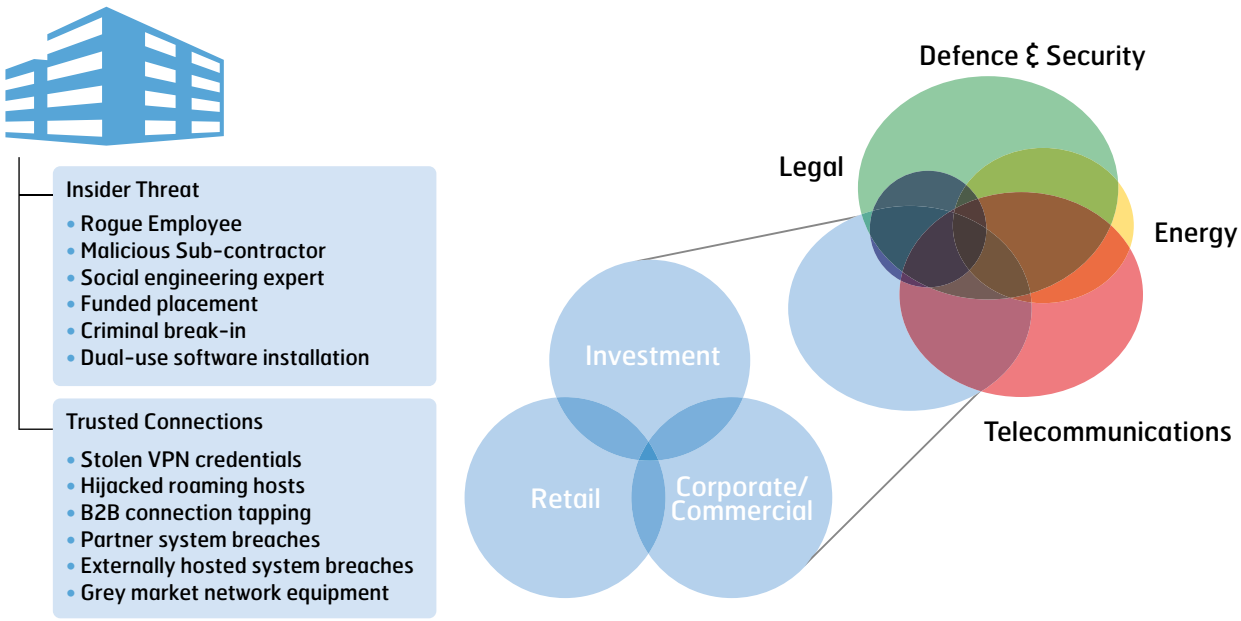
State sponsored attacks against Saudi Aramco, the Stuxnet sabotage of Iranian centrifuges, sustained network phishing attacks by organised crime threat networks, allegations of industrial espionage against Chinese telecommunications providers and the evolution of the ZEUS exploit all provide high profile indicators of a congested and highly contested cyber operational space.

The cyber domain represents a further challenge to security managers, in that a single individual can command the skills and support base to represent a hazard across the entire threat spectrum.

High Priority Targets

Banking and Payment Services remains a high priority target and a key element of the Critical National Infrastructure of the states it serves with investment, corporate and retail operations. Payments systems are the central nervous system of global Banking and Payment Services inter-dependence. The Payments Council believes that the UK Banking and Payment Services sector requires a collaborative and federated Cyber Threat Intelligence (CTI) capability in order to provide a Common Operating Picture (COP) of the covert and clandestine cyber threat networks conducting cyber network attacks (CNA) against financial institutions and key elements of the supply chain.

Attack vectors and resources available to a cyber attacker

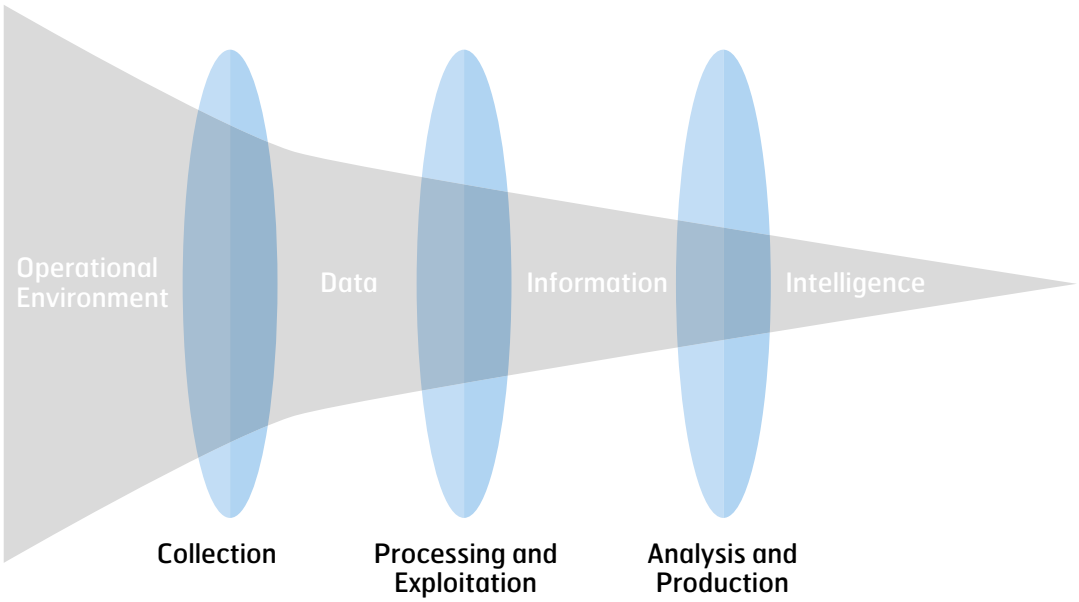


High threat sectors in relation to Banking and Payment Services

Institutions at risk of cyber attacks operate in key sectors; Defence & Security, Energy, Telecommunications and Banking and Payment Services[9] have individually embraced initiatives such as the HM Government sponsored Cyber Information Sharing Partnership (CISP). They have also established sector information sharing forums to exchange data on the operational characteristics of the cyber attacks against their systems. These are necessary to focus on the particular threats prevalent in each sector. For example the challenge of the exfiltration of intellectual copyright and protectively marked material from the secure networks of institutions in the Defence and Security sector, is very different to the subversion and illegitimate use of communication networks that Telecommunications corporations must counter. A common threat in Banking and Payment Services is theft, but confidentiality and integrity is a key consideration for payment systems and their customers in investment, corporate and retail banking operations.

The Payments Council believes that there is a complimentary role for industry centric, cyber threat intelligence generating capabilities within a collaborative network of information sharing nodes. These entities will enhance the defensive capabilities of the sponsoring and supported institutions. They will also provide data of sufficient granularity and integrity to provide investigatory start points for law enforcement. These nodes will oxygenate the exchange of information between sectors to provide a more evaluated and nuanced strategic understanding of the cyber threat spectrum from criminal and subversive sources. This intelligence led strategy, in partnership with law enforcement agencies, seeks to disrupt and degrade those cyber attackers and their supporting networks that represent a significant threat.

9 The Legal sector is emerging as a fifth critical area, as cyber criminals target these firms to breach the cyber defences of institutions operating in the other key sectors.



Relationship between data, information and intelligence

Data, Information & Intelligence

The distinction that is fundamental to this concept is the difference between data, or simply exchanging information between institutions, and generating cyber threat intelligence. The latter requires both sector and operation specific data that has been collected in a systematic and systemic methodology, evaluated and codified to an agreed and interoperable standard. This is vital if the quantitative and qualitative materiel necessary for objective analysis, using specialist analytical tools, is to be achieved. The codified data would be derived from cyber attacks, suspicious cyber activity (anomalous activity) and declined data against investment, corporate and retail banking networks. This focused approach is a key prerequisite for achieving the best possible "signal" of highly sophisticated cyber attacks from the "noise" of daily, legitimate cyber traffic and illegitimate low end cyber network attacks that are detected and countered by current CND.

A "Hierarchy of Data" is perhaps the most accessible way of appreciating the utility of different collection and processing techniques, the value to the end user and the resource cost of collection and processing in a cyber threat intelligence context. Taking a Banking and Payment Services sector specific focus (high noise, low signal) it has been demonstrated that information, whilst useful qualitatively, does not illuminate the breadth or depth of the threat spectrum. US Intelligence Doctrine (JP 2-0[10]) illustrates the relationship between data, information and intelligence as a series of lenses. Each lens should be considered a processing or refinement procedure that allows indicators and warnings to be distilled for the available sources.

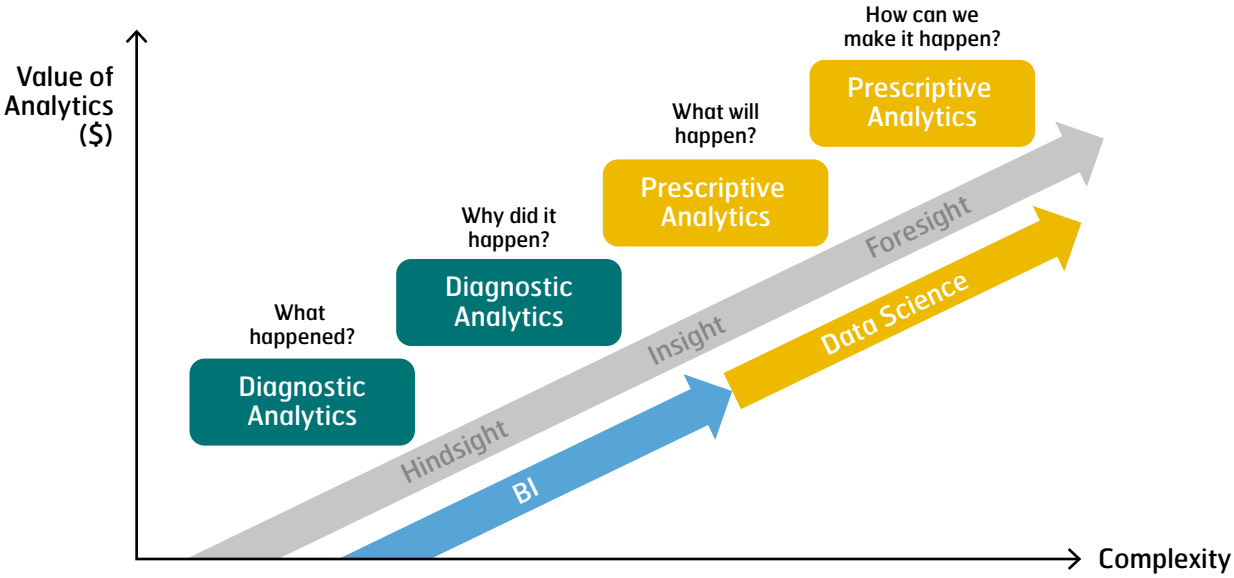
Data, collected and processed systemically and systematically from sources assessed as pertinent, even core to the objective of the analysis, offers greater insight, but arguably not foresight. Data analytics using Search, Visualisation and Analysis (SV&A) tools allows trend analysis and patterns of behaviour to be discerned from even fragmentary data sets over time. Aggregating data into a single secure environment, a "data lake", offers the potential to employ big data analytic tools.

10 Joint Publication 2-0, Joint Intelligence dated 22 Oct 2013.

Big Data Analytics

Big Data, articulated the volume, velocity, variety and veracity[11], can be analysed at rest (batch processing) or in motion (stream processing). Batch processing is used for large volumes of data (Petabytes) on long lead times (hours), whereas stream processing is more useful for smaller volumes of data (Gigabytes and Terabytes) on shorter lead times (seconds and minutes). The volume of data generation is increasing exponentially with a corresponding increase in the speed of transmission or dissemination. It is estimated that 90% of data in existence was generated in the last 2 years[12]. Data is now collected and used in ways not even considered even a few years ago and in both structured formats and unstructured. The increasing maturity of Big Data analytical tools, notably HADOOP at Version 2.3.0 (20 February 2014, a batch processing tool), is beginning to match stakeholder expectations. Influenced by a decrease in data storage costs, flexibility of data centres and cloud storage the value that large data sets, known as "data lakes", can provide to security intelligence is beginning to be realised. The relationship between business intelligence and data analytics as a foundation of cyber threat intelligence is illustrated below[13]. Big data analytics will provide the electronic Pattern on Life (ePoL) and Electronic Finger Printing (EFP) of high end cyber network attacks against banking and payment systems targets.

Initially it is envisaged batch processing, where HADOOP is rapidly emerging as the dominant open source tool, will be used to provide ePOL and EFP that underpins Cyber Threat Intelligence. However, stream processing is rapidly evolving and offers the potential to achieve near real time "tactical tip offs" of emerging attack patterns as the ambition of scale and speed of processing potential increases, beyond the scope of traditional Security Incident and Event Management (SIEM) tools. Cardenas et al (2013) reference applications in APT profiling that are directly relevant to the cyber threat intelligence concept. Similarly they detail Symantec's work to create a Worldwide Intelligence Network Environment (WINE) which is consistent with the matrix of intelligence fusion node model.



The value and complexity of big data analytics

11 Veracity is attributed to an IBM definition, but is a useful addition for considering the use of big data as the basis of a cyber threat intelligence capability.

12 http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

13 Pivotal Software Inc.

Intelligence

Intelligence is data that provides both insight and foresight to the end user and a degree of understanding of complex situations by consideration of the provenance, pedigree and context of the source material, the processing methods and the documents that verify the findings. Arguably the most demanding levels of information collaboration and veracity constitute evidence. This is the most demanding material to collect and process because of the standards of integrity and continuity required for the collection, processing and dissemination of the data. Moreover, the actionable value of evidence is limited to law enforcement agencies and civil litigation.

To operate a cyber threat intelligence capability, in an intelligence fusion node, will require codified inputs and the ability to collect relevant data from contributing network surveillance systems. The cost and difficulty of aligning different organisational communication information systems into a single model should not be under-estimated. However, the emergence of international standards for data structures will considerably reduce the complexity of this task and improve inter-operability. The inter-dependence and interconnectivity of financial institutions and payments systems considered against the increasing scale and capability of the threat indicates that the required investment would be a timely one.

Key Principles

The key factor that will define the success of this "intelligence led" approach is the quality and interoperability of the data inputs into a single fusion analysis centre. This in turn derives some key principles of the operational characteristics:

- **Trusted forum.** In order to ensure detailed data inputs are achieved from all contributors and to operate both collaboratively and in an efficient, federated structure the intelligence capability must be completely trusted. This will be achieved by ensuring all data inputs are anonymised and filtered, to ensure the data sample is pertinent to the subsequent analysis.
- **Responsive and Agile.** To create a truly intelligence-led function the dissemination of intelligence must be achieved in a rapid turnaround and respond to specific requests for information or priority intelligence requirements from contributors. This will be achieved by employing specialist tools known as Search, Visualisation and Analysis (SV$A) applications and automation to achieve the timely dissemination required.
- **Cost Efficient.** The greatest intelligence value is achieved from a broad and comprehensive data input from institutions in the financial sector. Similarly, interdependence between institutions and banking systems requires broad accessibility to this vital key decision support intelligence. This can be achieved by vesting ownership and direction of the cyber threat intelligence capability in the contributing financial institutions and avoiding a client-vendor cost spiral.
- **Interoperable.** Interconnectivity and interdependence does not end at national borders, not least because a key threat actor, organised crime, is transnational in nature. The intelligence derived must be interoperable with similar functions being established in the US, the EU and by the international exchanges. This will be achieved by adopting emerging international standardised technical reports.

The strategic end state is clear; a more secure and resilient UK Banking and Payments Services sector working in partnership with law enforcement and overseas partners to facilitate the disruption and degradation of the cyber network attack threat. The means will be limited unless security budgets are increased, underlining the requirement for greater collaboration and a federated intelligence architecture.

Section 3.0

Research Review

The research review details and assesses relevant industry and government research concerning cyber threat intelligence and security. The conclusions and recommendations of this research have been integrated with current intelligence doctrine and methodology in order to understand:

- Why cyber threat intelligence is required as part of an effective cyber security strategy.
- What the essential elements of a cyber threat intelligence capability are.
- How a cyber threat intelligence capability would integrate into existing information sharing forums.
- How the outputs would add value to cyber security management.
- What the outputs of a cyber threat intelligence capability are.
- How those outputs influence and inform cyber security management.

“Build a network to defeat a network”

STANLEY McCRYSTAL (1954–)

Common Issues in Cyber Security

There is a convergence of research that acknowledges that cyber security is not purely a technical discipline. Klaus[14] (2013) identifies that major weaknesses in cyber network defence and cyber security persist, despite considerable investment. Notably:

- **Poor Decision Support Analysis**. Decisions about security are frequently based on intuition rather than data and rigor; this introduces cognitive biases and undermines decision quality.
- **Flawed Physical and Procedural Security**. Many organisations fail to implement foundational security controls and consequently, are easy targets for opportunistic and novice attackers.
- **Computer Network Defence (CND).** There is an overreliance on the relatively static threat knowledge products such as virus scanners, while an inability to learn and adapt dynamically opens the door for advanced threats.
- **Security Management.** Weaknesses in security governance create systemic control gaps and vulnerabilities.

Similarly Townsend et al[15](2013) identified 11 challenges for US industry and governance in their Cyber threat Intelligence Tradecraft Project (CITP). These are:

- **Applying a strategic lens to cyber threat intelligence analysis.** Despite having a wealth of data available, many organisations struggle with moving beyond the functional analysis of low-level network data to incorporate strategic analysis of threats and threat indicators.
- **Information sharing isn't bad; it's broken**. The highest performing organisations actively share, not just consume, data in formal and informal information sharing arrangements.
- **Understanding threats to the software supply chain.** The unknown provenance of software complicates the ability to define the cyber environment.
- **Determining where cyber threat intelligence belongs organisationally.** Where the cyber threat intelligence function is organisationally situated can affect its focus, performance, and effectiveness.
- **Lack of standards for open source intelligence data taxes resources.** The prevalence of non-integrated, non-standard content and delivery approaches from open source intelligence providers and subscription services burdens analysts, complicates correlation, and contributes to missed analytic opportunities.
- **Adopting a common cyber lexicon and tradecraft.** The lack of a common lexicon and tradecraft is an impediment to the credibility of cyber threat data, which hampers analysis, attribution, and action.
- **Filtering critical cyber threats out of an abundance of data.** Organisations struggle to accurately focus analytical efforts on critical threats because they cannot adequately filter out data that once analysed ends up being classified as low to moderate threats.
- **No industry standard for cyber threat intelligence education and training.** The cyber threat intelligence workforce is a heterogeneous mix of technical experts and non-technical intelligence analysts, neither completely familiar with the nuances and complexity of the other half.
- **Adapting traditional intelligence methodologies to the cyber landscape.** Technology changes very quickly, therefore the process of producing cyber threat intelligence analysis must be dynamic enough to capture rapidly evolving tools, capabilities, and the increasing sophistication of adversaries.
- **Communicating "cyber" to leadership.** Decision makers removed from the cyber environment generally lack technical backgrounds, and functional analysts generally lack experience writing for nontechnical audiences.
- **Difficulty capturing return on investment.** Organisations typically use return on investment (ROI) calculations to justify the costs associated with business practices or infrastructure requirements. In cyber threat intelligence, coming up with ROI remains difficult.

Kim[16] et al (2013) are more unequivocal in their analysis of Cyber Network Attacks (CNA) advocating that only the concept of security intelligence can defend again advanced persistent cyber threats. Their conclusions were derived from attacks in 2009 against over 30 large US corporations (Operation Aurora), and from 2011 attacks against transnational oil and gas corporations. They also examined attacks against French diplomatic targets and security companies.

Bamford[17] et al (2013) also conclude that current reactive approaches are not working, and believe changes in the way we view and operate in cyberspace are necessary. The ethos of the rationale to this research is that "thinking beyond the network" is required to focus on the actors rather than the actions of cyber-attacks. They attribute the current focus as a factor of the origins of cyber security from network security citing:

"Essentially, the status quo is to be too attached to what is visible on a network, instead of looking outside of a network and complementing that knowledge with additional information."

14 Understanding and overcoming cyber security anti-patterns, Computer Networks Volume 57, Issue 10, 5 July 2013, Pages 2206–2211 (Klaus, Julisch), Deloitte Enterprise Risk Services.

15 Software Engineering Institute Emerging Technology Center: Cyber threat intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University. (Troy Townsend, Melissa Ludwick, Jay McAllister, Andrew O. Mellinger, Kate Ambrose Sereno) http://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf

16 Analysis of Cyber Attacks and Security Intelligence, Mobile, Ubiquitous, and Intelligent Computing Lecture Notes in Electrical Engineering Volume 274, 2014, pp 489-494. (Youngsoo Kim, Ikkyun Kim, Namje Park)

17 Intelligence and National Security Alliance, Cyber threat intelligence Task Force, Operational Levels of Cyber threat intelligence dated Sep 2013. (George Bamford, John Fekker and Matthew Mattern) http://issuu.com/insalliance/docs/insa_wp_cyberintelligence_pages_hir?e=6126110/4859250

Cyber Threat

Barnum[18] (2012) concurs, stating "traditional approaches for cyber security that focus inward on understanding and addressing vulnerabilities, weaknesses and configurations are necessary but insufficient". Barnum advocates the centrality of "understanding the adversary's behaviour, capability and intent" to counter current and future cyber-attacks. Within UK doctrine "capability+intent=threat" thus intelligence becomes absolutely central to any threat centric approach to cyber security. Arguably in a cyber context "opportunity" becomes the third factor that increases or reduces the sophistication level of the threat and the breadth of the threat spectrum which exploit the opportunity.

Considering these factors in the context of the threat to banks and payments systems it becomes clear that the Cyber network attack threat is increasing. The comparatively low impact, high probability cyber crime that has been contained to a tolerated friction, within the risk appetite of boards, is becoming eclipsed by the threat of high impact, low probability cyber threats that are increasing in prevalence and effectiveness. Cyber threats once dismissed as too unlikely to consider, are increasingly being reported as serious breaches of confidentiality, integrity and availability that cause serious reputational damage.

Sharing

Moriaty (2013[19]) develops Bamford's theme further assessing that manually intensive information sharing does not meet the operational requirement "leading to lost opportunities to avoid serious losses, improve security practices, prevent attacks and predict attacks". Furthermore, she concludes that information shared widely tends to produce information useful to no one. She concludes that Information Sharing and Analysis Centres (ISACs) is a promising direction to explore.

This commercial initiative, which originates from a US government funded initiative, and has achieved considerable traction in the US Banking sector is completely consistent with national cyber operations policy and concepts. US doctrine offer the most accessible comparator of an integrated cyber security strategy, incorporating cyber network defence, cyber threat intelligence and cyber network attack. Clearly cyber network attack is the preserve of national and trans-national law enforcement and national security and intelligence agencies.

Cyber Warfare

There is considerable commercial scepticism over the use of the term "cyber warfare" (Gonsalves A, 2014[20]), which is also reflected in the UK at board level. Too many sales pitches founded on "fear, doubt and uncertainty" or internal budget requests caveated as "cyber" initiatives have eroded the willingness to engage upon cyber security or cyber threat intelligence issues at senior security management and board levels. However, consideration of the US cyber operations model (US TRADOC[21]) indicates that many activities and lines of operation that institutions and payments systems invest in, do closely correlate to the cyber network operations and cyber support areas.

Moreover, institutions already conduct activities which could be considered cyber warfare, notably: collect and analyse network data, study and characterise the cyber threat, provide cyber trends indicators and warnings, contribute to cyber situation awareness, conduct dynamic cyber defence and assist attack investigations to determine attribution. Those activities considered beyond the scope, interest and resources of the UK Banking sector have been shown in grey. It can therefore be seen that the majority of a proven cyber operations model can be applied and the role of a collaborative and federated cyber threat intelligence capability nests within this concept to improve cyber network defence (cyber network operations).

Cyber threat to UK financial institutions and payments systems			
Capability	Increasing	Network threats becoming more penetrative. State sponsored threats are more active. Individual actors have better access to commoditised exploit kits. Attack technology allows attacks to evolve from intrusive to disruptive to destructive.	High
Intent	Increasing	Increase in hybrid attacks using a combination of physical and technical penetration. State sponsored actors using cyber network attack on commercial targets to influence foreign policy. Organised criminal syndicates are becoming increasingly industrialised and effective.	High
Opportunity	Increasing	The digitalisation of the economy, reflected by the migration of commercial and government services to the Internet, combined with the rise in the use of mobile devices and services represents an increase in potential attack surfaces for cyber adversaries.	High

18 Standardising Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX), The Mitre Corporation. Barnum, Sean, 2012. http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf

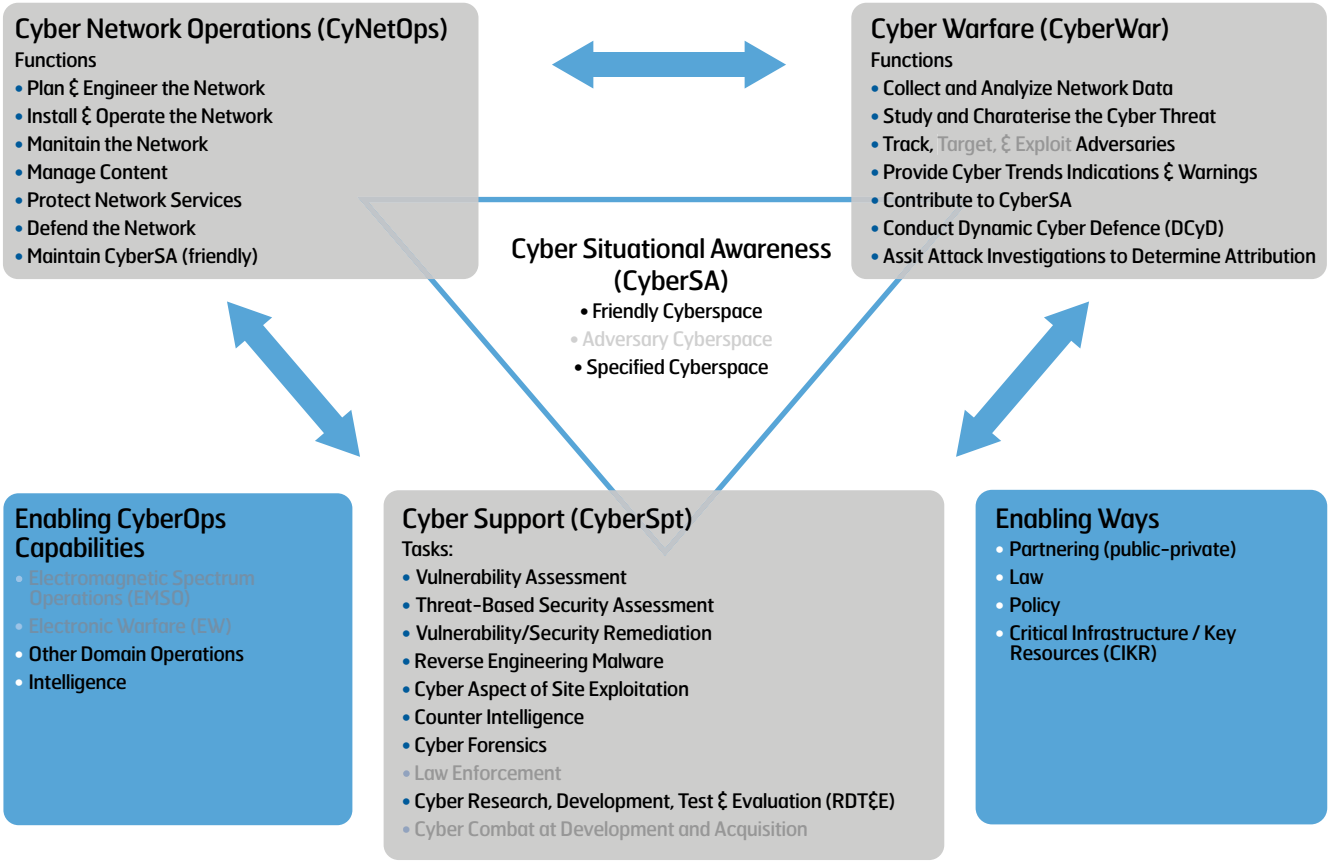
19 Transforming Expectations for Threat-Intelligence Sharing, EMC2 RSA Perspective, Moriarty K, August 2013. http://www.csoonline.com/article/745444/talk-of-cyberwarfare-meaningless-to-many-companies-experts-say

20 Talk of cyberwarfare meaningless to many companies, experts say, CSO, Gonsalves A, 6 Jan 2014. http://www.csoonline.com/article/745444/talk-of-cyberwarfare-meaningless-to-many-companies-experts-say

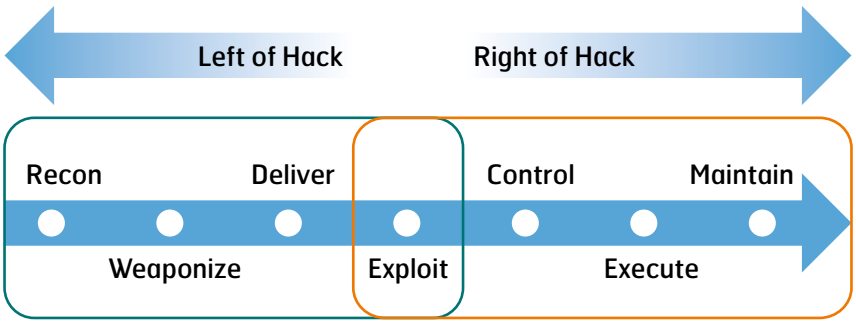
21 Cyberspace Operations Concept Capability Plan 2016-2028 dated 22 Feb 2010, TRADOC Pamphlet 525-7-8 http://www.fas.org/irp/doddir/army/pam525-7-8.pdf

Cyber Kill Chain

Banford et al (2011) expand the role of cyber threat intelligence in any decision support analysis by situating the impact in the action of cyber attack itself, quoting the seminal work of Hutchins et al[22] (2011), on the Cyber Kill Chain, which is itself derived from US Air Force Doctrine. Kill chain methodology models the phases of an attack in order to understand the potential for disruption or defeat of an adversary intervention against a network. The aim is to clearly identify the indicators and warnings of a cyber-attack in order to deploy appropriate counter measures to mitigate or limit the effect of the attack. This is known as "left of hack" (shown below, from Banford et al 2011).



US TRADOC Cyber Operations Model



The Lockheed Martin Cyber Kill Chain

22 Lockheed Martin Corporation: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Hutchins, Cloppert and Amin, dated Aug 2011. http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08/iciw2011.pdf

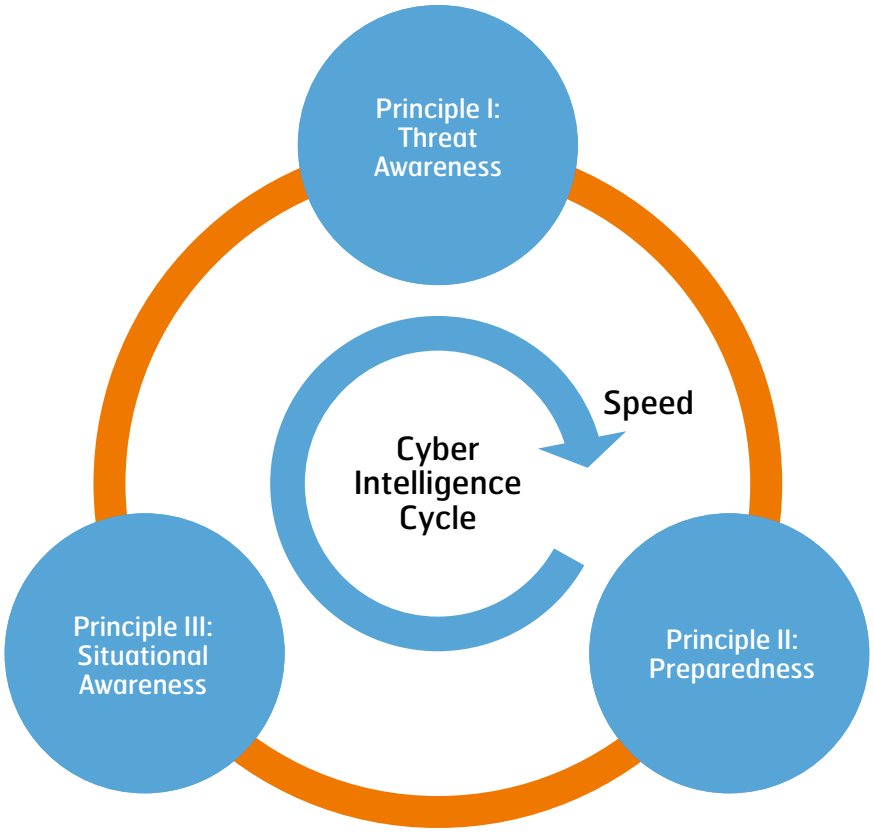
Reconnaissance	Research, identification and selection of targets, often represented as trawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on special technologies.
Weaponisation	Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponiser). Increasingly, client application data such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponised deliverable.
Delivery	The three most prevalent delivery vectors for weaponised payloads by APT actors, are email attachments, websites and USB removable media.
Exploitation	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
Installation	Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
Command and Control (C2)	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual
Actions on Objectives	Only now, after progressing through the preceding phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

Tactical, Operational and Strategic Cyber Intelligence

Bamford et al (2013) articulates the outputs for strategic, operational and tactical cyber threat intelligence citing examples (shown on the next page). This allows the scope of the output of any UK Banking and Payment Services cyber threat intelligence capability to be considered holistically to achieve a federated intelligence support capability to financial institutions, national and international cyber information exchanges. For the financial sector a strategic metric would be anomalous activity representing a breach in the confidentiality, integrity or availability of national or international payment systems because of the implications for the cohesion of wider system. Conversely, tactical intelligence indicators could be derived from technical log analysis using basic indicators.

Strategic	Operational	Tactical
• The decision by a competitor or potential competitor to enter your market space (e.g. a foreign competitor's new five-year plan now shows interest in developing a domestic capability in a technology your company is known for). • Indications that a competitor, or foreign government, may have previously acquired intellectual property via cyber exploitation. • Indications that a competitor, or foreign government, is establishing an atypical influential relationship with a portion of your supply chain. • Indications that your corporate strategic objectives may be threatened due to adversarial cyber activity.	• Trend analysis indicating the technical direction in which an adversary's capabilities are evolving. • Indications that an adversary has selected an avenue of approach for targeting your organisation. • Indications that an adversary is building capability to exploit a particular avenue of approach. • The revelation of adversary tactics, techniques, and procedures. • Understanding of the adversary operational cycle (i.e. decision making, acquisitions, command and control [C2] methods for both the technology and the personnel). • Technical, social, legal, financial, or other vulnerabilities that the adversary has. • Information that enables the defender to influence an adversary as they move through the kill chain.	• Host-based security system alerts. • Signature or behaviour detection efforts, and in advanced cases, some form of kill chain. • Analysis based upon known actors or network behavioural patterns.

Klaus (2013) infers a similar demarcation between the use of cyber threat intelligence in his description of a cyber-intelligence cycle, which would generate security intelligence. The emphasis of his model is the tempo of operations and the timeliness of dissemination of intelligence. The viability of real-time or near real-time tactical cyber threat intelligence, at an individual institutional level, would be greatly enhanced by greater situational awareness across the entire banking and payments system sector, which represents a single cohesive and inter-dependent target set to potential cyber attackers. In this way in can be seen the Klaus' (2013) Three Principles for Cyber threat intelligence (see overleaf) can be equated to Bamford's (2013) application of cyber threat intelligence. In this model it is considered that a UK Banking and Payments System cyber threat intelligence capability will initially focus on strategic and operational intelligence. This will augment the institutional cyber network defence intended to prevent and mitigate cyber network attacks in progress or detected by network intruder detection systems.



The Klaus (2013) 3 principles for Cyber Threat Intelligence

Cyber threat intelligence combines the strategic intelligence of understanding and preparing for threats (Principles I and II) with the tactical intelligence of responding to dynamic threat situations (Principle III).

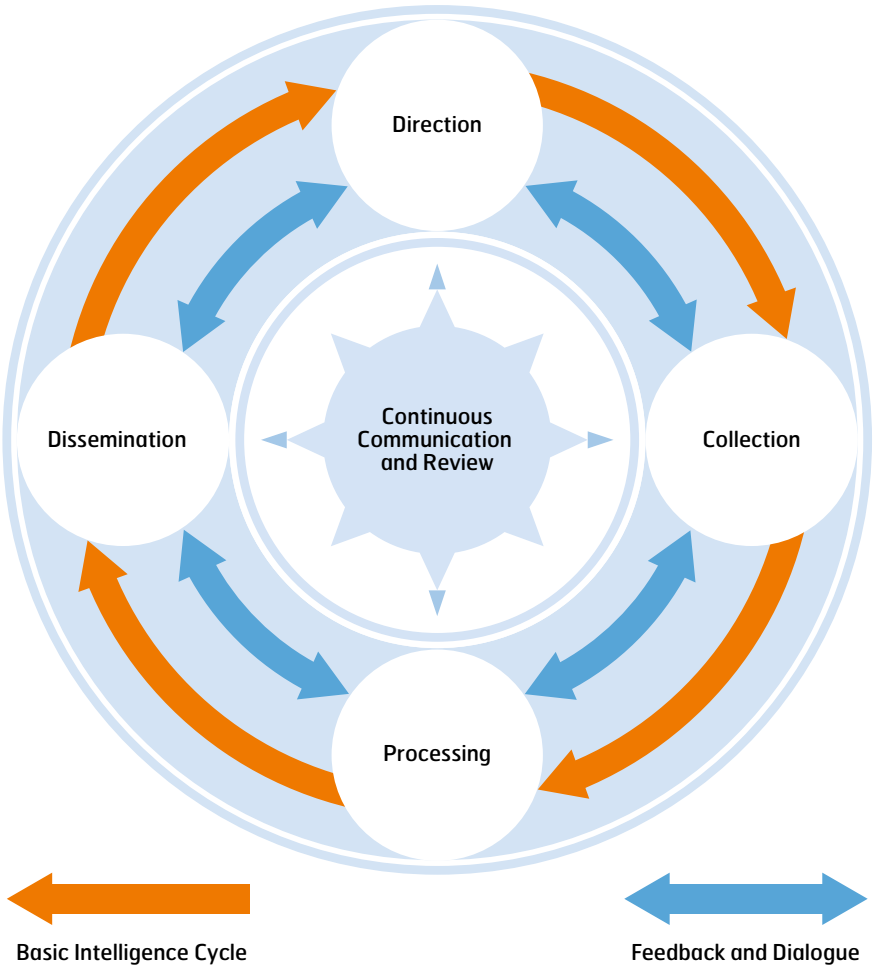
Both the intelligence cycle and the term "understanding" need to be clearly defined in order to comprehend the components of cyber threat intelligence and set the terms of reference for any UK Banking and Payment Services intelligence capability.

The Intelligence Cycle

The intelligence cycle is defined by the UK MoD[23] (Third edition, 2011) as Direction, Collection, Processing and Dissemination (DCPD). The DCPD, or intelligence, cycle is widely understood in the UK, US and Europe as a systematic methodology to conduct intelligence collection, analysis and reporting. Once seen as a cyclic process (shown in orange) it is now recognised to that feedback and re-assessment at every stage (shown in blue) increases flexibility and agility. Therefore a cyber threat intelligence cycle is articulated by the blue lines. This is the central mechanism for operational and strategic collection and analysis. Tactical intelligence threat reporting may require a less integrated approach in the first instance in order to publish threat warnings that should subsequently be confirmed by more considered and multi-source intelligence analysis.

The cyber threat intelligence cycle will now be considered in detail.

23 Joint Defence Publication 2.00 Understanding ξ Intelligence Support to Joint Operations, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33704/20110830JDP2003rdEDweb.pdf

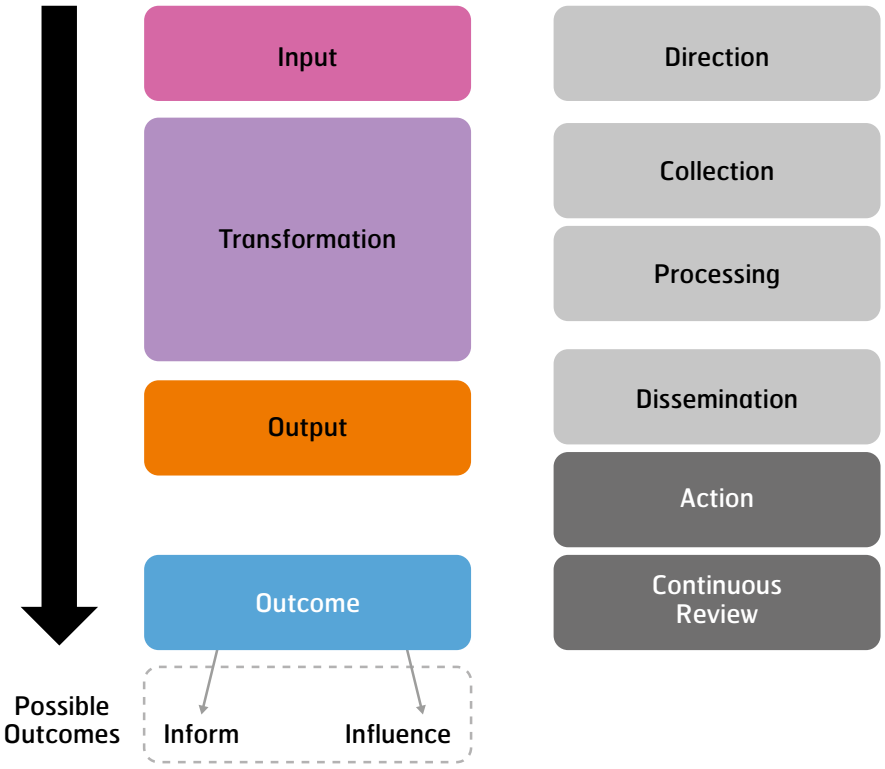


The intelligence cycle

Direction

Direction refers to the leadership decision of collection and analysis priorities, which draws out a key operating concept of any UK Banking and Payment Services cyber threat intelligence capability, operated for the benefit of member institutions. Tactical and operational direction can be an internal tasking of the cyber threat intelligence capability, but external strategic and some operational taskings should be directed externally and represented in a formal Intelligence Collection Plan (ICP). Therefore an oversight steering committee of representatives appointed by member institutions will be required to ensure the intelligence remains relevant to the strategic security environment of members and the wider threat spectrum affecting UK Banking and Payment Services. Ownership and control of the intelligence capability ensures responsiveness and accountability are embedded as central operating features. In this way federated analytical resource is tasked against documented priority intelligence requirement (PIRs) agreed by C-level and senior security managers within the UK Banking and Payment Services sector.

When the intelligence cycle is aligned to process theory (see overleaf, UK MOD, 2011) the outputs and limits of exploitation of cyber threat intelligence for the UK financial sector become evident. Cyber threat intelligence will inform and influence the development of corporate or institutional cyber security strategy and policy.



The intelligence cycle aligned to process theory

Collection

In this proposal the primary inputs, or collection, to a UK financial sector intelligence capability would be provided by member institutions according to their risk appetite. Each institution would moderate the level of detail by redaction before publication. Albeit, to an agreed minimum standard to ensure that all data inputs contribute to the Common Operating Picture (COP). It is considered that a founding principle of any UK Banking or Payments Service cyber threat intelligence capability is the anonymity of all member data inputs to encourage the least redaction as possible in order to derive the most detailed situational awareness across the industry. The aggregation of individual institutional data will produce a Common Operating Picture (COP) for cyber security threat landscape for each threat landscape; investment, corporate and retail businesses. Even without any further analysis or data enrichment this would represent a considerable capability increase for each individual financial institution. It would also enhance the input to the Cyber Information Sharing Partnership (CISP) by providing an industry view of the cyber operating environment that can be analysed against other sector COPs to derive indicators and warnings of sophisticated attack Techniques, Tactics and Procedures (TTPs) across target sets.

Standard Technical Reports Using Modules (STRUM)

Collection can be further enhanced by establishing a Standard Technical Report Using Modules (STRUM) that allows auto entity extraction at the point of collection and analysis. Extrapolating this methodology to cyber threat intelligence and security applications is considered a cornerstone of cyber threat intelligence capability development.

Anomaly detection reporting can be automated. When the institution's cyber network defences encounter anomalous activity the cyber threat intelligence messages could be sent to both the intelligence capability and partner institutions. This allows cyber defence protocols and postures to mitigate CNA TTPs before activation. This includes those anomalous intrusions detected and defeated by cyber network defences, known as decline data, which constitutes a resource that contributes to the Common Operating Picture (COP). STRUM facilitates technical inter-operability between sectors and information sharing forums. Categorisation also allows security managers to visualise the threat spectrum more systematically than current practices of exchanging cyber network attack experiences anecdotally. There are currently a number of established STRUM formats operating within the cyber security industry.

Processing

High volumes of technical data both requires and lends itself to data fusion management software, known colloquially as Search, Visualisation and Analysis (SV£A) tools. These sophisticated applications assimilate

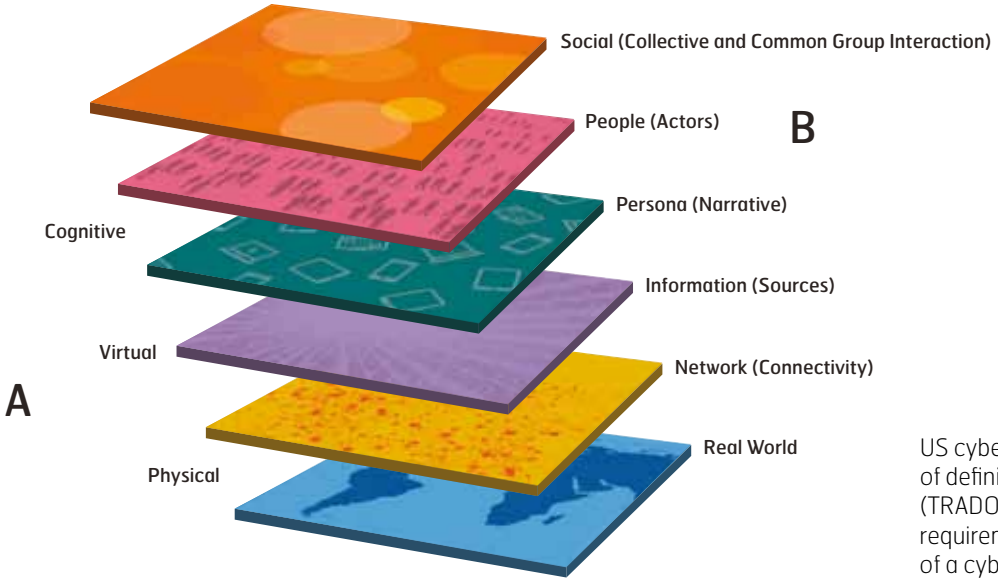
both structured and unstructured data and by meta-tagging all the essential elements of information (EEIs) of a data packet, discarding any formatting from subsequent analysis. This allows each element of a complex scenario of interconnected, inter-related and inter-dependent variables to be considered from either a single user defined start point or a parameter not initially evident from the data alone.
These applications are not a replacement for professionally trained, educated and experienced analytical staff. However, the right application can significantly leverage the skills of a single analyst to provide comprehensive breadth and depth on subject areas previously served by a whole team. Therefore the right data fusion management software is essential to the success of any Banking and Payment Services cyber threat intelligence capability.

Two key outputs, fundamental to achieving a common operating picture (COP) of cyber attacks and anomalous activity across the Banking and Payment Services can be achieved from SV€A analysis of data alone. The first is an Electronic Pattern or Life (EPoL) that demonstrates the peaks and troughs of activity on different networks.
The second is Electronic Finger Printing (EFP) that provides details of the techniques, tactics and procedures (TTPs) that aggressors are using to gain access to financial networks.
Therefore the attack data submitted into a single secure environment is absolutely vital to achieving predictive intelligence, providing insight and foresight of cyber network attacks and promoting understanding of the cyber threat spectrum. This aggregation of data, or "data lake", represents a high value target for cyber attackers, so security of the data is a key planning and operational consideration.

The outputs of this process will be both positive and negative. Technical data alone does not represent a panacea for all cyber security issues. There will be occasions when access to a target network has been achieved without any anomalous technical indication until the attack profile actually commences. For example when social engineering or an insider threat facilitated access to the target.

Search, Visualisation and Analysis (SV€A)

Search, Visualisation and Analysis (SV€A) tools have their origins in law enforcement and intelligence agencies. They have been heavily utilised to understand and exploit terrorist and insurgent networks which share characteristics with covert and clandestine cyber network attack threat networks. They provide an excellent medium to correlate inputs from the cognitive, virtual and physical domain (A) into outputs (B) (JDP 04, 2010) that can develop actionable security intelligence for UK Banking and Payment Services security leaders and managers or investigatory start points for law enforcement or security and intelligence agencies.



UK MOD View of the Operational Environment

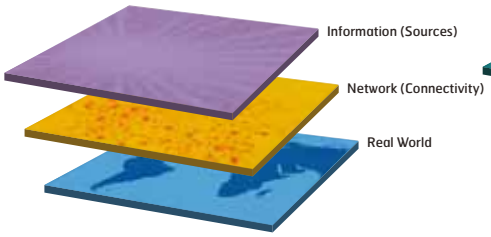
US cyber doctrine takes a similar view of defining cyber space in three layers (TRADOC, 2010[24]) which emphasises the requirement for the analytical engine of a cyber threat intelligence capability to be configurable to include these parameters.

Physical Layer

Geographic Components

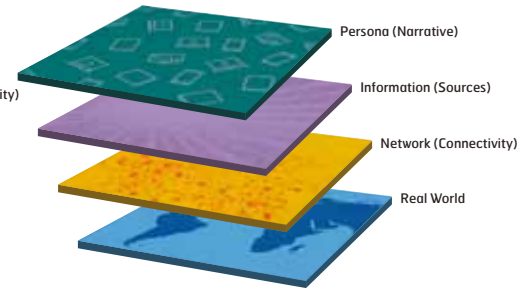
Logical Layer

Logical Network

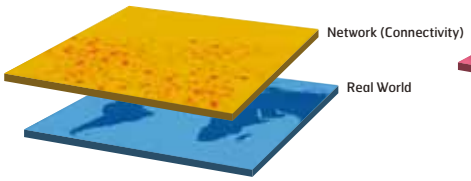


Social Layer

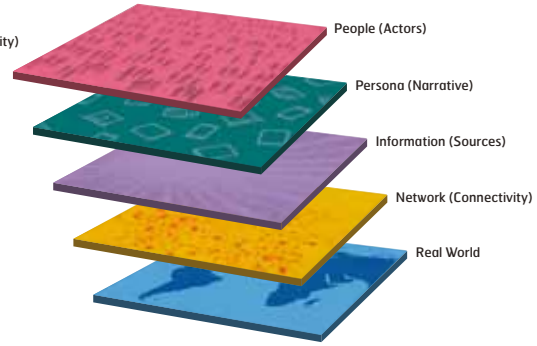
Persona Components



Physical Network Components

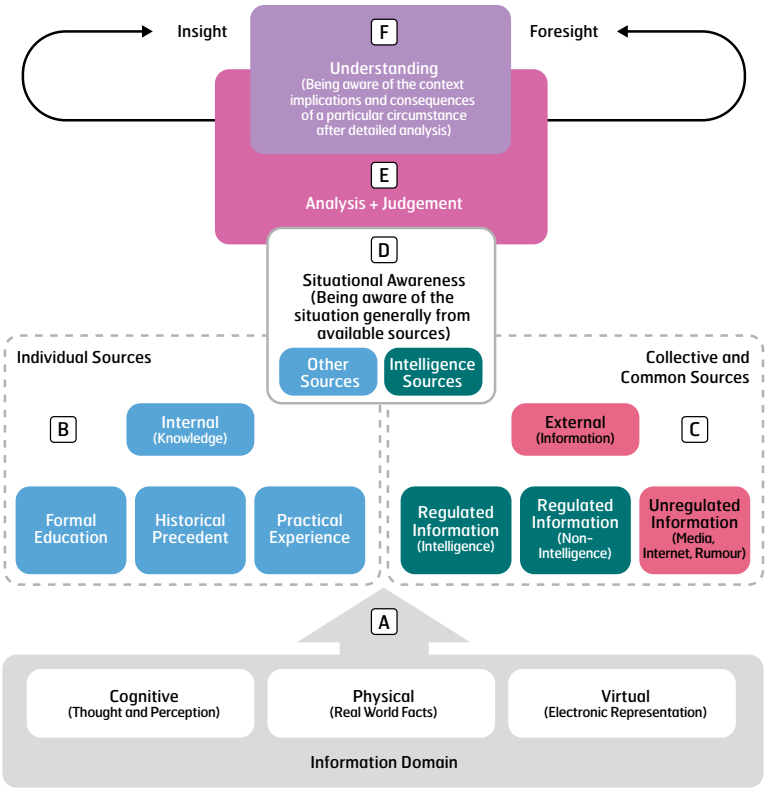


Cyber Persona Components



US TRADOC view of the operational environment

24 Cyberspace Operations Concept Capability Plan 2016-2028 dated 22 Feb 2010, TRADOC Pamphlet 525-7-8 http://www.fas.org/irp/doddir/army/pam525-7-8.pdf



The components and prerequisites of understanding

These applications accelerate the acquisition of situational awareness, but understanding remains the preserve of analysts, intelligence managers and key decision makers in security leadership functions.

Situational Awareness ₹ Understanding

The UK MOD[25] (2010) defines the cognitive state produced from the fusion of situational awareness (the COP) and analysis (electronic pattern of life and TTPs) as comprehension (shown below), leading to insight. Foresight would be provided by comprehension and judgment, but judgment will only be informed after a volume of analysis has proved accurate and reliable. For this proposal **A** is would be the open sources and media available to both member institutions and an UK Banking and Payment Services cyber threat intelligence capability. **B** represents the resources available to individual financial institutions, which will vary in maturity dependent on the sophistication of institutional network monitoring and analysis. **C** represents the federated intelligence capability, operated for the UK Banking and Payment Services sector. This entity should provide foresight and decision support analysis for security management at an individual institutional level.

Phases **D,E,F** occur both concurrently and simultaneously in the intelligence capability and in each institutional security intelligence capability. It is assessed that the current forums and information exchanges, both closed and open, provide data of sufficient granularity to only achieve Situational Awareness (SA). Whilst individual institutions may have sufficient resource to achieve understanding this is not possible across the UK Banking and Payment Services sector within current resourcing and structures.

Aggregated data for all contributing financial institutions would be the basis of trend and characteristic analysis. Over time this will allow a detailed electronic Pattern of Life (ePoL) to be collated for cyber attacks against UK financial targets. Similarly Tactics, Techniques and Procedures (TTPs) of cyber attacks can be compiled, even from fragmentary surveillance of cyber intrusions and attacks, by aggregating types of attack. This will develop a database of attack characteristics or Electronic Finger Printing (EFP) of cyber network attack actors and networks.

The predicative element can be achieved by correlating attack profiles with open source monitoring that may provide Indicators and Warnings (I₹W) of the collaboration, organisation and co-ordination necessary for some forms of sophisticated cyber network attack (CNA).

25 Joint Defence Publication 04: Understanding, dated Dec 2010.

Principles of Intelligence

This analysis of processing should be conducted within the established principles of intelligence, which JDP 2.00[26] defines as:

Command led	An inherent command responsibility: commanders provide the direction, resource the capability and create the right command climate.
Objectivity	Intelligence must be unbiased, undistorted, intellectually honest and free of prejudice.
Perspective	Get inside the mindset of the key actors, particularly adversaries; try to think like them.
Agility	Look ahead, identify threats and opportunities, develop the flexibility to react to changing situations and be ready to exploit opportunities as they arise. Agility is not about absolute speed: it is an ability to exploit information in context at the right tempo.
Timeliness	Providing intelligence on time, even if incomplete, to enable commanders to make decisions at a pace that maintains the initiative.
Collaboration	A duty to share as well as to protect.
Continuity	Develop and retain subject matter expertise.
Collaboration	Security must permeate the entire intelligence enterprise, but should balance the need to share with the need to protect people and plans.

These principles resonate with the experience of commercial intelligence support. Verisign offer the CROSSCAT-V model as guidance for establishing a Formal Cyber Threat Intelligence capability[27]:

- **Centralised Control:** A single point of control for intelligence team simplifies interactions and eliminates duplication of effort.
- **Responsiveness:** The team must answer the question the customer asked, not the question the intelligence team wishes to answer.
- **Objectivity:** An intelligence team should not pick sides, no matter how emotive a subject.
- **Source and Methods Protection:** Sources of information (both human and non-human), an organization's technical capabilities and its operational methodologies are the lifeblood of an intelligence team and must be protected.
- **Systematic Exploitation:** Intelligence is a methodological practice of research and review, using multiple sources and agencies.
- **Continuous Review:** Intelligence has a shelf life, and the intelligence team must carry out a periodic review of their product to ensure it remains relevant.
- **Accessibility:** An intelligence team must constantly balance the risk of its product falling into the wrong hands with the need for the customer to access that product.
- **Timeliness:** Delivering intelligence products to customers in a timely fashion is central to the intelligence function.
- **Vision:** The intelligence team must consider possibilities that are not immediately obvious. Often, the vision of an intelligence analyst, combined with the moral courage to voice an unconventional theory in an open forum, can make the difference between operational failure and mission success.

26 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33704/20110830JDP2003rdEDweb.pdf
27 https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf

Suitably Qualified and Experienced Personnel (SQEP)

The selection of Suitably Qualified and Experienced Personnel (SQEP) should not necessarily be limited to those with formal training and experience of intelligence or law enforcement. It is considered that the following skillsets constitute an appropriate combination of skills for a cyber threat intelligence team:

a. Intelligence management and leadership.

b. Data Science and Statistical Analytics.

c. Fraud Investigation.

d. IT Network Engineering.

e. Intelligence Analysis.

f. Software coder (Malware and AV)

The desirability to incorporate UK protectively marked, or classified, material into the analysis processing function may place constraints on the selection and employment of personnel, due to the inherent requirement to be suitable for security vetting as a UK national.

Dissemination

The inherent characteristics of Dissemination, the requirement to be timely and accurate, are particularly demanding in the cyber domain. At full operational capability (FOC[28]) a UK Banking and Payment Services cyber threat intelligence capability should aspire to near real time reporting and automated indicators and warnings (I₤W) of CNA against member institutions, who would contribute both data and funding. However, informal stakeholders including, but not limited to; Bank Of England (BoE), Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA) and other information sharing forums have an important role as collectors and customers of cyber threat intelligence products.

Arguably the driver that undermines current Computer Network Defence (CND) as an security strategy is detention. Therefore a major output of an intelligence led cyber security strategy must be to reinforce the detention effect. Consequently the continuity and integrity of intelligence, derived from the standardised and codified data inputs from financial institutions is a key measure of performance for a cyber threat intelligence capability. A key measure of effectiveness is the productive liaison with law enforcement to prosecute targets identified by cyber threat intelligence.

Conclusion

Industry and academic research presents a considerable body of analysis which indicates that the evolution of the cyber network attack threat now requires an intelligence led cyber security strategy to mitigate highly sophisticated cyber network attacks. This threat represents a strategic risk with potential to cause significant reputational damage and cause a major outage of cyber resilience across banking and payments systems. Previously the business case for a collaborative, federated cyber threat intelligence capability may have been opaque to individual institutions. This research underlines that high impact events and the inherent reputational risk they represent can no longer be dismissed as low probability. This is evidenced by the proliferation of vendor cyber threat intelligence services including security operations room, offering real-time and near real-time monitoring and reporting of cyber threats, proving that a business case exists, amongst a client base for which there is an operational requirement.

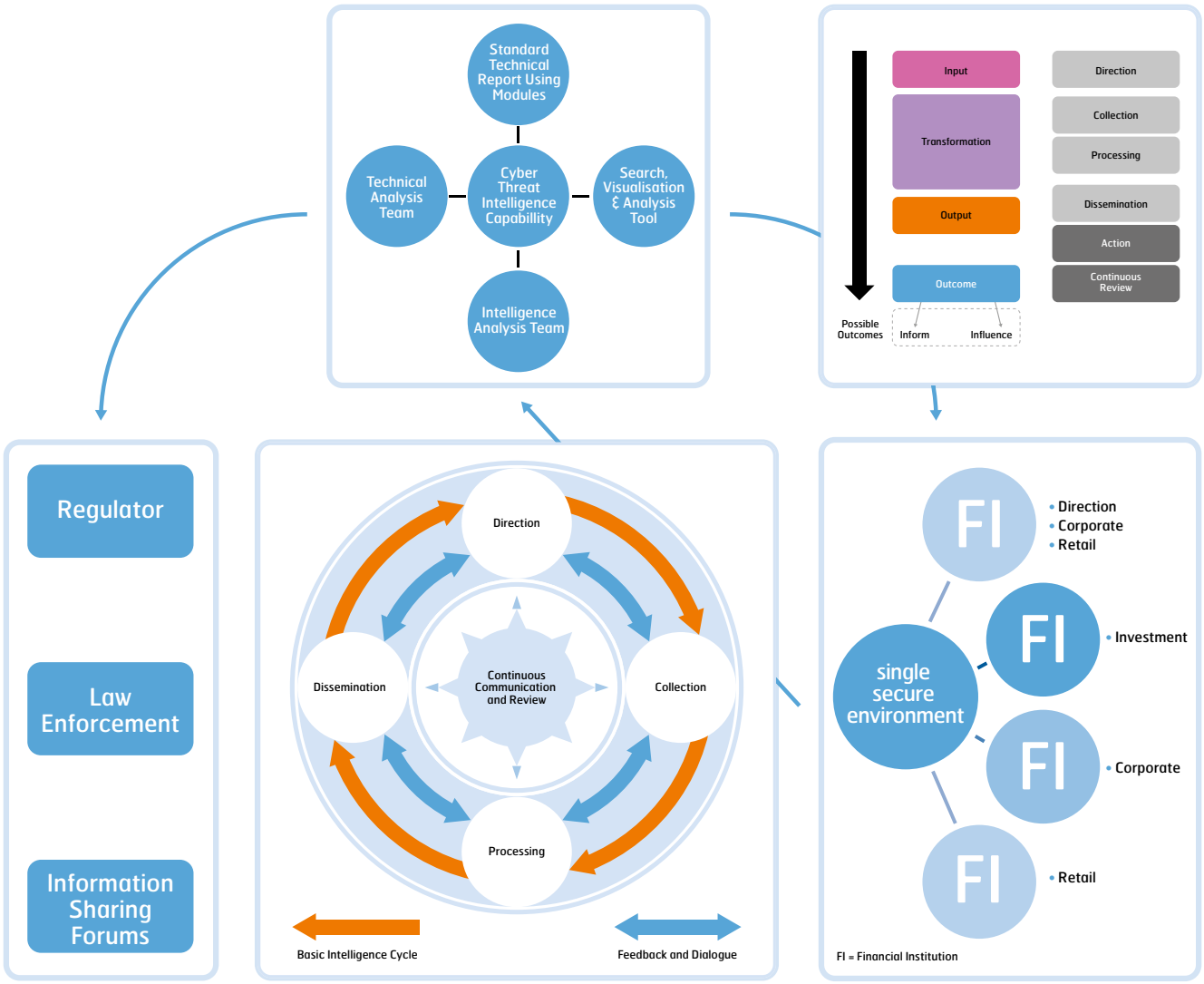
Cyber threat intelligence is not just a concept. It is a method of improving cyber security that has been proven in other sectors and other Banking and Payment Services markets. The US experience of a sustained state sponsored cyber network attack offers an insight into the future evolution of the threat. A cyber threat intelligence capability will provide actionable intelligence of insight and foresight that allows security managers to prioritise security measures according to the prevalent threats thereby increasing individual and collective resilience.

28 Implementation phases are considered to be: 1 Research and Proposal. 2 Scoping and Support. 3 Concept Capability Demonstrator (CCD). 4 Initial Operating Capability (IOC). 5. Full Operating Capability (FOC).

Section 4.0

Technical Appendices

Principles and Concepts



The fundamental principle of any UK Banking and Payment Services cyber threat intelligence capability is the requirement of the fullest disclosure possible of cyber network attack indicators from financial institutions. Therefore the data feeds (identified attacks, anomalous and decline data) from contributing and member institutions must be anonymised to achieve systematic collection of systemic data from which an electronic pattern of life of attacks and electronic finger printing of the modus operandi of those attacks can be achieved.

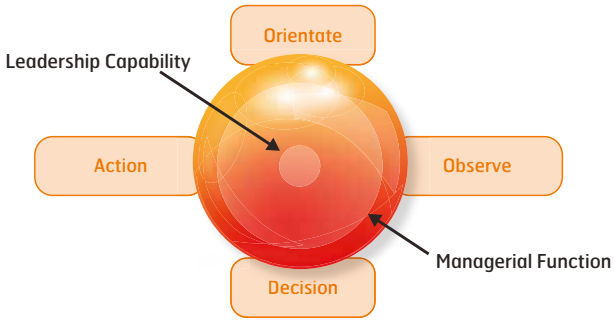
Collection is enhanced by using standard and interoperable formats such as STIX and TAXII. Moreover feeds should be distinguished to target activity to discern specific attack profiles for investment, corporate and retail banking operations.

Strategic and some operational intelligence collection requirements are directed by a managerial oversight committee to ensure appropriate direction is achieved and maintained in a formal intelligence collection plan. Agility and flexibility are maintained by the discretion of the intelligence collection manager to develop intelligence by prioritising threat indicators.

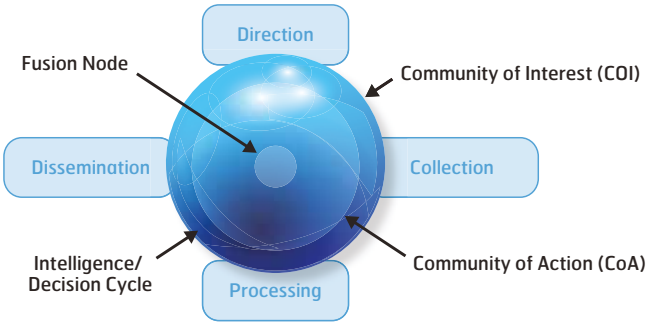
Processing is achieved in a single secure environment by using data management fusion software, known as search visualisation and analysis tools, to provide a graphic representation of the cyber common operating picture and detailed technique, tactic and procedure analysis of high threat, new or novel attack profiles.

Fusion Node Network

Fusion nodes, whether for information sharing or intelligence production, are formed of several components. The basis of existence is a community of interest that is usually issue or subject specific. The more active members of that group form a community of action which directs and manages the outputs of a committee or staff that run the administration or core operational process of the fusion node. The larger the community of action the longer and less flexible the decision cycle (Orientate, Observe, Decision, Act) or Intelligence cycle (DCPD) tends to be.

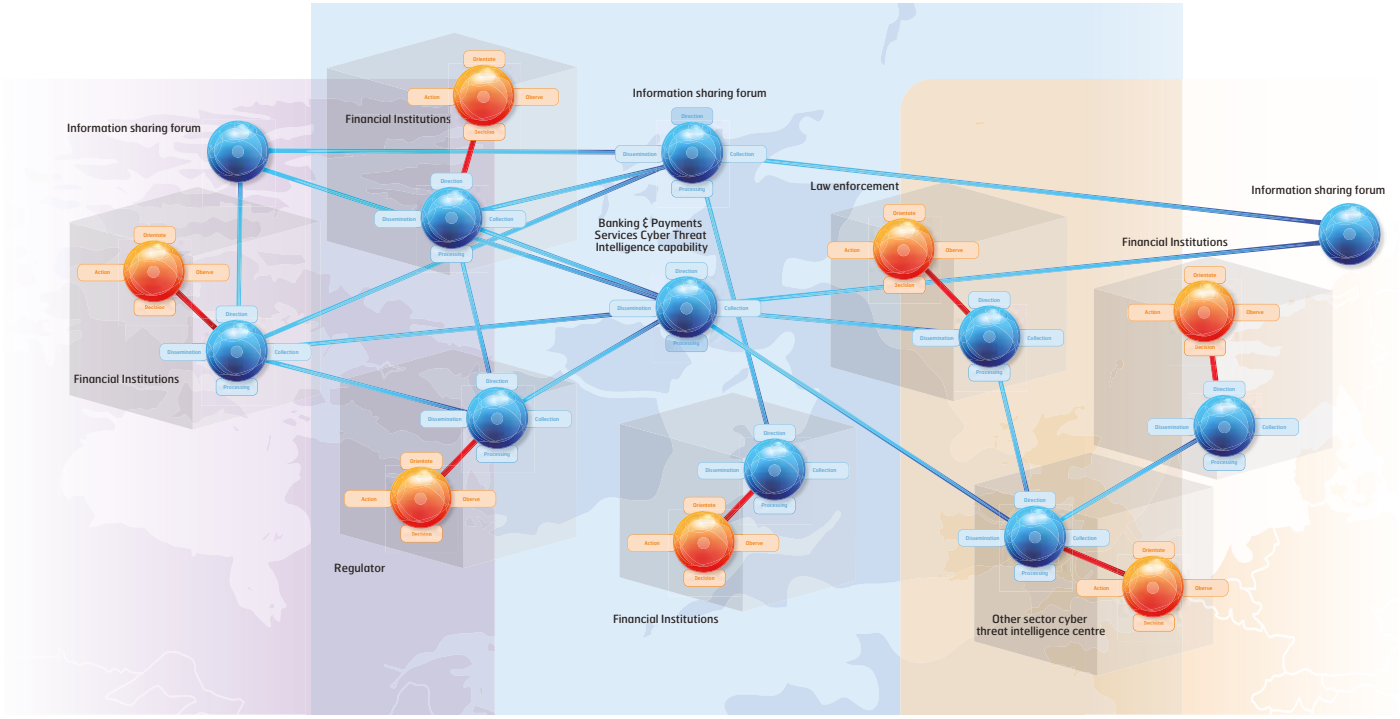


Key Decision Maker forum or Management Node



Intelligence Fusion Node or Decision Support Node

Therefore the tendency is to expand any subject specific fusion node to incorporate new stakeholder groups in a single entity. This reduces the tempo of operations and tends to produce homogenised intelligence by inadvertently imposing hierarchical structures over analytical rigour. Therefore a series of fusion nodes, each serving and closely aligned to decision makers provides an appropriate balance of tempo, decision support and peer review.



Intelligence fusion matrix

Area of Intelligence Interest (AOII) and Area of Interest Responsibility (AOIR)

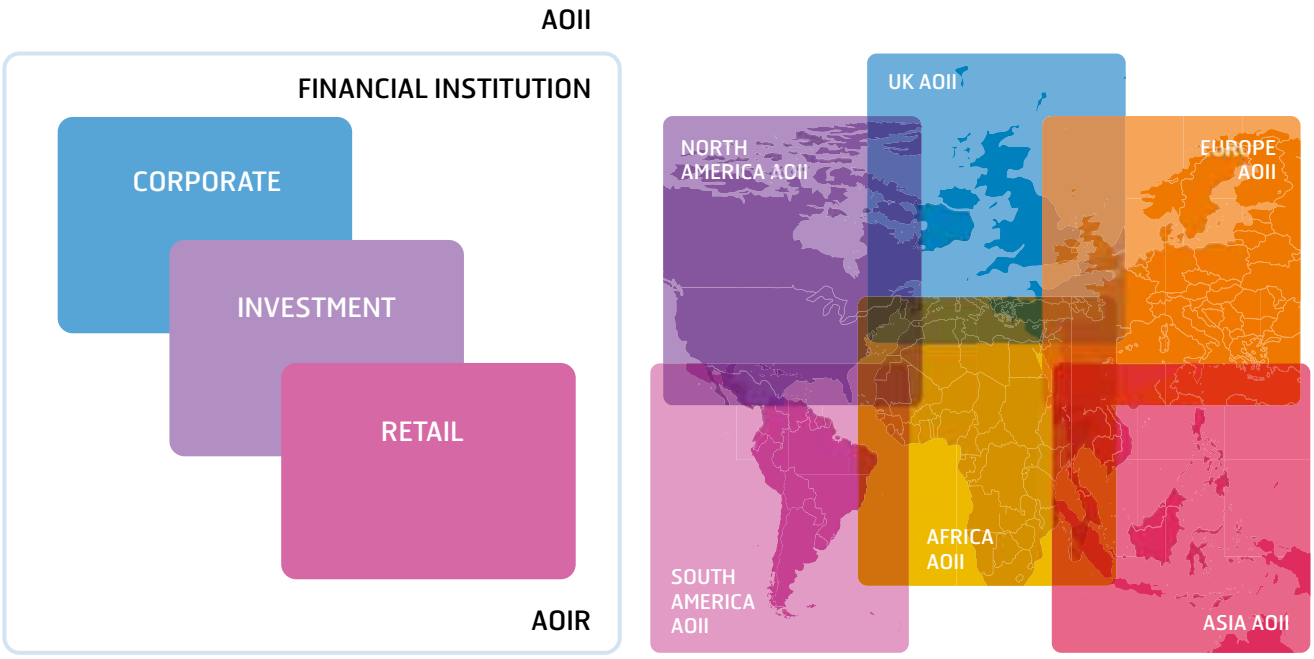
An Area of Intelligence Responsibility (AOIR) is that for which an entity is assigned control and required to collect intelligence and data that affords effective coverage of the activity of interest within that space. This is not necessarily total coverage, but should afford collection to achieve no less than the equivalent of Maturity Level 3 (see criminological appendix for full details), in order to be of intelligence value to other stakeholders.

If collection is conducted focused on the three specific target sets; Corporate, Investment and Retail banking then the "signal vs noise" separation an the processing stage is far easier to discern. This is a key feature of the CONcept of OPerationS (CONOPS).

In a cyber context institutions or payments system infrastructure providers "own" their networks and retain responsibility for monitoring and logging network traffic and identifying anomalous activity. The nature and characteristics of anomalous activity will vary according the threat actors intent and understanding of the targeted network.

From a threat centric perspective the time zone and geographic location of the target or target set is a discriminating factor. Timing of attacks against institutions and payments systems and the prevalence of the language of the business infrastructure are two rudimentary, but key influencing factors of target selection. Less obviously the effectiveness of legislation and law enforcement in an international context can also influence an aggressor's choice of target selection.

This may evolve as series of areas of intelligence interest for a trans-national financial institution with a spectrum of threats, within legislative frameworks with varying constraining or enabling characteristics, notably in the area of data protection. The primary value of the data and information derived in these sectors will be to serve the institution or payment system that collects it. However, increasing national and regional emphasis on cyber resilience may lead to a regulatory requirement to report externally. This level of reporting would represent a potential reputational risk factor.



Course of Action (COA) Analysis

A Course Of Action analysis considers six potential courses of action for the development of a cyber security capability. A planning assumption is that large trans-national financial institutions will have developed organic cyber security capabilities that include a technology led Computer Network Defence (CND) programme, a network surveillance capability and an internal security education and training regime. Some large corporations will also have a cyber threat intelligence function, principally focused on deriving intelligence value from internal network metrics, but also with an external focus on information sharing. Equally, the COAs have been considered for a small or medium sized financial institution that understands the value of a dynamic cyber security strategy, but whose economies of scale and resources preclude an intelligence led strategy using network surveillance data.

	Strengths	Weaknesses	Opportunities	Threats	Conclusion
Do Nothing	In an inter-dependent inter-connected Banking and Payment Services sector cyber security is a collaborative, not competitive discipline. Other entities and institutions may provide support in their best interests.	Reputational risk in the event of a cyber attack is high.	Reduces costs of cyber defence to the minimum required for pragmatic cyber hygiene in accordance with national and international standards.	The regulator and partner organisations may consider this an irresponsible security posture because it effectively transfers security risks.	More likely to be associated with new or small financial institutions that lack the resource or depth of subject matter expertise to engage in a complex and dynamic threat environment. (Maturity Level 1)
Invest in Computer Network Defence	Continues to build upon cyber network defence strategies to mitigate low and medium level threats. Therefore coverage of high probability and low impact cyber network attacks is achieved.	No coverage afforded for the low probability, high impact attack, which will increase in likelihood as CNA capability increases.	No development risk for a new capability and no reputational risk of being associated with a new strategic direction. Potential to adopt emerging polymorphic defence technologies and increase effectiveness of CND.	Discounts the Kuhnian paradigm shift requirement and does not acknowledge that cyber network attack outpacing the evolution of cyber network defence.	Medium and large financial institutions with bespoke and technically proficient cyber security capabilities may consider this course of action represents best return on investment with the least reputational risk if their own analysis does not identify increasing capability and capacity of the cyber threat. (Maturity Level 2)
Invest in Information Sharing Forums	Broadens the community of like-minded security practitioners to achieve a trip wire situational awareness of "zero day" or advance persistent threats.	Unlikely to produce data of sufficient granularity, quality with known provenance, context and pedigree to achieve intelligence led cyber security.	Excellent forums to establish bi-lateral and multi-lateral links to develop cyber security training and education to improve professionalism of cyber security management and practitioners.	Not all financial institutions have sufficient reputational risk appetite to participate or release data of sufficient detail in these forums.	Information exchange is a vital component of an intelligence led cyber security strategy, but any insight and foresight that is achieved is difficult to quantify or rely upon. (Maturity Level 3)
Subscribe to a Vendor service	Accesses suitable subject matter expertise and the nexus peer effect of other institutions and other sector data to achieve a rapid "lessons identified" or "lessons learnt" led capability evolution.	Unlikely to be wholly focused on the UK Banking and Payment Services sector, therefore a low signal, high noise common operating picture is produced.	Allows a cyber security capability to be established rapidly, including the network surveillance capability required to collect data.	Vendor client cost spiral and reliance of an external supplier for a banking essential service, security. Likely to only ever receive an 80/20% return on data provided.	A useful strategy to rapidly acquire a cyber security capability and create systematic surveillance of CNA systemic indicators and warnings.
Invest in CPNI	Backed by HMG and enjoys the support of the Security and Intelligence Agencies with well established and comprehensive protocols for information sharing.	A very broad client base and therefore inevitable inertia to build up to a cyber threat intelligence capability.	A well resourced and objective information sharing portal. Potential forum to develop and accommodate a Banking and Payment Services cyber threat intelligence capability.	Non anonymised feeds prevents some financial institutions fully participating. Absence of ownership may preclude capability development at best speed. Transparency to financial regulators may also preclude full and frank member disclosure required to achieve a COP.	A key initiative to address the Kuhnian turning point in the cyber security industry. Developing all the time, but potentially not configured to support or develop a cyber threat intelligence capability. (Maturity Level 4)
Establish a UK Banking and Payment Services Cyber threat intelligence capability	Acknowledges the increased threat (capability+intent+ opportunity) of Computer Network Attack and provides a mechanism to increase productive law enforcement liaison. Builds wider threat awareness within the Banking and Payment Services sector.	Unproven capability that may not meet stakeholder expectations or operational requirements. Not every potential contributor or member has sufficient CIS infrastructure to participate.	Potential to build a cost effective and efficient collaborative and federated cyber threat intelligence capability using data not otherwise available to individual institutions and achieve a return on investment that cannot be matched by an internal focus.	Theoretical only at this stage albeit similar "SOC in a box" services are available from vendors. A concept capability demonstrator, then an initial operating capability have to first be designed and developed until a full operational capability can meet near real time reporting of a common operating picture for cyber attacks against the UK Banking and Payment Services sector. Therefore an 18 month lead time seems a pragmatic expectation.	The principle of collaboration to achieve sufficient defence mitigation from emerging cyber network attack threats is widely understood. The differences between information, data, analytics, intelligence and evidence are not. In an industry suffering from "initiative fatigue" and "strategy by the school of good ideas" potential benefits are by no means self-evident.

Each area is now graded by the perceived risks shown as red (severe), amber (moderate) and green (manageable). It is very easy to see that in terms of risk the "Do Nothing", laissez-faire approach sits firmly at one end of the spectrum and UK Banking and Payment Services cyber threat intelligence capability sits at the other. This is a valid perspective at the current time for both enthusiasts and critics of an intelligence led, threat centric approach to cyber security. However, when considered within the strategic environment of increasing Computer Network Attack capability out pacing Computer Network Defence capability a sense of urgency may incline critics to accept the risks of development to re-acquire current levels of threat mitigation.

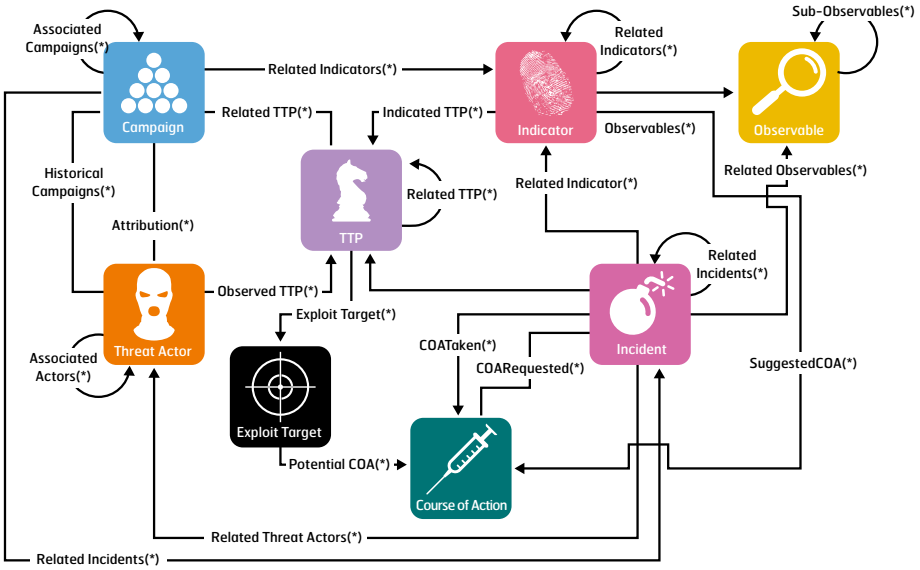
	Strengths	Weaknesses	Opportunities	Threats	Conclusion
Do Nothing	Minor financial institutions may escape the attentions of CNA threat networks.	The BoE cyber security scheme will soon detect financial institutions with sub-optimal cyber security.	Larger financial institutions may develop capabilities that will improve individual resilience and security.	A zero day (low probability, high impact) attack could cause irreparable reputational risk.	Not feasible in the long run, potentially understandable in the short term for small or new institutions. Nonetheless likely to lead to a CNA honey pot feeding frenzy when discovered.
Invest in Computer Network Defence	Little reputational risk, but little additional return on investment.	Passive and static defences will be breached over time.	Well established funding lines for further capability development.	The risk of being the "odd man out" if a collaborative and federated cyber threat intelligence capability gains traction.	The path of least resistance, but static, passive defence is not the basis for a strategic line of development.
Invest in Information Sharing Forums	Some information exchanges are very professionally administered and managed and provide excellent resources to increase training and education levels.	Information is not intelligence and therefore security management intuition and judgement remains the key driver for cyber security capability development.	Information exchange is a key drive of a collaborative strategy. Therefore individual membership of suitable forums is a valuable investment for an active cyber security posture.	Reliance of information alone may create a parallax to intelligence led situational awareness and contribute to cognitive dissonance that no further change is security posture is necessary.	A vital component on an intelligence led, threat centric, cyber security strategy, but not sufficient to meet the operational requirement and defeat high end threats.
Subscribe to a Vendor service	Potential to achieve blue chip insight and foresight of general cyber threats.	Cost of the vendor-client cost spiral and perpetuating a supply chain relationship for a core process of Banking and Payment Services transactions.	Quick way to establish a competent maturity model.	May be insufficient for the board to have true ownership of cyber security	An alternative to owning an organic cyber security capability if cost base precludes investment in the right infrastructure and expertise, but not as responsive as the threat seems to require.
Invest in CPNI	Secure, well managed, HMG backed, gaining wider acceptance and participation.	Broad client base across all sectors can dilute the signal in the noise of non-relevant cyber attacks.	The CPNI closed cells could be developed into a Banking and Payment Services specific cyber threat intelligence capability with access to public domain protectively marked intelligence.	Command and control, the Direction of the intelligence cycle, is outside individual or collective control. This might be at the expense of Banking and Payment Services priorities in favour of security and intelligence agency development against cyber network attack targets.	Another key component of a collaborative, intelligence led, threat centric cyber security strategy. It meets some, not all of the objectives of a cyber threat intelligence capability
Establish a UK Banking and Payment Services Cyber threat intelligence capability	Will provide a common operating picture for investment, corporate and retail banking operations at full operational capability that will detect sustained cyber network attack campaigns including advance persistent and insider threats.	New, novel approach with multiple stakeholders could complicate and elongate the route to market.	The potential to develop a world class collaborative and federated capability that represents a means to maintain the competitive edge of Banking and Payment Services in the global markets.	Another initiative at the back of a very long queue that may be eclipsed by legislatively mandated external funding requirements individual financial institutions feel are more pressing.	Initial indications are that elements of the market are pressing for such a capability with hopeful optimism; others are justifiably sceptical until they are presented with compelling data and intelligence for the requirement.

In summary the development of a cyber threat intelligence capability, which seems a leap of faith to some now, will be self-evident in 12 to 24 months. The modus operandi of Financial Fraud Action UK (FFA UK), the secure server and infrastructure and the jointly funded industry and Metropolitan Police Service (MPS) Dedicated Cheque and Plastic Crime Unit (DCPCU) offers an insight for a future development avenue for a collaborative and federated cyber threat intelligence capability.

Standardised Report Formats

Standard Technical Reports Using Modules (STRUM) will be a key feature of a Cyber Threat Intelligence capability by facilitating semi or full automation of attack or anomalous activity reporting. This will be required in order to achieve timely indicators and warnings to supported financial institutions.

This appendix details some of the key research on STRUM formats and makes recommendations on a format that could be adopted.

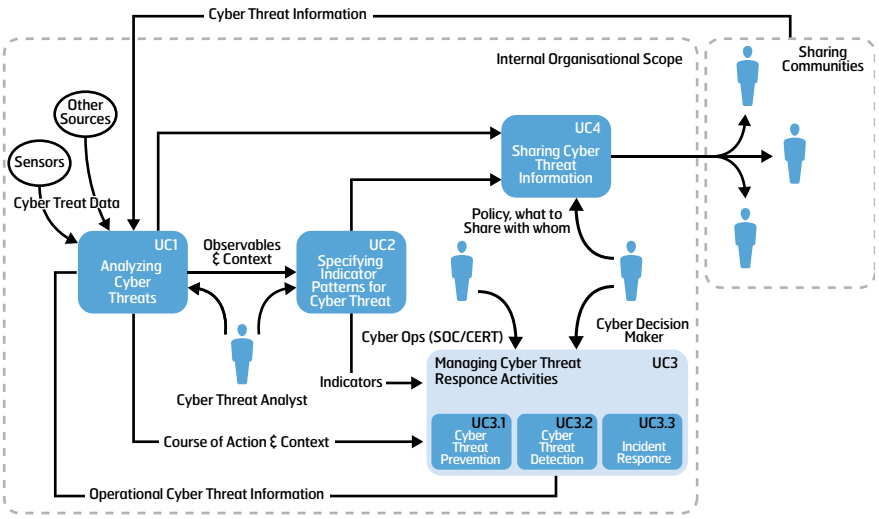


STIX architecture

Structured Threat Information Expression (STIX)[29]. STIX is a U.S. Department of Homeland Security (DHS) led initiative, established in 2012, of the office of Cyber Security and Communications. MITRE, operating as DHS's Federally funded research and development centre, manages the programme. This includes the STIX website, community engagement, and discussion lists to enable open and public collaboration with all stakeholders. This has led to the development of a standard lexicon and standard operating procedures (SOPs).The range variables within the STIX architecture is detailed overleaf. Banking and Payment Services-ISAC and CERT-EU use STIX and the obvious inter-operability between UK and US financial systems indicates that STIX represents a viable STRUM for the future development of a UK Banking and Payment Services cyber threat intelligence capability. Therefore it is a suitable standard for institutions lacking a network surveillance capability to use and the minimum output requirement, which in turn will allow the CNA attack data to be collected and processed by a UK Banking and Payment Services cyber threat intelligence capability.

MITRE provide an illustrative simplified example to demonstrate the utility within architecture and structure representative of the proposed Banking and Payment Services cyber threat intelligence capability and within wider information sharing forums. This underlines the key relationship between cyber intelligence nodes and cyber information sharing forums.

29 http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf



MITRE envisage that STIX will operate within the Trusted Automated eXchange of Indicator Information (TAXII)[30] protocols to ensure secure and timely threat intelligence collection and dissemination. Current work strands include services, message types, message exchanges, defined standards of network transportation and format bindings. The use of automated exchanges is designed to achieve near real time reporting.

STIX is by no means the only STRUM format operating within the market. The work of Hernandez-Ardieta[31] et al (2013) presents a mathematic model for information sharing. It also analyses MITRE's Making Security Measurable (MSM) initiative to compare STRUM standards and utility. Their findings are summarised below:

Core use targeted by STIX

	CPE	OVAL	SWID	XOCDF	CCE	OCIL	CCSS	CVE	CWE	CVSS	CAPEC	CVRF	MAEC	CybOX	IndEX	STIX	IODEF	CPE	CEE	RID	RID-T	CYBEX	CWSS
Asset Definition (Inventory)	■	■	■															■					
Configuration Guidance (Analysis)		■		■	■	■	■																
Vulnerability Alerts (Analysis)		■						■	■	■		■											
Threat Alerts (Analysis)								■	■	■	■		■	■	■	■	■		■	■	■		
Risk/ Attack Indicators (Intrusion)	■							■					■	■	■	■	■	■	■	■	■		
Incident Report (Management)	■	■			■			■	■	■			■		■	■	■			■	■	■	■

CPE Common Platform Enumeration
OVAL Open Vulnerability and Assessment Language
SWID Software Identification tags
OCIL Open Checklist Interactive Language
CCSS Configuration Scoring System
CVE Common Vulnerabilities and Exposures
CWE Common Weaknesses Enumeration
CVSS Common Vulnerability Scoring System
CAPEC Common Attack Pattern Enumeration and Classification
CVRF Common Frameworks for Vulnerability Disclosure & Response
MAEC Malware Attribute Enumeration and Characterisation
CybOX Cyber Observable Expression
IndEX Individual Event eXpression
STIX Structured Threat Information Expression
IODEF Incident Object Description Exchange Format
CPE Common Platform Enumeration
CEE Common Event Expression
RID Real-Time Inter-network Defence
RID-T Transport of Real-Time Inter-network Defence
CYBEX The cyber security Information exchange framework
CWSS Common Weakness Scoring system

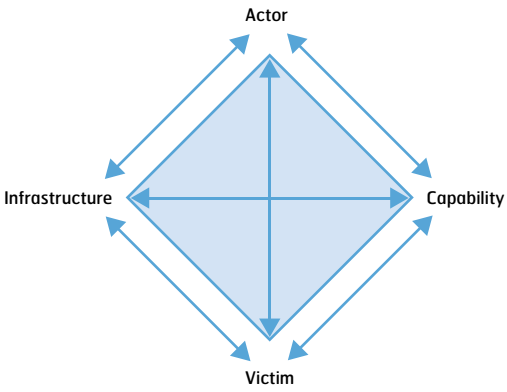
30 Connolly, Davison and Schmitt, TAXII, Nov 2013
http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_July_2013.pdf

31 Information Sharing Models for Cooperative Cyber Defence. Hernandez-Ardieta JL, Tapiador JE, Suarez-Tangil G, 2013. NATO.
http://www.ccdcoe.org/publications/2013proceedings/d1r2s2_hernandezardieta.pdf

The work of Hernanadez-Ardieta et al (2013) demonstrates that STRUM formats for expressing CNA threat data (columns shown in red) is not suited to articulating system vulnerability and weaknesses (shown in blue). This comparison by functional capability focus demonstrates that STIX has sufficient functionality to other threat languages, but would require the recipient of cyber threat intelligence to rapidly disseminate system vulnerability and remediation direction across their own network in a different format. The distinguishing feature of STIX, as a preferred STRUM format, is the support of the US government and the traction it is gaining in other sectors.

This work compliments the earlier industry research of Obrst et al (2012)[32], from MITRE, that derived the diamond model to model the objective for the development an ontology for cyber security. The aims of this research were to design protocols more flexible and comprehensive than that previously used to record malware incidents.

STIX is therefore emerging as the most interoperable of the STRUM formats that has been devised to record malware incidents, but still retains sufficient flexibility to encompass broader current and emerging cyber network attack TTPs.



The earlier work of Simmons[33] et al (2009) which developed the AVOIDIT taxonomy (Attack, Vector, Operational Impact, Defence, Information Impact and Target seeks to combine attack data and vulnerability data into a single STRUM format. Simmons et al examined and assessed 5 previous taxonomies in order to derive a combined reporting format that includes the following categories:

This combined approach appears contrary to the later research of Hernandez-Ardieta[34] et al (2013), but the prospect of a STRUM format that provides a single medium for attack and vulnerability reporting does appear to offer greater analytical value than either a single attack or vulnerability report.

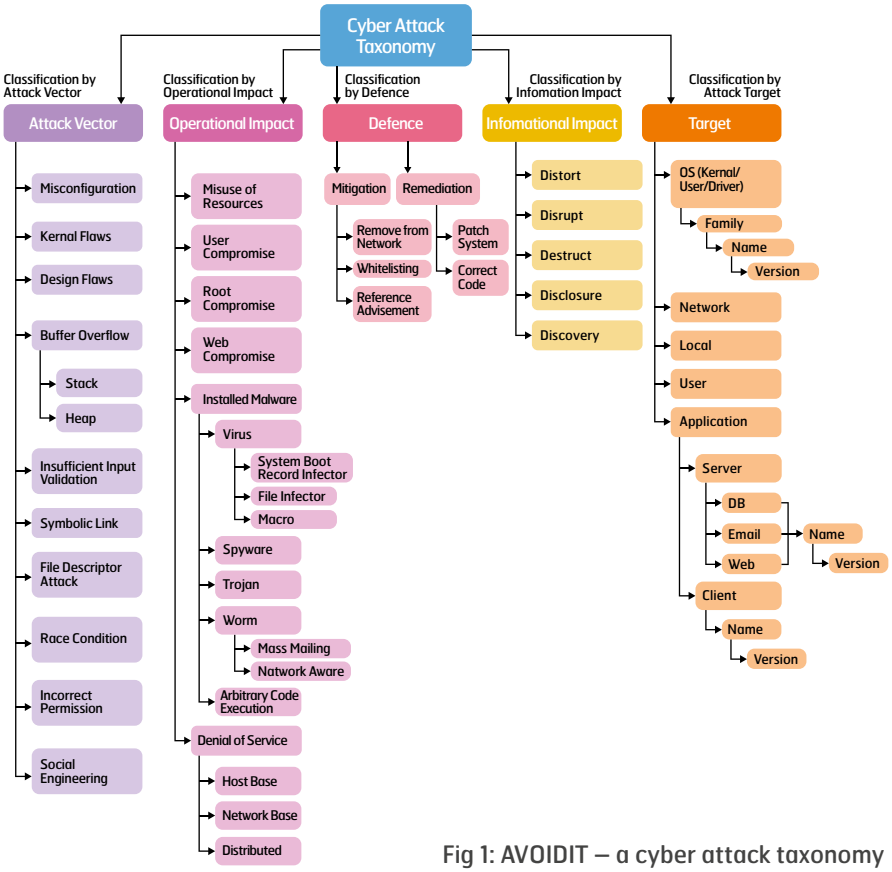


Fig 1: AVOIDIT – a cyber attack taxonomy

32 Obrst L, Chase P, Markleoff R, Developing an Ontology of the Cyber Security Domain, MITRE, 2012. http://www.franz.com/agraph/cresources/white_papers/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf

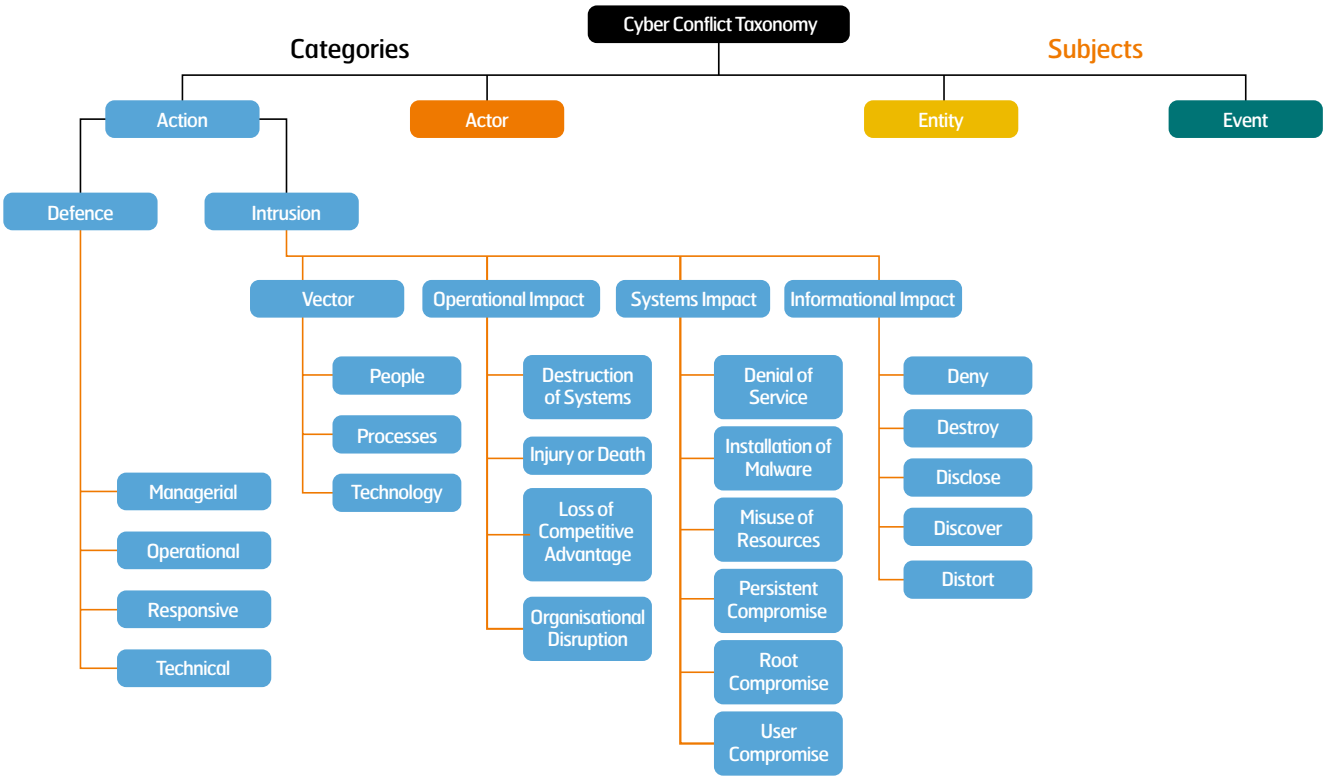
33 AVOIDIT: A cyber Attack Taxonomy, University of Memphis 2009 http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf

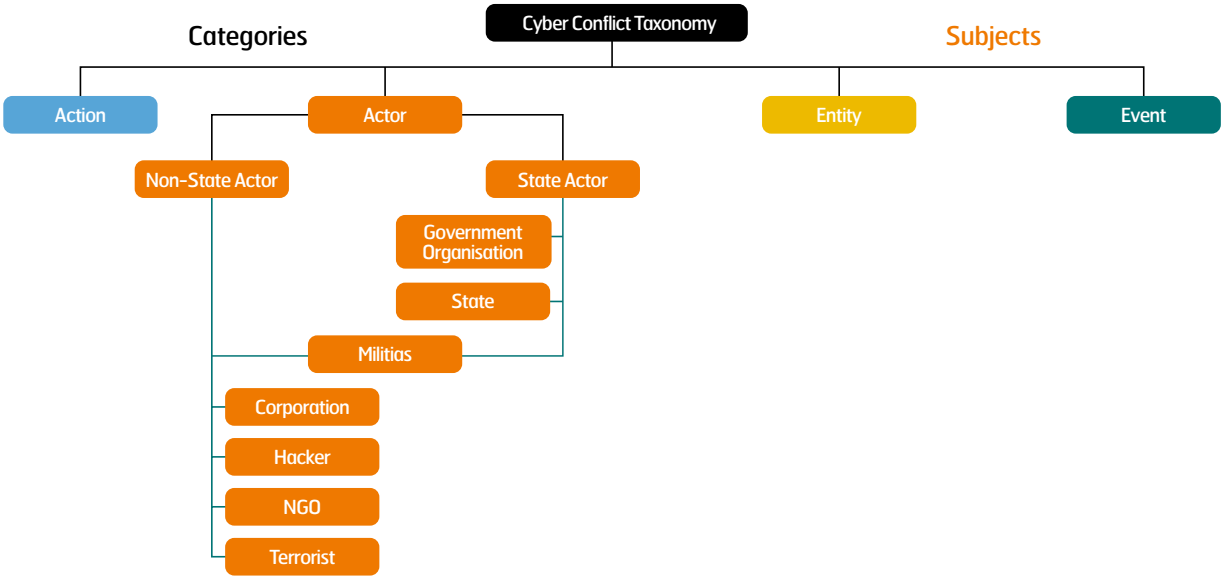
34 Information Sharing Models for Cooperative Cyber Defence. Hernandez-Ardieta JL, Tapiador JE, Suarez-Tangil G, 2013. NATO. http://www.ccdcoe.org/publications/2013proceedings/d1r2s2_hernandezardieta.pdf

Applegate and Stavrou[35] (2013) acknowledge the contribution of previous research and taxonomies, but conclude that these STRUM formats do not allow "the complex interactions between attacks, actors and other potentially related events". Their format focuses on actors and actions (see below) and incorporates much of the taxonomy captured in the AVOIDIT STRUM format.

Entities refer to the victim of the attack and are envisaged as user designated, but categorised from the actor menu. Similarly events categories are derived from the actions menu.

Notwithstanding the diverse research on cyber taxonomies, as their pivotal function as a factor of an effective cyber threat intelligence capability, it is inter-operability rather than functionality that should drive the adoption of any particular format or taxonomy. In these circumstances STIX and TAXII appear the most appropriate STRUM formats at this time.





35 Towards a Cyber Conflict Taxonomy (2013)

Further Research and Briefing Resources

VIDEOS:

1. Threat Intelligence and the Paradigm Shift in Cyber Defense – Neal Rothleader

A TED lecture from the University of Vermont's Complex Systems Centre which provides a useful explanation of the requirement to adopt an intelligence led approach to cyber security for both security subject matter experts and laymen. At 17:10 minutes there is enough detail and accessible analogies, notably the use of ice hockey, to advance individual and collective understanding of the concepts and objective of cyber threat intelligence.

http://www.youtube.com/watch?v=tYil33JkS0s

2. Intelligence-Driven Security: A New Model using Big Data – RSA

A good lecture filmed last year and worth the 21:38 minute investment to understand how data analytics can add value to visualising and modelling the threat. It covers the evolution of the threat from intrusive to disruptive and ultimately destructive. It also assesses attack surface as porous, inverted and virtual.

https://www.youtube.com/watch?v=R31Ez1XJEeI

3. Cyber threat intelligence & Response Technology – Access Data

A very polished and professional "infomercial" designed to promote vendor services, but nonetheless provides a very useful summary, at 4:29 minutes, of the differences between technology led, target centric, cyber network defence and intelligence led, threat centric, cyber network security.

http://www.youtube.com/watch?v=NRJk9ZwXY5

4. Introduction: Recorded Future Cyber threat intelligence Application – Recorded Future

A useful example of what data fusion management software, or search visualisation and analysis too, can do to leverage the training, education and experience of an analyst. At 3:51 minutes it is an extended promotional video, but does drawn out the principles and key benefits of SV&A tools, albeit for a less sophisticated platform.

http://www.youtube.com/watch?v=DgkHLMhpqkA

5. NextGen Cyber threat intelligence Center Wipro Webinar – WiPro

Notwithstanding, the heavily accented English commentary this Webinar is a surprisingly well structured overview of the cyber network attack threat spectrum. There is value in some of the illustrative slides, even if the commentary and the jargon (the use of cybertage for sabotage) can be a little galling. At 48:17 it is probably too much for those new to the subject.

http://www.youtube.com/watch?v=olS__Z3rzKI

6. Test Cyber Threat Intelligence Video 1 – Deloitte

This "infomercial" is intended for North American viewers and may prove a little disconcerting by using some dubious analogies to European ancient and medieval history, but a good layman's introduction to cyber threat intelligence. Nonetheless, worth the 5:48 minute investment for those new to the subject.

http://www.youtube.com/watch?v=x9vUKt6qGyY

7. Cyber Security Primer – Chatham House

A brief video setting out the challenges of security cyber space and how it may affect existing organisational structures. (2:48 minutes).

Vendor Cyber Threat Intelligence & Security Services

Mention of specific vendor services in no way represents a recommendation. The examples are listed below to provide a guide to turn key services available to UK Banking and Payment Services clients.

8. Deloitte

http://www.cyberintelligencecentre.com/

9. Hewlett Packard

http://www8.hp.com/uk/en/software-solutions/software.html?compURI=1346136

10. IBM

http://instituteforadvancedsecurity.com/

11. Lockheed Martin

http://www.lockheedmartin.co.uk/us/what-we-do/information-technology/cyber-security/cyber-intelligence-professional.html

12. Qinetiq

http://www.qinetiq.com/what/capabilities/cyber/Pages/cyveillance-cyber-intelligence.aspx

13. RSA

http://uk.emc.com/security/rsa-identity-protection-and-verification/rsa-cybercrime-intelligence-service.htm

14. Verisign

http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/index.xhtml?loc=en_US

15. Verizon

http://www.verizonenterprise.com/solutions/security/

Vendor Search, Visualisation & Analysis Tools

16. Detica

https://www.baesystemsdetica.com/services/cyber-security/what-we-offer/monitor/cyberreveal

17. Palantir Technologies

http://www.palantir.com/solutions/cyber/

18. IBM i2

http://www-01.ibm.com/software/uk/industry/i2software/

Cyber Security Reporting

19. IBM 2013 Cyber Security Intelligence Index

http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html

http://public.dhe.ibm.com/common/ssi/ecm/en/sew03034usen/SEW03034USEN.PDF

20. Verizon 2013 Data Breach Investigations Report

http://www.verizonenterprise.com/DBIR/2013/

21. UK Government – The UK Cyber Security Strategy

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

22. Department for Business Innovation and Skill 2013 Information Security Breaches Report

http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf

23. Competitive Analysis of the UK Cyber Security Sector

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

24. ICAEW Cyber Security in Corporate Finance

http://www.icaew.com/~/media/Files/Technical/Corporate-finance/Corporate-finance-faculty/tecpln12526-cyber-web.pdf

25. KPMG Cyber Threat Intelligence and Lessons from Law Enforcement

http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

26. CESG Cyber Security Documents

http://www.cesg.gov.uk/News/Pages/10-Steps-to-Cyber-Security.aspx

- Cyber Risk: A Board Management Responsibility

http://www.bis.gov.uk/assets/biscore/business-sectors/docs/c/12-1119-cyber-risk-management-board-responsibility

- Ten Steps to Cyber Security – An Executive Companion

http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive

- Ten Steps to Cyber Security

http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1121-10-steps-to-cyber-security-advice-sheets

27. Chatham House Cyber Security and Global Interdependence: What Is Critical?

http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

28. RSA Cyber Security Reports

- The Current State of Cyber Crime
- The Cyber Espionage Blueprint

http://web.emc.com/UK/trust-cyber-security?cmp=knc-trusted_IT-adv_security_cybersecurity-cybersecurity-UK&activity_id=266732&division=rsa

29. World Economic Forum Risk and Responsibility in a Hyperconnected World

http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world

CISO Resources

30. IBM Blogs and Webinars
http://securityintelligence.com/ciso/

31. MWR Knowledge Centre
https://www.mwrinfosecurity.com/knowledge-centre/

32. CPNI Research Programmes
http://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/

33. Banking and Payment Services ISAC Webinars
https://www.brighttalk.com/webcast/9217/72629

Case Studies

1. DarkSeoul. On 20 March 2013 the financial sector in South Korea experienced a Distributed Denial of Service (DDoS) attack that affected corporate and retail operations. The Jokra exploits wiped hard drives and closed branches. Several banks were paralysed despite previous experience of similar attacks in South Korea in 2009 and 2011.

2. Saudi Aramco. On 15 August 2012 the Saudi state oil corporation, Saudi Aramco, lost over 30,000 hard drives to an attack by the Shamoon virus from a group calling themselves the "Cutting Sword of Justice". Saudi Aramco denied any effect on production, but there is considerable debate on the scale of this catastrophic outage and the level of state support required to restore services.

3. Operation Ababil. In September 2012 a group calling itself Cyber fighters of Izz Ad-Din Al Qassam and also known as Qassam Cyber Fighters launched Distributed Denial of Service (DDOS) attacks against the US banking system. Initial results appear limited to damage to target websites, but Phase 2, launched in December 2012 was more successful, disrupting electronic banking, retail and corporate, for up to three months. The level of resourcing required is consistent with a state sponsored actor. Public domain information indicates that Iran, potentially with the support of the Anonymous group were responsible for the attacks. The cost per minute, for attacks that lasted up to three months, is estimated at US$30,000.

4. Operation Aurora. In mid 2009 six months of cyber attacks in the US were attributed to The Elderwood Group. This group, associated with the People's Liberation Army, deployed advanced persistent threat (APT) exploits to penetrate technology and defence corporations using a "stepping-stone" attack profile through their supply chains. Open source information indicates that the Chinese Politburo authorised the attacks to gain insight of Google's intentions in the PRC. Defence intelligence technology remain a high intelligence collection requirement for the PRC.

5. Operation Night Dragon. A cyber espionage campaign against the US energy sector commenced in November 2009 stole sensitive intellectual property from petro chemical corporations. The electronic pattern of life of the attacks was notable as all incidents took place between 0900 and 1700 Beijing time.

6. Soldier of Tallinn. On 27 April 2007 Estonia experienced some of the most complex and intense distributed denial of service attacks noted in an event that has since become as seminal case study of cyber warfare. Estonian law enforcement eventually traced the source of the attacks to actors under Russian jurisdiction. On one conviction has been made thus far, a single Russian national. The catalyst for the attack is believed to be the removal of a bronze statue commemorating the Soviet "liberation" of Estonia in 1994. The attacks against Estonia are widely assessed as a Russian state sponsored response.

Glossary

Analytics Analytics is the process of developing actionable insights through problem definition and the application of statistical models and analysis against existing and/or simulated future data. (Cooper, A 2008)

Area of Intelligence Interest (AOII) Those subjects or geographical areas which constitute which represent areas of concern or importance, but which legislative control or influence cannot be exercised to achieve direct collection and processing of the required materiel.

Area of Intelligence Responsibility (AOIR) The space in which an actor has sovereign control or responsibility for identifying and reporting activity of intelligence value to the appropriate key decision maker (KDM) or body of KDMs.

Capability The technical competency, means and resources available to an adversary to conduct operations.

Centre for Protection of National Infrastructure (CPNI) A UK Government authority which provides protective security advice to business and organisations across the national infrastructure, formed in February 2007.

Computer Network Operations (CNO) The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG).

Cyber Intelligence Material concerning cyber network attack techniques, tactics, procedures, actors and capabilities acquired and systematically processed that provides insight and foresight of adversary capability, and intentions.

Computer Network Attack (CNA) Offensive manoeuvre or actions employed by adversaries, varying from individuals to those who may be state or corporately enabled or sponsored that seeks to penetrated the cyber network defences of targets information systems, infrastructures or information technology devices for illegal, illegitimate or subversive ends. Also described as Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defence (CND) Protective security measures and protocols integrating software and hardware to achieve protection against the penetration of defended information systems, devices or networks. Also described as Actions taken to protect, monitor, analyse, detect, and respond to unauthorised activity within the DOD information systems and computer networks.

Cyber Network Exploitation (CNE) The actions including, but not limited to crime, subversion, espionage, sabotage and terrorism conducted against a targeted network, system or device. Also described as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Cyber Space A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Network Operations The component of Cyber Operations that establishes, operates, manages, protects critical infrastructure and key resources It consists of three core elements: Cyber enterprise management (CyEM), cyber content management (CyCM), and cyber defence (CyD), including information assurance, computer network defence (to include response actions), and critical infrastructure protection.

Cyber Support A diverse collection of supporting activities which are generated and employed to specifically enable both Cyber Network Operations and CyberWar. These activities are called-out in this unifying category due to their unique and expensive nature as high-skilled, low-density, time-sensitive and intensive activities requiring specialised training, processes, and policy. Additionally, several of these activities also require specialised coordination, synchronisation, and integration to address legal and operational considerations. It is because of these considerations and their overall importance that these activities are addressed as a Cyber Operations core component.

Cyber Warfare The use of computer technology to disrupt the activities of a state or organisation, especially the deliberate attacking of communication systems.

Common Operating Picture (COP) A common operational picture (COP) is a single identical understanding of relevant (operational) information shared by all entities with access to it. A COP facilitates collaborative planning and assists all entities to achieve shared situational awareness (SSA) of an operational environment.

Community of Action A community of action (CoA) exists in a situation where actors have the possibility of bringing about change. CoAs possess some of the characteristics of communities, such as the development of a common language and mutual learning in the course of action. However, they also possess some of the characteristics typical of more associative social relationships, such as the "voluntary" nature of association and the importance of "common goals" in directing collective activity.

Community of Interest Community of Interest is a means by which network assets and or network users are segregated by some technological means for some established purpose.

Concept of Operations (CONOPS) A concept of operations is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders

Course of Action (COA) A possible plan or scheme available to an individual or group that would accomplish, or is related to the accomplishment of a task of objective.

Cyber Threat Intelligence (CTI) Materiel detailing the actions and intent of cyber threat actors.

Electronic Pattern of Life (EPoL) The activity by a cyber actor or aggregated activity of multiple users that defines network usage by a group of cyber entities, either legitimately or for subversive intent.

Electronic Finger Printing (EFP) The characteristics of the deployment and employment of cyber network attack techniques that allow the modus operandi of a cyber threat actor or threat network to be identified. Including, but not limited to; the timings of an intrusion, the method of gaining access to the targeted site, the anonymity measures used and the exploitation of the targeted system.

Essential Elements of Information (EEIs) The most critical information requirements regarding the adversary and the environment needed by a key decision maker by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

Financial Intelligence Sharing Service (FISS) A Fraud Intelligence Sharing System (FISS) was established in 2008, which enables the banking industry to share information on all confirmed, attempted and suspected fraud in a central, shared database. Established specifically to combat all types of banking-related fraud in the UK, the system provides the industry with a secure and robust reporting mechanism supporting the industry's long-term fraud prevention strategy.

Indicators & Warnings (I&W) Recognition of indicators and warnings is the ability to perceive trends, indications, and/or from the data, information and intelligence processed after collection.

Intelligence The aggregation of pertinent, codified and evaluated materiel that improves the perception of an operational environment or an action within such an environment.

Intelligence Cycle The Intelligence cycle is the fundamental cycle of intelligence processing. The stages of the intelligence cycle include the issuance of requirements by decision makers (Direction), obtaining relevant materiel (Collection), codifying, evaluating and analysing the collection sample with appropriate consideration for the provenance, context and source reliability (Processing), and publication of intelligence (Dissemination) to inform or influence the actions of key decision makers by providing relevant and timely decision support advice that affords insight and foresight and achieving greater levels of understanding than would otherwise be possible.

Intelligence Fusion Node A capability within an intelligence fusion matrix able to assimilate multiple information, data and intelligence feeds in order to provide a local key decision makers with situation awareness that informs and influences actions and reaction to a complex and dynamic operational environment. The speed of communication and dissemination within a fusion node matrix is a key driver for reducing latency that allows the collation of a common operating picture (COP) that achieves shared situation awareness (SSA) for all fusion nodes and their respective decision, leadership or management functions.

Intelligence Led The primacy of intelligence in the assessment and management of risk in order to respond to current and emerging threats with appropriate mitigation and counter measures.

Kuhnian Paradigm Shift A paradigm shift, or scientific revolution, is a pivotal change in the basic assumptions, or paradigms, within the ruling theory of science. Thomas Kuhn posited in his influential book The Structure of Scientific Revolutions (1962), that "A paradigm is what members of a scientific community, and they alone, share". He contrasted this with humanities where a number of competing and incommensurable solutions to problems appear to co-exist. In the cyber domain the technology led approach to cyber security has been the "scientific basis" for the development of cyber security.

Observe, Orient, Decision, Action (OODA) The OODA loop is a concept originally applied to the combat operations process, often at the strategic level in military operations. It is now also often applied to understand commercial operations and learning processes.

Shared Situation Awareness (SSA) Shared Situation Awareness is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status after some variable has changed, such as time, or some other variable, such as a predetermined event (in this case a cyber network attack (CAN). It is also the state of perception of an operational environment critical to decision-makers in complex, dynamic areas.

Search, Visualisation & Analysis (SV&A) Analytical tools that allow pattern and trend analysis to be achieved from significant data samples, known as "big data" that can be subsequently displayed from the perspective of any entity to discern interconnections and interdependencies not readily apparent.

Standard Technical Reports Using Modules (STRUM) Standard reports that allow diverse data to be codified by means of modular reporting to facilitate systemic and rapid processing.

Tactics, Techniques and Procedures (TTPs) The modus operandi of an adversary to employ particular methods of exploitation to achieve a espionage, subversion, sabotage or terrorism effect.

Target Hardening The combination of virtual, electronic and physical protective security measures and procedures that increase the time, effort and complexity of illegitimate access or use of a defended asset.

Threat The combination of adversary Capability, Intent and Opportunity that can be used to increase the effectiveness of a Cyber Network Attack (CNA).

Threat Centric The central consideration of threat actors and actions in order to prioritise preventative (reduction of the attack surfaces), mitigation (intrusion prevention and malware detection) and recovery measures (cyber forensics and SIEM) to the most appropriate threat vectors. This will include an evaluation of probability and impact.

Acknowledgements

Any errors, inaccuracies or attribution omissions are the responsibility of the author (Head of Security). All corrections, amendments or clarifications should be addressed to him at the details provided at the end of this report. The support and efforts of the following people who provided numerous research sources, advised on presentation and diligently removed the errors has been key to the publication of this research paper.

Research

Rhiannon Butterfield	Head of Regulatory and Government Engagement, Payments Council
Elizabeth Fraser	Head of European Developments, Payments Council
Ben Lindgreen	Principal Security Consultant, Payments Council
Dom Lucas	Security Consultant, Payments Council
Karen Milton	Director of Finance, Payments Council
David Song	European Consultant, Payments Council
Jack Wilson	Government Engagement Advisor, Payments Council

Review

David Ferbrache OBE	Special Advisor, Cyber Security, KPMG
Brendan Pickering	Head of Group Fraud Technology, HSBC
Mark Stanhope	Head of Operations and Governance, Mobile Payments Service

Proofing

Jake Horwood	Payments Integrity Advisor, Payments Council
Krystle Kingston	Payments Integrity Co-Ordinator, Payments Council
Doriena Koldenhof	Communications Officer, Payments Council

References

Amin, Rohan	Lockheed Martin Corporation: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (with Eric Hutchins and Michael Cloppert), dated Aug 2011
Bamford, George	Intelligence and National Security Alliance, Cyber threat intelligence Task Force, Operational Levels of Cyber threat intelligence dated Sep 2013 (with John Fekker and Matthew Mattern)
Backhouse, J	(2004) Computer Crime at CEFORMA: A Case Study, International Journal of Information Management, 24, 2004, 551-561 (with Silva, L and Dhillon, G)
Barnum, Sean	Standardising Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX), The Mitre Corporation, 2012
Beebe, Nicole Lang	Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security, Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, Dec 2005 (ISBN: 0-9772107-0-7) with V Srinivasan Rao (2005)
Cardensa, Alvaro A	(2012) Big data Analytics for Security Intelligence, Cloud Security Alliance, September 2013 (with Pratyusa K Manadhata and Sree Rajan)
Chase, Penny	Developing an Ontology of the Cyber Security Domain, MITRE, 2012 (with Leo Obrst and Richard Markleoff)
Clarke, R V	(1980) Situational Crime Prevention: Theory and Practice, British Journal of Criminology, 20, 136-147
Clarke, R V	(1997) Situational Crime Prevention: Successful Case Studies, Harrow and Heston Publishers: Guilderland, 1-357
Cloppert, Michael	Lockheed Martin Corporation: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (with Eric Hutchins and Rohan Amin), dated Aug 2011
Connolly, Julie	The Trusted Automated eXchange of Indicator Information (TAXII™) Whitepaper, MITRE Corporation, 7 Nov 13 (with Mark Davidson and Charles Schmidt)
Cooper, Adam	(2008) JISC Centre for Educational Technology and Interoperability Standards, Analytical Series, Vol 1, Number 5, What is Analytics?, Definition and Essential Characteristics
Davidson, Mark	The Trusted Automated eXchange of Indicator Information (TAXII™) Whitepaper, MITRE Corporation, 7 Nov 13 (with Julie Connolly and Charles Schmidt)
Dasgupta, Dipankar	(2009) AVOIDIT: A Cyber Attack Taxonomy, University of Memphis (with Charles Ellis, Sajjan Shiva, Chris Simmons, Qishi Wu)
Dhillon, G	(1999) Managing and Controlling Computer Misuse, Information Management ξ Computer Security, 7, 4, 171
Dhillon, G	(2001) Computer Crimes: Theorizing About the Enemy Within, Computers ξ Security, 20, 8, 715-723 (with Moores, S)
Dhillon, G	(2004) Computer Crime at CEFORMAS: A Case Study, International Journal of Information Management, 24, 2004, 551-561 (with Silva, L and Backhouse, J)
IBM	Cyber Security Intelligence Index
Ellis, Charles	(2009) AVOIDIT: A Cyber Attack Taxonomy, University of Memphis (with Chris Simmons, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu)
Fekker, John	Intelligence and National Security Alliance, Cyber threat intelligence Task Force, Operational Levels of Cyber threat intelligence dated Sep 2013 (with George Bamford and Matthew Mattern)
Gonsalves, Antonio	Talk of cyberwarfare meaningless to many companies, experts say, CSO, 6 Jan 2014
Hernandez-Ardieta, JL	Information Sharing Models for Cooperative Cyber Defence, 2013, NATO (with Juan E Tapiador and Guillimero Suarez-Tangil)
Hutchins, Eric	Lockheed Martin Corporation: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (with Michael Cloppert and Rohan Amin) dated Aug 2011

Kaspersky	Security Bulletin 2013
Kim, Ikkyun	Analysis of Cyber Attacks and Security Intelligence, Mobile, Ubiquitous, and Intelligent Computing Lecture Notes in Electrical Engineering Volume 274, 2014, pp 489-494 (with Youngsoo Kim, Namje Park)
Kim, Youngsoo	Analysis of Cyber Attacks and Security Intelligence, Mobile, Ubiquitous, and Intelligent Computing Lecture Notes in Electrical Engineering Volume 274, 2014, pp 489-494 (with Ikkyun Kim, Namje Park)
Klaus, Julisch	Understanding and overcoming cyber security anti-patterns, Computer Networks Volume 57, Issue 10, 5 July 2013, Pages 2206–2211, Deloitte Enterprise Risk Services
Ludwick, Melissa	Software Engineering Institute Emerging Technology Center: Cyber Intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University (with Troy Townsend, Jay McAllister, Andrew O Mellinger, Kate Ambrose Sereno)
Manadhata, Pratyusa K	(2012) Big data Analytics for Security Intelligence, Cloud Security Alliance, September 2013 (with Alvaro A Cardensa and Sree Rajan)
Markleoff, Richard	Developing an Ontology of the Cyber Security Domain, MITRE, 2012 (with Leo Obrst and Penny Chase)
McAllister, Jay	Software Engineering Institute Emerging Technology Center: Cyber Intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University (with Troy Townsend, Andrew O Mellinger, Kate Ambrose Sereno)
Mattern, Matthew	Intelligence and National Security Alliance, Cyber threat intelligence Task Force, Operational Levels of Cyber threat intelligence dated Sep 2013 (with George Bamford and John Fekker)
Mellinger, Andrew O	Software Engineering Institute Emerging Technology Center: Cyber Intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University (with Troy Townsend, Andrew O Mellinger, Kate Ambrose Sereno)
Moores, S	(2001) Computer Crimes: Theorizing About the Enemy Within, Computers ξ Security, 20, 8, 715-723 (with Dhillon, G)
Moriarty, Kathleen	Transforming Expectations for Threat-Intelligence Sharing, EMC2 RSA Perspective, August 2013
MOD	Joint Publication 2-0, Joint Intelligence dated 22 Oct 2013
MOD	Joint Defence Publication 04: Understanding, dated Dec 2010
Obrst, Leo	Developing an Ontology of the Cyber Security Domain, MITRE, 2012 (with Penny Chase and Richard Markleoff)
Park, Namje	Analysis of Cyber Attacks and Security Intelligence, Mobile, Ubiquitous, and Intelligent Computing Lecture Notes in Electrical Engineering Volume 274, 2014, pp 489-494 (with Youngsoo Kim, Ikkyun Kim)
Rajan, Sree	(2012) Big data Analytics for Security Intelligence, Cloud Security Alliance, September 2013 (with Alvaro A Cardensa and Pratyusa Manadhata)
Rao, V Srinivasan	Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security, Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, Dec 2005 (ISBN: 0-9772107-0-7) with Beebe, Nicole Lang
Schmidt, Charles	The Trusted Automated eXchange of Indicator Information (TAXII™) Whitepaper, MITRE Corporation, 7 Nov 13 (with Julie Connolly and Mark Davidson)
Sereno, Kate	Software Engineering Institute Emerging Technology Center: Cyber Intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University (with Troy Townsend, Melissa Ludwick, Jay McAllister, Andrew O Mellinger)
Shiva, Sajjan	(2009) AVOIDIT: A Cyber Attack Taxonomy, University of Memphis (with Charles Ellis, Chris Simmons, Dipankar Dasgupta, Qishi Wu)
Silva, L	(2004) Computer Crime at CEFORMA: A Case Study, International Journal of Information Management, 24, 2004, 551-561 (with Backhouse, J and Dhillon, G)
Simmons, Chris	(2009) AVOIDIT: A Cyber Attack Taxonomy, University of Memphis (with Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu)

Straub, D W, Jr	(1987) Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures, Eighth Annual International Conference on Information Security, Pittsburgh, PA, 277-289
Straub, D W, Jr	(1990) Effective IS Security: An Empirical Study, Information Systems Research, 1, 3, 255-276
Suarez-Tangil, Guillimero	Information Sharing Models for Cooperative Cyber Defence, 2013, NATO (with Juan E Tapiador and Jorge L Hernandez-Ardieta)
Tapiador, Juan E	Information Sharing Models for Cooperative Cyber Defence, 2013, NATO (with Guillimero Suarez-Tangil and Jorge L Hernandez-Ardieta)
Townsend, Troy	Software Engineering Institute Emerging Technology Center: Cyber Intelligence Tradecraft Project dated Jan 2013, Carnegie Mellon University (with Melissa Ludwick, Jay McAllister, Andrew O Mellinger, Kate Ambrose Sereno)
US TRADOC	Cyberspace Operations Concept Capability Plan 2016-2028 dated 22 Feb 2010, TRADOC Pamphlet 525-7-8
Verisign	Establishing a Formal Cyber Intelligence Capability, A whitepaper, iDefense security Intelligence services
Verizon	Data Breach Investigations report 2013
Wu, Qishi	(2009) AVOIDIT: A Cyber Attack Taxonomy, University of Memphis (with Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Chris Simmons)

Notes

Notes

Notes

Contact Details

Craig Rice MBA, MSc, BSc(Hons)
Director of Security

T: +44 (0)20 3217 8453
E: **Craig.Rice@paymentsuk.org.uk**

“The elephant in the room?

A challenge so big it can only be taken one bite at a time?

A Hadoop application yet to be fully realised?”

Payments UK
2 Thomas More Square,
London, E1W 1YN

Tel: 020 3217 8200
Email: questions@paymentsuk.org.uk
www.paymentsuk.org.uk