1

Introduction

Everything has a beginning. Chapter 1 sets out to define cyber threat intelligence and chart the development of the concept from antiquity to the present day. Despite cyber threat intelligence being a recent concept, the need to characterise threats and to understand the intentions of enemies has ancient roots.

1.1 Definitions

'Cyber Threat Intelligence' is a term which is readily understandable, but not necessarily easy to define.

There are a variety of different perspectives and experiences which lead to different understandings of the term. For some, cyber threat intelligence refers to the collection of data. For others the term refers to teams of analysts and the processes required to analyse data. For many it is the name of a product to be commercialised and sold.

Cyber threat intelligence encompasses all these perspectives, and more. This book addresses the many facets of the term, ranging from the historical development of intelligence through to the modern application of cyber threat intelligence techniques.

One area of threat intelligence is purposefully omitted. The covert collection of intelligence from human agents (HUMINT), often obtained from participants within underground criminal forums is beyond the scope of this book. This domain and the associated techniques are a distinct specialism with their own risks and dangers which merits a separate book.

To define what is meant by cyber threat intelligence we must start by understanding the meanings of the constituent terms, 'intelligence' and 'cyber threat'.

Cyber Threat Intelligence, First Edition. Martin Lee.

1.1.1 Intelligence

To better understand the concept of intelligence, we can examine the domain from the viewpoints of the different practitioners.

The field of Intelligence is most commonly associated with the military. The multi-national military organisation, North Atlantic Treaty Organization (NATO) defines Intelligence as:

> The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.
>
> *(NATO 2017a)*

Intelligence is not exclusively military in nature. Intelligence activities may be undertaken by non-military governmental organisations, the Central Intelligence Agency (CIA) being one such example. Despite having the term 'intelligence' as part of its name, the early years of the agency were marked by much discussion debating the nature of what is meant by intelligence (Warner 2002). One document reflecting the uncertainties of the time, succinctly defines intelligence as:

> Intelligence is the official, secret collection and processing of information on foreign countries to aid in formulating and implementing foreign policy, and the conduct of covert activities abroad to facilitate the implementation of foreign policy.
>
> *(Bimfort 1958)*

Intelligence is not the exclusive preserve of the state. The private sector also engages in intelligence activities, such as conducting competitive intelligence, which may be defined as:

> ... actionable recommendations arising from a systematic process involving planning, gathering, analyzing, and disseminating information on the external environment for opportunities, or developments that have the potential to affect a company's or country's competitive situation.
>
> *(Calof and Skinner 1998)*

As with other forms of Intelligence, there is much debate regarding what is exactly meant by 'Competitive Intelligence'. Definitions range from those that could apply equally to military intelligence:

> A process that increases marketplace competitiveness by analysing the capabilities and potential actions of individual competitors as well as the overall competitive situation of the firm in its industry and in the economy.
>
> *(Pellissier and Nenzhelele 2003)*

Across the various disciplines and specialisations associated with the notion of 'intelligence', there are commonalities within definitions, namely:

- Intelligence is both a process and a product.
- The Intelligence process consists of gathering information, analysing this and synthesising it into an Intelligence product.
- Intelligence products are intended to be used by recipients in order to assist in decision making.

1.1.2 Cyber Threat

As a prefix, the term 'cyber' dates back to the 1940s, and was first used in the concept of 'cybernetics' relating to the communication and control interfaces between living things and machines (Coe 2015). Since this date the term has been used widely in the context of futuristic technology.

The term has undergone a rapid evolution. To Internet users of the mid to late 1990s, the term 'cyber' was used to describe the practice of conducting intimate relationships online (Newitz 2013). Yet in a relatively short time, the term has become closely associated with security and attacks against computing systems.

The origins of this evolution lie in the 1960s use of the term 'cyberspace' to refer to environments outside of normal experience (Ma et al. 2015; Strate 1999). Over time this notion of a separate domain came to be used to refer to the space created by the network of connected computing systems that comprises the Internet.

NATO defines cyberspace as:

> The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.
>
> *(NATO 2017b)*

Hence, the 'cyber domain' is a potentially contested space which is equivalent to the traditional militarily contested environments of the land, sea, and air (Crowther 2017). Following this logic, in the same way that there is an army to fight on land, a navy to fight on the sea, an air force for air battles, a cyber capability is required to defend and project national interests within this new domain (Ferdinando 2018; Emmott 2018).

Threats are to be found within the traditional domains of the land, sea, and air. These threats are diverse in nature, ranging from hostile adversaries who seek to cause harm, to adverse weather conditions which may damage ships or planes, or simply geographical features such as mountain ranges which might block routes.

A military commander wishing to operate in any of these domains must collect intelligence to understand the threats that may be encountered. This intelligence

should be expected to describe where a threat is located, the specific danger that the threat may pose, and how the threat is changing over time.

In this respect, cyberspace is no different. Within this new domain hostile adversaries may be operating, physical features of the infrastructure may constrain operations, and software installations may change as frequently as the weather (Mavroeidis and Bromander 2017).

In order to operate in this cyber environment, we also must gather intelligence. Decision makers must remain abreast of the nature and risk posed by current threats so that an appropriate response can be orchestrated allowing everyday activities to be conducted safely and successfully.

1.1.3 Cyber Threat Intelligence

Clearly, cyber threat intelligence is the application of intelligence to threats that affect the cyber realm. This concept can be expressed in many different ways. The research organisation Gartner defines threat intelligence as several items that contribute to decision making:

> Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
>
> *(Gartner Research and McMillan 2003)*

The Forum of Incident Response and Security Teams (FIRST) emphasises the informational aspect of threat intelligence.

> Cyber Threat Intelligence is systematic collection, analysis and dissemination of information pertaining to a company's operation in cyberspace and to an extent physical space. It is designed to inform all levels of decision makers.
>
> *(FIRST 2018)*

The Bank of England's framework for threat intelligence-led operations, CBEST, states that an intelligence-based approach to cyber security should have the following goals:

> to prevent an attacker from successfully attacking;
>
> to be able to recognise and respond effectively to an attack that has already happened.
>
> *(Bank of England 2016)*

Again, we can see common threads between these definitions. A working definition of cyber threat intelligence should combine definitions from the realm of traditional intelligence, emphasise the application to the notion of 'cyber', and state the use of intelligence.

Throughout this book I use the following as my working definition of cyber threat intelligence:

> The process and outcome of gathering and analysing information relating to threats that may cause damage to electronic networked devices, in order to assist decision making.

1.2 History of Threat Intelligence

This section is not intended to be an exhaustive study of history, but to highlight significant mileposts in the development of the discipline of intelligence, and to show how many of the issues faced by today's threat intelligence practitioners are not too different from those of the past.

1.2.1 Antiquity

The earliest recorded reference to Intelligence activities is found within the Biblical Book of Numbers. The book was probably written in the fifth century BCE describing events that took place many centuries earlier (McDermott 2002).

> And Moses sent them to spy out the land of Canaan, and said unto them, Get you up this way southward, and go up into the mountain;
>
> And see the land, what it is, and the people that dwelleth therein, whether they be strong or weak, few or many;
>
> And what the land is that they dwell in, whether it be good or bad; and what cities they be that they dwell in, whether in tents, or in strong holds;
>
> *(Numbers n.d.)*

Moses is the earliest example of a leader instructing teams to conduct an intelligence operation; gathering information regarding a domain in order to assist with decision making.

Also, during the fifth century BCE, the Chinese general Sun Tzu wrote his treatise on warfare, 'The Art of War'. This is one of the earliest descriptions of how to conduct warfare, although the text was not translated into English before the beginning of the twentieth century, it has become widely influential in the decades following the World War II onwards.

Sun Tzu recognised the importance of intelligence, and of having an understanding not only of the enemy's strengths and weaknesses, but also your own:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
>
> *(Giles 1910)*

Indeed, intelligence was fundamental to Sun Tzu's understanding of how to wage war. An entire chapter of his treatise was devoted to 'The Use of Spies', including descriptions of the different ways that intelligence can be gathered. Within this chapter, Sun Tzu emphasises the use of 'foreknowledge'.

> What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is *foreknowledge*. Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy's dispositions can only be obtained from other men.
>
> *(Giles 1910)*

It is informative to compare this quote on the importance of 'foreknowledge' with the multitude of definitions of Intelligence written twenty-five centuries later. Clearly the nature of intelligence has changed little over the years.

In tandem with the development of intelligence as the art of uncovering useful information, so the art of concealing useful information has also developed. Steganography is the science of hiding messages within other objects. Writing in the fifth century BCE, the Greek historian, Herodotus, described how messages could be tattooed on a slave's scalp before allowing the hair to grow and hide the message. Herodotus also described writing hidden messages on wooden backing of the wax tablets used by scribes to record and send messages (Fabien et al. 1999).

Discovering the hidden message required knowing how the message had been concealed. In the absence of this information, discovering the message was, by design, difficult. Uncovering hidden writing required a new skill set, that of cryptanalysis.

The first recorded cryptanalyst was Queen Gorgo of Sparta. A member of the Spartan royal family, Demaratus had been exiled to Persia. Upon learning of the Persian King Xerxes I's plans to invade Sparta, he sent a message inscribed on a wooden tablet hidden by a covering of wax to warn the Spartans.

However, the court of the Spartan king could make no sense of the apparently blank tablet until Gorgo correctly deduced that Demaratus would not have gone to the effort and danger of sending the item without good reason. She ordered the wax to be removed revealing the message concealed beneath (Baker 2022).

The fact that Gorgo's name is recorded along with her wisdom and insight in revealing the message demonstrates how highly regarded she and her actions were.

Through these snippets from prehistory we perceive glimpses of characters, and their efforts to gather intelligence and keep valued information secret. These illustrate how fundamental intelligence has been to humanity since the beginning of recorded time.

1.2.2 Ancient Rome

Rome was the dominant military power in the Mediterranean and Western Europe until the fourth century CE. Roman leaders made extensive use of intelligence in order to keep control over the empire and manage hostile borders (Austin and Rankov 1998).

Intelligence responsibilities were split between different functions, which changed and developed over time. In addition to scouts who operated to identify the location of the enemy for the legions, the *exploratores* operated at distance from the legions conducting reconnaissance and communicating with their generals by courier. Additionally, the enigmatic *speculatores* also conducted intelligence operations, including clandestinely listening to chatter within enemy camps, however detailed understanding of their function has yet to be determined (Campbell and Tritle 2013).

At the very least we know that Julius Caesar in the first century BCE made great use of intelligence. Contemporaneous reports describe Caesar as always reconnoitering the country when leading an army and seeking to understand the nature of his enemies from a geographical, economic, and even ethnographic point of view. He is known to have interrogated captured prisoners himself to understand how their customs and beliefs might affect their choice of how and when to conduct battle (Evov 1996).

We sense the presence of hostile intelligence operatives in the use of simple cryptography by Julius Caesar. Despite being the emperor, leading the largest and most efficient state apparatus in existence at the time, he found it necessary to write confidential matters using a substitution cypher (Reinke 1962).

The method of encrypting his messages is simplistic by modern standards. Caesar shifted the letters of the alphabet by four so that instead of writing the letter 'A', he would write 'D', and so forth. Nevertheless, the techniques necessary to reliably decrypt such messages were not described before the ninth century CE

(Lee 2014). In the Roman era, this was state of the art cryptography, indeed the technique would not be improved upon before the Renaissance.

In using cryptography, Caesar was clearly aware that his writing could be intercepted by operatives outside of his control, and potentially how the intelligence derived from his writings could be used against his interests. In this observation we sense an awareness of Communications Intelligence (COMINT) and the collection of intelligence from communications, alongside an awareness of the importance of Communications Secrecy (COMSEC) in the ancient world.

1.2.3 Medieval and Renaissance Age

During the eighth century CE, the Arabic philologist Al-Khalil ibn Ahmad al-Farahidi studied the nature of Arabic poetry, compiled the first Arabic dictionary, and studied cryptography, writing one of the first books on the subject, '*Kitab al-Mu'amma*' – 'The Book of Cryptographic Messages' (Broemeling 2011).

Although no copies of the book are known to have survived, the work influenced the Arabic philosopher Al-Kindi. Within a century of the publication of *Kitab al-Mu'amma*, Al-Kindi had expanded on Al-Khalil's ideas and developed the technique of frequency analysis in order to break the simple substitution cyphers in use at the time. Al-Kindi's book '*Risalah fi Istikhraj al-Mu'amma*' – 'A Manuscript on Deciphering Cryptographic Messages', detailed the techniques required in order to break any cryptographic cypher known at the time (Al-Kadit 1992).

Although the authors of the various medieval Arabic treatises on breaking cryptographic messages are clearly familiar with cyphertexts, little information remains of the content of the decyphered text, or who requested the decryption. A possible clue to the nature of the patrons of these works is to be found in the title of Ali ibd Adlan's manual of practical cryptanalysis '*Fi hall al-mutarjam*' – 'On Cryptanalysis', also known as '*al Mu'allaf Lil Malik al Ahraf*' – 'The Manual for King al Ahraf'. King al Ahraf being Al-Ashraf Musa, the Egyptian emir of Damascus, and a likely candidate for someone who would be interested in intercepting and decyphering messages.

Within Renaissance Italy, the associations between political power and cryptanalysis were clear. The first European cryptography manual was written in 1379 by Gabriele de Lavinde of Parma while working for Pope Clement VII. One hundred years later in 1474, Cicco Simonetta working for the Sforza, Dukes of Milan wrote the first European treatise on cryptanalysis and breaking cyphers (Bruen and Forcinto 2011).

Knowledge of how to hide messages quickly spread. Polydore Vergil observed in 1499 that *secret writing* (cryptography and steganography) had become widespread:

> But today this way of writing is so common that no one, sovereign or subject, is without his special signs, called cyphers in the vernacular.
>
> *(Marcus and Findlen 2019)*

Ambassadors, nobles, politicians, and their secretaries plotted and communicated in secret while keeping abreast of the plans and dispositions of other nation states or adversaries who, in turn, were also communicating and plotting in secret. Merchants communicated using 'secret writing' both to protect their trade secrets, but also to act as unofficial agents of the state, conducting diplomacy and collecting intelligence on foreign powers.

As Renaissance states developed, ensuring the confidentiality of communications became a state priority. Within Venice, cryptography developed into a professional branch of the civil service, with formal training and entry exams. This ensured that Venetian encrypted communications were as secure as possible, and that the Doge had a team of trained professionals who could decrypt intercepted documents (Iordanou 2018).

The breaking of cyphers was a technical problem; however, the collection of documents to decrypt was an operational problem. Networks of spies and informers could be tasked with collecting information from suspect individuals, or exiles. In Tudor England, Sir Francis Walsingham established a network of informers both within and outside the country, through which letters could be intercepted and potential threats to state security identified (Leimon and Parker 1996).

Walsingham's surveillance network, and his success in uncovering real or imagined Catholic plots against the nascently Protestant English nation helped secure Elizabethan England. At the same time, his network's infiltration of potential plots against the crown and their active involvement in instigating plots designed to uncover potential adversaries, helped temper the aspirations of those who might have preferred a change of political regime (Edwards 2007; Farhat-Holzman 2007).

The interception of private communications could be formalised as part of state functions. The *bullette* of Renaissance Siena was tasked with inspecting every letter sent from, or received within the city in order to identify any suspect contents (Shaw 2000). The establishment of the English postal service was strengthened by an ordinance of 1657, which included the provision that a national postal service '*will be the best means to discover and prevent many dangerous and wicked designs against the Commonwealth*'. Nevertheless, the secrecy of postal communication was not without protection. Postmasters were forbidden from opening any letter unless by warrant from the Secretary of State (Dugald et al. 1842).

Across seventeenth century Europe, *Cabinets noirs* or 'black chambers' were created by governments to intercept and monitor correspondence (Iordanou 2018; De Leeuw 1999). Intercepted encrypted messages could then be passed to the state cryptographers for decyphering. So efficient was the interception and decoding of the Viennese *Geheime Ziffernkanzle* (Secret Cypher Office) that the Viennese sold intercepted and decyphered diplomatic correspondence to France and Russia (Hillenbrand 2017).

The Snowden revelations of widespread state-sponsored monitoring of electronic communications during the twenty-first century should not have been

a surprise (MacAskill and Dance 2013). Technology has facilitated and automated a state function that has already existed for many centuries.

1.2.4 Industrial Age

With the industrialisation of societies during the eighteenth and nineteenth centuries, Intelligence became an increasingly specialised function. Outside of the military, many states had some form of intelligence capacity, which included ensuring the secrecy of official communications, while seeking to compromise the secrecy of the communications of others. However, it was the upheaval of the French Revolution of 1798 which created an environment in which long-lasting intelligence innovations were made during the early industrial era.

The paranoia of the years following the revolution necessitated the surveillance of political agitators who sought to overthrow the new government. Joseph Fouché headed the Ministry of General Police *ministère de la police générale,* organising it into an effective surveillance engine. His daily *bulletin de police* provided the first known regular intelligence briefings by a state intelligence apparatus, supplying Napoleon Bonaparte with information relating to political opposition, public order, and crime throughout the French empire (Fijnaut and Marx 1995).

This high-level strategic intelligence may have been sufficient to inform the head of state, but it didn't meet the needs of those trying to secure personal property, or considering whether to enter into a financial relationship with another party.

In 1811, the ex-convict Eugène François Vidocq founded the *Brigade de la Sûreté* as part of the prefecture de police. He recruited ex-criminals to infiltrate the criminal underworld to collect intelligence on illicit activities, and provided his services as a private detective to those who wished to chase bad debts or establish the creditworthiness of potential business partners. Thus creating both the first criminal intelligence agency, and establishing the provision of financial intelligence as a business model (Vause 2014).

As the Industrial Revolution gathered pace technological advances provided opportunities for Intelligence gathering. The detailed reports of action in the Crimean War of 1854–1856 collected by journalists, sent by steam ship, and published by the newspapers could provide the enemy with more information, more rapidly than could be achieved with existing intelligence apparatus. This led Tsar Nicholas I to half-jokingly proclaim '*We have no need for spies. We have the Times*'. (Dylan 2012).

The ability of the telegraph to rapidly transmit reports and receive orders from high command proved invaluable for conducting military operations. However, messages sent over the telegraph were liable to interception. During the American

Civil War, both the Confederacy and the Union used the telegraph to send signals, both used cryptography to encrypt the contents of their messages, and both intercepted each other's communications.

Initially the Confederacy allowed commanders to choose their own cyphers. Unsurprisingly this proved insecure and unworkable. The Union demanded strict communications discipline and used an effective substitution cypher, which coupled with a lack of crypto-analysts on the Confederate side meant that although the Union could read Confederate messages, the Confederacy could not routinely decrypt Union messages, giving the Union a large intelligence advantage (Sapp 2009).

Interestingly, the importance of communications secrecy and the opportunities provided to the enemy through intercepting military communications and using intelligence against operations has been forgotten and re-invented more than once. One hundred years after the successful use of communications intercepts during the American Civil War, the US Air Force was surprised to find that the North Vietnamese forces had up to 24 hours advanced warning of air operations during the Vietnam War. The North Vietnamese were able to intercept poorly encrypted communications and take advantage of unencrypted voice communications of incoming air strikes both to reduce the effectiveness of the missions and to increase the effectiveness of anti-aircraft fire (Johnson 1995a).

During the nineteenth century the various world powers of the time created dedicated Intelligence arms within their militaries (Wheeler 2012). These were of great use in processing the information generated from technological advances such as aerial reconnaissance, reports of enemy activity sent by field telegraph, and most importantly by the emerging technology of radio.

1.2.5 World War I

The utility of effective Intelligence was demonstrated in one of the early battles of the World War I, the Battle of Tannenberg in August 1914. The Russian plan was to destroy the German army forces in East Prussia through a pincer movement using the Russian First and Second armies. This plan required coordination and planning between the two army groups.

The Russian armies lacked the necessary cables to construct wired telegraph communication infrastructure, so they relied heavily on the mobility and range of radio communication. Unfortunately, they lacked trained signal troops and cryptographers. Hence, in order to ensure that orders and reports were received clearly, the Russian troops routinely conducted radio communication without encryption. These communications were consistently intercepted by the German army, swiftly translated and used to understand the location, disposition, and intentions of the Russian units (Norwitz 2001).

In addition, the German army used aerial reconnaissance reports to understand the supply situation for the Russians, and to verify the accuracy of radio intercepts. As the Russians advanced, human intelligence from the populace and disguised soldiers also greatly benefitted the Germans.

Through their understanding of the situation, the German army was able to use their numerically smaller forces to destroy the Russian Second Army, before repositioning to attack and defeat the Russian First Army. Despite lacking numerical superiority, the Germans were able to develop informational superiority and use this to their advantage, striking a decisive blow on the Eastern front from which Imperial Russia never recovered (Kahn 2006).

Effective Intelligence wasn't confined to the Eastern front. Throughout 1917 onwards, the movement of German forces to and from the Western front was being monitored by the '*La Dame Blanche*' network of spies. This network conducted espionage within occupied Belgium and France; by the end of the war, it was reliably reporting the movement of all German troops to British military Intelligence (Decock 2014).

Thus, as the German Spring Offensive of 1918 was being prepared, Allied forces were aware of the build-up and that an attack was imminent. In March 1918, days before the German offensive began, the German Army switched to using a new cypher to encrypt their communications. This ADFGX cypher was derived from the signalling techniques used in ancient Greece, providing an encryption technique that was both simple to implement by radio operations and believed to be uncrackable (Dipenbroek 2019).

Within one month of the cypher being used, the French cryptanalyst Georges Painvin was able to decrypt some messages. The Germans made changes to their cypher in order to improve it, but again Painvin was able to crack the cypher. Painvin was also able to distinguish that the Germans only changed their encryption keys daily when a major offensive was planned. This allowed him to identify not only the location of the attack planned for June 1918 from decrypted messages, but from the fact that this attack was associated with daily key changes, that it was an attack of great significance (de Lastours 2014).

In response to this intelligence, the French high command was able to reinforce the area and repulse the attack, citing the intercepted communication as '*Le Radiotélégramme de la Victoire*' (the radiogram of victory) (de Lastours 2014). Successful execution of this offensive was vital to Germany before the full deployment of American troops could be achieved by the Allies.

The entry into the war by the United States was itself partly due to Intelligence. The Germans proposed to the Mexican government that if the United States joined World War I on the side of the allies that Germany and Mexico should form an alliance. As part of this alliance Germany would support Mexico in acquiring their 'lost' territory including Texas, Arizona, and New Mexico.

The encrypted telegramme containing this offer was transmitted via the diplomatic telegraph cables of neutral Sweden and the US. The British intercepted and decrypted the message, but could not pass the plain text to the US without disclosing that they monitored the communications of neutral countries. This dilemma was solved by the British Ambassador in Mexico who arranged for an official copy of the document to be 'acquired' by him in return for a sum of money. Presumably, a bribe was paid to someone with legitimate access to the document, or possibly a third party was contracted to steal a copy of the document.

Armed with a 'legitimately' procured version of the document, the British were able to pass the document to the American government. Publication of this intelligence coup caused a furore amongst the American public, helping to convince an until then sceptical public to enter the war on the side of the Allies (von Gathen 2007).

1.2.6 World War II

The story of Bletchley Park and the work done there building on the work of French and Polish cryptanalysts to break the German Enigma cypher has been well documented elsewhere (Ferris 2020). In passing, it is interesting to reflect that the first electronic computers built as part of the effort at Bletchley Park were designed to break the communications secrecy of a third party. This history of modern computers is inseparable from that of cyber security. Electronic computers have been used to compromise data since their first invention.

The contribution of Bletchley Park to traffic analysis is often overlooked. Gordon Welchman was one of the early recruits to Bletchley Park along with Alan Turing. He recognised that there was much useful intelligence to be gleaned from the traffic analysis of enemy signals identifying when and from where a signal had been sent, even without requiring the message to be decrypted.

The patterns of communication used between enemy units in the field could be used to identify command structures, the locations of headquarters as distinct from subordinate units. The frequency of communications, often referred to as 'chatter', tells much about the activity of units with the frequency of communications increasing before conducting operations as orders are issued and situational reports broadcast.

Welchman was able to create a fusion centre within Hut Six of Bletchley Park where the metadata from communications analysis was combined with the decrypted content of messages to create intelligence, which was more valuable than either source of intelligence on its own (Grey 2012; Welchman 2017). Indeed, combining intelligence from many different sources enriches reports since each

independent source provides its own viewpoint on an issue. Many different perspectives and viewpoints help to provide a more complete picture.

> No-one else was doing anything about this potential goldmine; so, I drew up a comprehensive plan which called for close coordination of radio interception, analysis of the intercepted traffic, the breaking of Enigma keys, and extracting intelligence from the decodes. – G. Welchman
>
> *(Martin 2015)*

This intelligence process became known as SIXTA, derived from 'Hut Six Traffic Analysis'. The importance of this process to the war effort is emphasised by the fact that although the work of cryptographers, such as Alan Turing, in decoding the Enigma cypher is declassified, published and well described, the history of SIXTA at Bletchley Park remains classified as a state secret (National Archives 1945).

The use of radio detection equipment to triangulate the location of a radio transmitter had been developed during World War I as a method of locating U-Boats (Grant 2003). This technique named 'radiogoniometry', and later 'huff-duff', could pinpoint the source of radio transmissions from a ship or submarine to within a few miles (Markus 1946).

So successful was this technique that a series of radio direction finding stations were established throughout the UK, and abroad during World War II. This network of stations referred to as the Y Service, not only recorded the intercepted morse code signals, but provided intelligence regarding the locations of radio transmitters. Particularly skilled operators could distinguish characteristics in how the morse key was tapped while sending messages to recognise the individuals sending the message (McKay 2012).

The intercepted messages were sent to Bletchley Park for decryption. However, even before the content of the message was discovered, the Y Service and Traffic Analysis could provide the location from which the message was sent, the identity of the individual who sent the message, and the wider context of activity of which the message was part, thus providing even more enrichment to intelligence reports.

1.2.7 Post War Intelligence

At the end of World War II, the analysis of radio magnetic emissions had proved itself vital to the conduct of the war. This field of Signals Intelligence (SIGINT) was recognised as comprising two distinct disciplines: COMINT relating to the analysis of signals used for communications such as voice or text, and Electronic Intelligence (ELINT) relating to the analysis of non-communications signals such as radar emissions (NATO 2017c, NATO 2017d).

Analysis of the intelligence successes of the war identified that SIGINT had played a major part, and that the centralised intelligence function at Bletchley Park had greatly facilitated the production and dissemination of intelligence. On the other hand, German SIGINT efforts had floundered due to the existence of five separate cryptanalytic efforts, which competed for resources and refused to cooperate together (Johnson 1995b).

In the US the dangers of too many competing intelligence efforts were recognised leading to the creation of centralised intelligence agencies: the CIA in 1947, and the US National Security Agency (NSA) in 1952. Presumably, similar discussions were happening behind the Iron Curtain leading to the creation of the Soviet *Komitet Gosudarstvennoy Bezopasnosti* (KGB) in 1954, and the East German *Hauptverwaltung Aufklärung* foreign intelligence branch of the Ministry of State Security (Stasi) in 1955 (Johnston 2019).

Increasing SIGINT capabilities for gathering intelligence combined with awareness of how intelligence could assist decision making led to the development of management models by which intelligence efforts could be conceptualised and directed. Dating from this period, the Intelligence Cycle became the most widely known conceptual model of intelligence operations (Glass and Davidson 1948). This model remains in use today.

Beyond the immediate post war period, much of the history of the development of intelligence techniques remains classified and beyond the reach of civilian research in the private sector. However, the development of computing systems saw the interests of the largely civilian community of computer system operators overlap with those of security and intelligence agencies within the public sector. The former were seeking to assure the security and safety of the computer systems within their care, the latter seeking to assure the safety and security of nation states as part of their mission.

1.2.8 Cyber Threat Intelligence

The development of computers during the 1960s led to the deployment of the first multi-user systems within universities. Computing resources were limited and expensive, therefore username and password-enforced quotas and limits to users' access to these resources had to be implemented.

To a generation of young students gaining extra computing time proved a strong temptation, and password protection did not prevent illicit access (Walden and Van Vleck 2011). However, in an environment where everyone who could possibly access the device was known, the discovery and holding to account of the perpetrator could be expected, even if sanctions for the transgressor were mild (Yost 2012).

The existence of vulnerabilities in computer systems were known and widely shared within the system administrator community (Yost 2012). 'Tiger teams'

were formed to hunt security vulnerabilities, so that they could be rectified. The weaknesses of such an approach and the prevalence of security vulnerabilities were recognised by the United States Air Force (USAF),

> ... the tiger team can only reveal system flaws and provide no basis for asserting that a system is secure in the event their efforts are unsuccessful. In the latter event, the only thing that can be stated is that the security state of the system is unknown. It is a commentary on contemporary systems that none of the known tiger team efforts has failed to date.
>
> *(Anderson 1972)*

Indeed, the USAF identified that,

> Based on current experience with penetration exercises, and assuming the availability of an individual with technical familiarity with the target system, the cost to find and exploit at least one design or implementation flaw in virtually any contemporary system is one man-month of effort or less.
>
> *(Anderson 1972)*

By the mid-1970s, computer security issues were discussed, and incidents of computer abuse shared within the computer security community. Motivations of early computer criminals ranged from theft of proprietary data, unauthorised access to services, through to financial fraud (Parker 1976). This set of motivations would seem remarkably familiar to today's cyber security teams.

By the mid-1970s, security practitioners had identified the fundamental tenets of computer security (Saltzer and Schroeder 1975). These included the importance of what we would now recognise as cyber threat intelligence,

> Detection and effective reporting of anomalous activity within a computer system and its environment is equally as important as prevention of unauthorized acts ...
>
> Monitoring the use of computers could be important for detecting the possible planning or practicing for attacks on computers.
>
> *(Parker 1973)*

By 1980 the techniques for analysing system data to identify anomalous activity by users or systems had been developed. The detection of anomalies within system data highlighted activity that was outside of that considered 'normal'. However, anomalous behaviour is not necessarily evidence of malicious behaviour.

Uncovering malicious acts requires investigation by a security operative to piece together the series of actions associated with the anomalous behaviour. Only with

the context of the behaviour, identifying any actions that preceded or followed the anomaly, can any indication of malice and the potential source of the behaviour be uncovered (Anderson 1980).

Anderson's paper also made two observations that are as relevant today as when they were first published in 1980 (Anderson 1980). First, relating to the nature of the system data which we rely on to be able to identify malicious behaviour and incursions:

> security audit trails, if taken, are rarely complete and almost never geared to the needs of the security officers.

Second, relating to the difficulty of identifying the most sophisticated malicious users who have high-level access to a device, and who are able to use this access to erase their traces:

> The clandestine user who effects a technical penetration to obtain control of the most privileged state (of) the computer system, is not capable of being audited.

The 1983 film *WarGames*, in which a teenager played by Matthew Broderick succeeds in gaining unauthorised access to a Pentagon computer, and nearly brings about the world's destruction, brought the issue of computer security to the mainstream. The film captured the mood of the time, mixing themes of advances in computer technology and communications with cold war paranoia and the dangers of teenage 'hackers' (Schulte 2008).

The influence of the film extended to the White House, reportedly leading President Reagan to question his staff if such a scenario was possible. The reply that in reality, '*the situation is much worse than you think',* apocryphally led to the issuing of National Security Decision Directive (NSDD) 145 (White House 1984; Kaplan 2016).

NSDD 145 explicitly recognised that by the mid-1980s, computer and telecommunications systems were becoming inseparable. Despite increasing use of computer technology by the government and the private sector, '*the technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements*'. (White House 1984). Significantly, the directive recognised that the solution to addressing these risks involved both the public and private sectors working together and sharing information, if only due to the recognition that many systems of key national interest were being operated within the private sector.

The wording of NSDD 145, '*widespread and is used extensively by foreign nations*' hints at the existence of many known but unpublished incidents of computer

intrusions undertaken by hostile entities. There is an inherent conflict between the desire to keep such incidents classified as state secrets so as not to alert the attackers to cyber detection capabilities, and the possibility that publishing such reports might help develop detection capabilities within the private sector. This conflict has yet to be resolved.

The first in-depth description of the discovery, investigation, and identification of a hostile computer incursion over the Internet was published in 1988 when Clifford Stoll, a systems administrator at Lawrence Berkeley Laboratory was asked to investigate an accounting error. A new user account had been created, but the particular user did not have a billing address to which use of the computing facilities could be charged.

Over the following months, Stoll diligently collected information recording the activities of the unknown user, quickly identifying that this was a malicious attacker. The attacker was using the Lawrence Berkeley Laboratory computer system not only to search for and collect potentially sensitive information from the laboratory itself, but also as a site to launch further attacks on computer systems within the US, many of which were hosted by, or closely associated with the military (Stoll 1988).

Ultimately, the attacker was identified as a KGB agent based in Germany, and brought to justice. Stoll's publications characterised the method by which the attacker conducted their attack, allowing others to consider how they might detect and repel such an attack in the future, and provided detailed guidance on how the investigation was conducted, serving as a reference for how investigations should be conducted (Stoll 1987, 1989).

This incident served as a warning to the security community, illustrating that innocuous systems within the civilian sector may nevertheless become embroiled in activity, which may seem to have come straight from a spy film. Clearly, the nature of computer incidents, which administrators may have to resolve now included incursions by agents of nation state intelligence agencies.

As the volume of cyber attacks increased through the mid-2000s, it became steadily clear that a small percentage of these attacks were significantly different from the others (Lee and Lewis 2011). These attacks were distinguished by their sophistication, and by their persistence. Once the attacker had fixed on a target, the attacker patiently continued to launch attacks against the target for extended periods of time until they were successful (Thonnard et al. 2012).

The term Advanced Persistent Threat (APT) came to be used to refer to these sophisticated, patient, attackers. One characteristic of early APT attacks was that they did not appear to be conducted for clear financial gain. Indeed, many APT attacks appeared to be conducted in support of the objectives of a nation state. Although the identity of the attackers could not be discerned, the term APT came to be used as an umbrella term to refer to any attackers who appeared to be conducting a state-sponsored attack (Bejtlich 2010).

1.2.9 Emergence of Private Sector Intelligence Sharing

Not only was Stoll's uncovering of a KGB agent's infiltration of computer networks notable for being the earliest disclosure of nation state attacks against computer systems, but it was also a significant milestone in the development of threat intelligence outside of the state sector (Stoll 1988).

In its infancy, any issues with the operation of the Internet were resolved between administrators who for the most part, knew each other personally. This network of trust and interpersonal relationships was largely successful in managing risks. Online resources such as the Forum on Risks to the Public in Computers and Related Systems founded in August 1985, amongst other similar initiatives, provided a mechanism by which information regarding cyber risks and vulnerabilities could be shared amongst the community (Neumann 1985; Slayton and Clarke 2020).

This informal information sharing model was severely tested by the Morris Worm in 1988. The worm spread autonomously and rapidly between connected systems, infecting systems multiple times over leading to resource depletion and denial of service (Orman 2003). The worm severely affected many institutions bringing IT services to their knees. However, without a single point of contact offering authoritative information and advice, administrators were left struggling to manage the many sources of advice and remediation (Slayton and Clarke 2020).

In response, the Defense Advanced Research Projects Agency (DARPA) funded the creation of the Computer Emergency Response Team Coordinating Center (CERT/CC) at the Software Engineering Institute of Carnegie Mellon University. The team was established to provide advice and services to those affected by computer incidents, and ultimately to act as a middle-man between researchers who had identified software vulnerabilities, and the vendors of the affected software who needed to provide remediation (Allen and Pethia 2006). This model proved a successful template for national CERT organisations that was replicated globally (Slayton and Clarke 2020).

How the details of vulnerabilities should be handled proved to be a contentious issue. One group espoused that information regarding vulnerabilities was highly sensitive and should be kept secret until a suitable remediation was available. At the point of public disclosure, only a minimum of information should be released to ensure that attackers couldn't learn how to exploit the vulnerability. This was the model adopted by CERT/CC. Others believed that information about vulnerabilities should be shared early, widely, and with as much detail as possible so that administrators could take steps to protect their systems before official remediation was released.

This schism led to the creation of the Bugtraq mailing list in 1993, a public mailing list where computer security issues could be publicly discussed, and where

researchers could disclose vulnerabilities that they had identified. The detail of technical discussion within the mailing list helped both vulnerability researchers and system administrators refine their skills. However, the potential price of such a discourse was that the same information could be used by attackers to refine and advance their own skills and create attack code quicker than may otherwise have been possible (Goerzen and Coleman 2022).

Yet, the development of detailed knowledge within the private sector was a source of strength. Discussions of vulnerabilities, security incidents, and protections developed organically into widely adopted practices for defending systems. The presidential commission on protecting critical infrastructure found that there was a need to improve information flow between the operators of critical infrastructure and the public sector. Operators would benefit from specialist knowledge within the public sector, and in turn the public sector could learn from the know-how and identification of cyber attacks within the private sector (Marsh 1997).

Aggregating and sharing threat intelligence both vertically between the private and public sectors, and horizontally amongst peers within industry sectors proved to be a compelling model for cooperation. The Presidential Decision Directive 63 (PDD-63) established Information Sharing and Analysis Centers (ISACs) by which trusted participants from industry could share intelligence together with representatives from law enforcement (White House 1998).

In parallel with the growing number of threats and attacks, private sector companies offering security solutions to detect and block threats also grew in number and capability. Protecting against the emerging threats such as computer viruses and trojans required collecting and analysing large numbers of the malware used in attacks (Kephart et al. 1997; Mezzour et al. 2016).

Over time, not only could providers of security services in the private sector detect distinct attacks, but also correlate many attacks against different victims into wider campaigns of activity carried out by a single threat actor. This intelligence gathering capability had previously been the preserve of the nation state.

In 2013, Mandiant had been able to collect sizable amounts of information relating to a single threat actor behind a large number of cyber attacks whom they referred to as APT1, which had been in operation since 2004. Unprecedentedly, Mandiant was able to identify the entity behind APT1, and feel secure enough in their conclusions to name the threat actor as a branch of the Chinese military (Mandiant Intelligence Center 2013).

In parallel, teams capable of performing in-depth investigations of cyber threats, and risks to human rights on the Internet developed within academia. The reports produced by entities such as Citizen Lab within the University of Toronto (Citizen Lab 2018), or the Georgia Tech Information Security Center (now part of the School of Cybersecurity and Privacy), provided balanced and open reporting and intelligence on emerging cyber security threats (Ahamad et al. 2008).

Stimulated by the ability of the private sector to generate cyber threat intelligence, and the hunger of organisations to understand cyber threats and to protect networks, commercial organisations such as Digital Shadows and Recorded Future were founded specifically to provide cyber threat intelligence to the private sector.

Alongside the commercial supply of threat intelligence, the non-profit organisation Bellingcat has emerged as an independent purveyor of intelligence, using the plethora of raw data and existing published intelligence reports to highlight human rights abuse and otherwise hidden conflicts.

Previously these capabilities were confined to national intelligence agencies. Intelligence agenies have not resisted the emergence of intelligence provision within the private sector. Indeed, the CIA has welcomed the work of Bellingcat as a means of discussing the policy implications of the attacks identified by the private sector without disclosing the classified intelligence gathering capabilities of the public sector (Mackinnon 2020).

1.3 Utility of Threat Intelligence

Put simply, you cannot protect against threats if you do not know that they exist, or do not understand their nature. This is the utility of threat intelligence, to describe what might cause harm so that decision makers can understand the threats they face and take appropriate action.

The process of generating threat intelligence results in information. On its own, this information is of little use. The ultimate utility of threat intelligence is in its application, putting the information to good use in support of an organisation's objectives.

These objectives should be set by the senior decision makers within the organisation and underpinned by a risk management strategy, which considers everything that might impede attaining those objectives.

Threat intelligence should inform and support the risk management process. Cyber threat intelligence specifically affects everything to do with risks relating to networked computer systems and the operations that these systems perform. As technology increasingly assists and enhances everything within our professional and personal lives, networked computer systems perform vital functions within our society. Cyber threat intelligence seeks to inform how we protect these vital systems against threats.

The threat landscape is dynamic and in constant flux. As an organisation's strengths and weaknesses change over time, so do those of attackers. The capabilities and ambitions of attackers evolve. Put bluntly, bad guys don't get any dumber. Threat intelligence reports on these changes, flowing into the risk management process so that our understanding of risk and the adequacy of our defences

changes accordingly. With better understanding of our weaknesses and the emerging strengths of those who would do us harm, we can make decisions regarding the allocation of resources to best protect us from harm.

Organisations may already by conducting threat intelligence under a different name. Risk management processes such as NIST SP 800-39 or ISO/IEC 27005 may already be in use within an organisation, and activities related to keeping abreast of current threats may be in place.

The NIST SP 800-39 framework describes how organisations should frame risk, i.e. place it within the context of the business and its operations; assess risk, i.e. understand likelihoods and potential impact; respond to risk once determined and monitor risk as a continuous activity (NIST SP 800-39 2011) (Figure 1.1).

Threat intelligence drives the assessment of risk through the description of the threats, which may impact an organisation. Similarly, the monitoring of risk is also a threat intelligence activity since we seek to understand how threats and our exposure to them evolves (Figure 1.2).

The ISO/IEC 27005 risk management process is subtly different. Organisations identify and estimate risk as part of a risk analysis process, including this with risk evaluation to form a risk assessment process. If the risk assessment process is satisfactory, the identified risks are managed through risk treatment.

Threat intelligence should drive the risk assessment process, again through describing the threats which they may impact. Communicating information about these risks is a threat intelligence activity in itself, informing others so they can make appropriate decisions and modify behaviour if required. Similarly, the ongoing review and monitoring of risk is also threat intelligence. The threat landscape is constantly changing: monitoring these changes is part of threat intelligence.

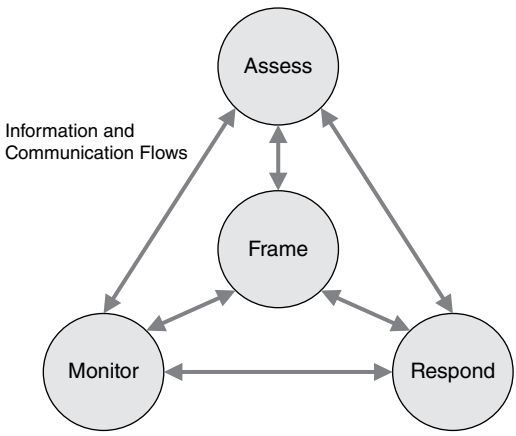

Figure 1.1 NIST SP 800-39 risk management process. *Source:* Adapted from NIST SP 800-39 2011.

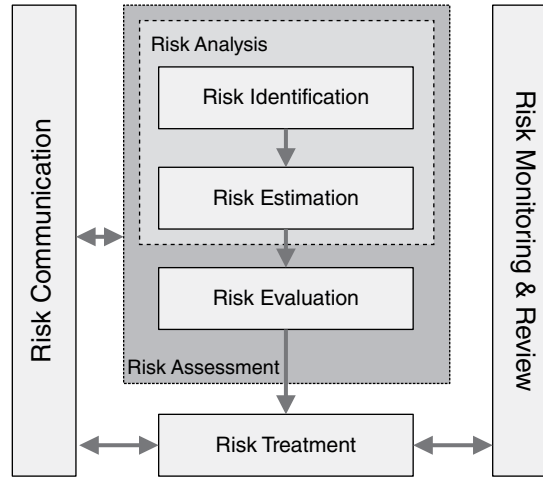

Figure 1.2 Detail of ISO/IEC 27005 risk management process. *Source:* Adapted from ISO/IEC 27005 2018.

1.3.1 Developing Cyber Threat Intelligence

Cyber threat intelligence is concerned specifically with threats to networked electronic systems. Understanding the threats against these computer systems and the consequent risks to the organisation requires developing a cyber threat intelligence programme.

This programme can identify the relevant threats, feeding into the risk management process, and providing intelligence to manage these threats. However, as this programme is developed the goals and requirements of the programme need to be clearly stated, and a plan formulated to decide how the capabilities of the cyber threat intelligence function will be developed over time to reach the required standard. Organisations should have a clear idea of why intelligence is needed, exactly how the intelligence will be used, and how the success of the intelligence programme will be measured.

Similarly, an organisation should have an understanding of the limits of threat intelligence. An intelligence function cannot foresee the future or read the minds of adversaries. The unpredicted and unpredictable does happen. Threat intelligence can provide three types of insight as to what might happen, or what is currently happening:

- Strategic threat intelligence – Describing long term changes, and the long term objectives of adversaries. Intended to be read by senior executives to drive long term strategy and priorities.
- Operational threat intelligence – Describing short to medium term changes in the threat landscape, and the current techniques used by adversaries. Intended to be read by security teams to help manage short term priorities and the current situation.

- Tactical (or technical) threat intelligence – Describing what is happening at this moment in time within the threat landscape. Largely intended to be read by machine to manage the immediate situation.

Security teams should be mindful of the words of Frederick the Great of Prussia, '*he who defends everything, defends nothing*'. It is fanciful to expect that every system within an organisation can be protected to a maximum extent. Resources are not infinite, and compromises must be made trading off security against usability.

Every system deserves at least a minimum level of protection. However, some systems require more protection than others due to the risk they pose to the organisation. Indeed, some systems will constitute the 'crown jewels' of an organisation, to the point that if they were successfully attacked the organisation would suffer extreme consequences.

This is where threat intelligence augments risk management. While risk management considers the risk (what might go wrong), threat intelligence considers how an eventuality might be achieved (how might it happen). Threat intelligence allows security teams to focus on what is *likely* to happen rather than what *might* happen, and to take a proactive approach in responding to a changing threat environment.

Threat intelligence is uncertain. This degree of uncertainty must be quantified and expressed. Nevertheless, threat intelligence can increase understanding within an uncertain world, driving good decision making, and when the threat landscape changes, provide a rapid indication of the nature of these changes so that informed decisions can be swiftly taken.

Summary

Cyber threat intelligence is both the process and outcome of studying threats against networked computer systems. The goal of threat intelligence is to inform decision makers about threats so that better decisions can be made.

Threat intelligence has a long history dating back to antiquity. With the advent of the Internet, and the development of computer systems, cyber threat intelligence has emerged as a speciality and a capability within the private sector.

References

Ahamad, M., Amster, D., Barrett, M. et al. (2008). *Emerging Cyber Threats Report for 2009*. Georgia Tech Information Security Center. https://smartech.gatech.edu/bitstream/handle/1853/26301/CyberThreatsReport2009.pdf.

Al-Kadit, I.A. (1992). Origins of cryptology: the Arab contribution. *Cryptologia* 16 (2): 97–126.

Allen, J. and Pethia, R. (2006). *Lessons Learned: A Conversation with Rich Pethia, Director of CERT Transcript, Part 1: CERT History*. Carnegie Mellon University. https://apps.dtic.mil/sti/pdfs/AD1130301.pdf (accessed 13 January 2023).

Anderson, J.P. (1972). Computer Security Technology Planning Study. Report to USAF Deputy for Command and Management Systems, HQ Electronic Systems Division. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf (accessed 13 January 2023).

Anderson, J.P. (1980). *Computer Security Threat Monitoring and Surveillance*. James P. Anderson Company. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf.

Austin, N.J.E. and Rankov, N.B. (1998). *Exploratio: Military and Political Intelligence in the Roman World from the Second Punic War to the Battle of Adrianople*. Psychology Press.

Baker, O.R. (2022). Gorgo: Sparta's woman of autonomy, authority, and agency. *Athens Journal of Humanities & Arts* 9 (2): 145–158.

Bank of England (2016). CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations version 2.0. www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf (accessed 13 January 2023).

Bejtlich, R. (2010). Understanding the advanced persistent threat. *Information Security Magazine Online* (13 July).

Bimfort, M.T. (1958). A definition of intelligence. *Studies in Intelligence* 2: 75–78.

Broemeling, L.D. (2011). An account of early statistical inference in Arab cryptology. *The American Statistician* 64 (4): 255–257.

Bruen, A.A. and Forcinto, M.A. (2011). *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*. Wiley.

Calof, J.L. and Skinner, B. (1998). Competitive intelligence for government officers: a brave new world. *Optimum* 28 (2): 38–42.

Campbell, B. and Tritle, L.A. (2013). *The Oxford Handbook of Warfare in the Classical World*. Oxford University Press.

Citizen Lab (2018). *The Citizen Lab*. University of Toronto. https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf (accessed 13 January 2023).

Coe, T. (2015). Where does the word cyber come from? *OUP Blog* (28 March). https://blog.oup.com/2015/03/cyber-word-origins (accessed 13 January 2023).

Crowther, G.A. (2017). The cyber domain. *The Cyber Defense Review* 2 (3): 63–78.

De Leeuw, K. (1999). The black chamber in the Dutch Republic during the war of the Spanish succession and its aftermath, 1707–1715. *The Historical Journal* 42 (1): 133–156. https://doi.org/10.1017/S0018246X98008292.

Decock, P. (2014). 'La Dame Blanche', *1914–1918-online. International Encyclopedia of the First World War.* https://doi.org/10.15463/ie1418.10241.

Dipenbroek, M. (2019). From fire signals to ADFGX. A case study in the adaptation of ancient methods of secret communication. *KLEOS Amsterdam Bulletin of Ancient Studies and Archaeology* 2 (Apr): 63–76.

Dugald, S., Playfair, J., Macintosh, J. et al. (1842). *Post Office*. Encyclopaedia Britannica. https://jstor.org/stable/10.2307/community.27604311.

Dylan, H. (2012). The joint intelligence bureau: (not so) secret intelligence for the post-war world. *Intelligence and National Security* 27 (1): 27–45.

Edwards, F. (2007). Review: Robert Hutchinson, Elizabeth's Spy Master. *Francis Walsingham and the Secret War that Saved England*, Weidenfeld and Nicolson, 2006, ISBN: 10 0 297 84613 2, pp. 399. *Recusant History* 28 (3): 483–488. https://doi.org/10.1017/S0034193200011535.

Emmott, R. (2018). NATO cyber command to be fully operational in 2023. *Reuters* (26 October). https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9 (accessed 13 January 2023).

Evov, A. (1996). The 'missing dimension' of C. Julius Caesar. *Historia: Zeitschrift Für Alte Geschichte* 45 (1): 64–94.

Fabien, A.P., Anderson, R.J., and Kuhn, M.G. (1999). Information hiding: a survey. *Proceedings of the IEEE* 87 (7): 1062–1078. https://doi.org/10.1109/5.771065.

Farhat-Holzman, L. (2007). Stephen Budiansky, *Her Majesty's spymaster: Elizabeth I, Sir Francis Walsingham, and the birth of modern espionage. Comparative Civilizations Review* 56 (56): 121–122.

Ferdinando, L. (2018). *Cybercom to Elevate to Combatant Command*. US Department of Defense Press Release. https://www.defense.gov/Explore/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command (accessed 13 January 2023).

Ferris, J. (2020). *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*. Bloomsbury Publishing.

Fijnaut, C. and Marx, G.T. (1995). *Undercover, Police Surveillance in Comparative Perspective*. Kluwer Law International.

FIRST, Cyber Threat Intelligence SIG (2018). Introduction to CTI as a general topic. https://www.first.org/global/sigs/cti/curriculum/cti-introduction (accessed 13 January 2023).

Gartner Research and McMillan, R. (2003). Definition: Threat Intelligence. https://www.gartner.com/en/documents/2487216/definition-threat-intelligence (accessed 13 January 2023).

von Gathen, J. (2007). Zimmermann telegram: the original draft. *Cryptologia* 31 (1): 2–37.

Giles, L. (1910). *Sun Tzu on the Art of War*. Project Gutenberg. https://www.gutenberg.org/files/132/132-h/132-h.htm.

Glass, R.R. and Davidson, P.B. (1948). *Intelligence Is for Commanders*. The Telegraph Press.

Goerzen, M. and Coleman, G. (2022). *Wearing Many Hats. The Rise of the Professional Security Hacker*. Data & Society. https://datasociety.net/wp-content/uploads/2022/03/WMH_final01062022Rev.pdf.

Grant, R.M. (2003). *U-Boat Hunters, Code Breakers, Divers and the Defeat of the U-Boats, 1914–1918*. Periscope Publishing Ltd.

Grey, C. (2012). Understanding Bletchley Park's work. In: *Decoding Organization: Bletchley Park, Codebreaking and Organization Studies*, 213–244. Cambridge University Press.

Hillenbrand, T. (2017). *The King's NSA. From 1684 to 1984*. Epubli.

Iordanou, I. (2018). The professionalization of cryptology in sixteenth-century Venice. *Enterprise & Society* 19 (4): 973–1013. https://doi.org/10.1017/eso.2018.10.

ISO/IEC 27005:2018 (2018). *Information Technology – Security Techniques – Information Security Risk Management*. International Standards Organization. https://www.iso.org/standard/75281.html (accessed 13 January 2023).

Johnson, T.R. (1995a). From Tonkin to Tet – the heart of the war. In: *American Cryptology During the Cold War, 1945–1989. Book II: Centralization Wins, 1960–1972*, 528–558. Center for Cryptologic History. National Security Agency. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB260/nsa-4.pdf.

Johnson, T.R. (1995b). AFSE and the creation of NSA. In: *American Cryptology during the Cold War, 1945–1989. Book 1: The Struggle for Centralization 1945–1960*, 23–59.

Johnston, M.K. (2019). The paradigm shifts in intelligence: from 1800 to present. *Illini Journal Of International Security* 5 (1): 56–64.

Kahn, D. (2006). The rise of intelligence. *Foreign Affairs* 85 (5): 125–134. https://doi.org/10.2307/20032075.

Kaplan, F. (2016). 'WarGames' and cybersecurity's debt to a Hollywood hack. *The New York Times* (19 February). https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html (accessed 13 January 2023).

Kephart, J.O., Sorkin, G.B., Chess, D.M., and White, S.R. (1997). Fighting computer viruses. *Scientific American* 277 (5): 88–93.

de Lastours, S. (2014). Les Travaux de la Section du Chiffre Pendant La Première Guerre Mondiale. *Cryptologie et mathématiques: Une mutation des enjeux* 87: 87–106.

Lee, M. (2014). History of hacking. *Engineering & Technology Reference* 1–7. https://doi.org/10.1049/etr.2014.0011.

Lee, M. and Lewis, D. (2011). Clustering disparate attacks: mapping the activities of the advanced persistent threat. *Proceedings of the 21st Virus Bulletin International Conference*.

Leimon, M. and Parker, G. (1996). Treason and plot in Elizabethan diplomacy: the 'Fame of Sir Edward Stafford' reconsidered. *The English Historical Review* 111 (44): 1134–1158.

Ma, J., Ning, H., Huang, R. et al. (2015). Cybermatics: a holistic field for systematic study of cyber-enabled new worlds. *IEEE Access* 3: 2270–2280.

MacAskill, E. and Dance, G. (2013). NSA Files: Decoded. What the revelations mean for you. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (accessed 13 January 2023).

Mackinnon, A. (2020). Bellingcat can say what U.S. intelligence can't. *Foreign Policy* (17 December). https://foreignpolicy.com/2020/12/17/bellingcat-can-say-what-u-s-intelligence-cant (accessed 13 January 2023).

Mandiant Intelligence Center (2013). APT1: Exposing One of China's Cyber Espionage Units. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed 13 January 2023).

Marcus, H. and Findlen, P. (2019). Deciphering Galileo: communication and secrecy before and after the trial. *Renaissance Quarterly* 72 (3): 953–955.

Markus, J. (1946). Huff Duff. *Scientific American* 174 (4): 155–157.

Marsh, R.T. (1997). Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. https://www.ojp.gov/ncjrs/virtual-library/abstracts/critical-foundations-protecting-americas-infrastructures (accessed 13 January 2023).

Martin, A.J. (2015). Bletchley Park remembers 'forgotten genius' Gordon Welchman. *The Register* (27 September). https://www.theregister.com/2015/09/27/gordan_welchman_bletchley_park_remembers/?page=1 (accessed 13 January 2023).

Mavroeidis, V. and Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *2017 European Intelligence and Security Informatics Conference (EISIC)*, 91–98. IEEE. https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis%25282017%2529.pdf (accessed 13 January 2023).

McDermott, J.J. (2002). *Reading the Pentateuch: An Historical Introduction*. Paulist Press.

McKay, S. (2012). *The Secret Listeners. How the Y Service Intercepted the German Codes for Bletchley Park*. Arum Press Ltd.

Mezzour, G., Carley, L.R., and Carley, K.M. (2016). Longitudinal analysis of a large corpus of cyber threat descriptions. *Journal of Computer Virology and Hacking Techniques* 12 (1): 11–12. https://doi.org/10.4102/sajim.v15i2.559.

National Archives (1945). GC&CS Sixta History. An account of the work of the Traffic Analysis Party at Bletchley. https://discovery.nationalarchives.gov.uk/details/r/C11177401 (accessed 13 January 2023).

NATO Terminology Office (2017a). *Intelligence*. NATOTerm, The Official NATO Terminology Database. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (accessed 13 January 2023).

NATO Terminology Office (2017b). *Cyberspace*. NATOTerm, The Official NATO Terminology Database. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (accessed 13 January 2023).

NATO Terminology Office (2017c). *COMINT*. NATOTerm, The Official NATO Terminology Database. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (accessed 13 January 2023).

NATO Terminology Office (2017d). *ELINT*. NATOTerm, The Official NATO Terminology Database. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (accessed 13 January 2023).

Neumann, P.G. (1985). Welcome! *The RISKS Digest. Forum on Risks to the Public in Computers and Related Systems* 1 (1). https://catless.ncl.ac.uk/Risks/1/1#subj1.1.

Newitz, A. (2013). The bizarre evolution of the word 'Cyber'. *Gizmodo* (16 September). https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (accessed 13 January 2023).

NIST SP 800-39 (2011). *NIST Special Publication 800-39. Managing Information Security Risk Organization, Mission, and Information System View*. National Institute of Standards and Technology, US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf (accessed 13 January 2023).

Norwitz, J.H. (2001). Leveraging Operational Intelligence: The Battle of Tannenberg and Masurian Lakes (1914). *NAVAL WAR COLL NEWPORT RI* [Preprint].

Numbers 13:17–19 (n.d.). *King James Bible*.

Orman, H. (2003). The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy* 1 (5): 35–43.

Parker, D.B. (1973). Threats to Computer Systems. Report for US Atomic Energy Commission, Lawrence Libermore Laboratory. https://apps.dtic.mil/sti/pdfs/ADA587846.pdf (accessed 13 January 2023).

Parker, D.B. (1976). Computer abuse perpetrators and vulnerabilities of computer systems. *Proceedings of the June 7–10, 1976, National Computer Conference and Exposition*. AFIPS '76, 65–73. https://doi.org/10.1145/1499799.1499810.

Pellissier, R. and Nenzhelele, T.E. (2003). Towards a universal definition of competitive intelligence. *SA Journal of Information Management* 15 (2): 559. https://doi.org/10.4102/sajim.v15i2.559.

Reinke, E.C. (1962). Classical cryptography. *The Classical Journal* 58 (3): 113–121.

Saltzer, J.H. and Schroeder, M.D. (1975). The protection of information in computer systems. *Proceedings of the IEEE* 63 (9): 1278–1308.

Sapp, R. (2009). No room for gentlemen: cryptography in American history. *Historia* 21: 1–11.

Schulte, S.R. (2008). 'The WarGames scenario' regulating teenagers and teenaged technology (1980–1984). *Television & New Media* 9 (6): 487–513.

Shaw, C. (2000). Keeping track. In: *The Politics of Exile in Renaissance Italy*, 143–171. Cambridge University Press.

Slayton, R. and Clarke, B. (2020). Trusting infrastructure: the emergence of computer security incident response, 1989–2005. *Technology and Culture* 61 (1): 173–206.

Stoll, C. (1987). What do you feed a Trojan horse? *Proceedings of the 10th National Computer Security Conference*, 21–24.

Stoll, C. (1988). Stalking the wily hacker. *Communications of the ACM* 31 (5): 484–497.

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday.

Strate, L. (1999). The varieties of cyberspace: problems in definition and delimitation. *Western Journal of Communication* 63 (3): 382–412. https://doi.org/10.1080/10570319909374648.

Thonnard, O., Bilge, L., O'Gorman, G. et al. (2012). Industrial espionage and targeted attacks: understanding the characteristics of an escalating threat. *International Workshop on Recent Advances in Intrusion Detection*, 64–85. Springer-Verlag.

Vause, E. (2014). 'The business of reputations': secrecy, shame, and social standing in nineteenth-century French Debtors' and Creditors' newspapers. *Journal of Social History* 48 (1): 47–71.

Walden, D. and Van Vleck, T. (ed.) (2011). *Compatible Time-Sharing System (1961–1973) Fiftieth Anniversary Commemorative Overview*. IEEE Computer Society. https://history.computer.org/pubs/2011-06-ctss.pdf.

Warner, M. (2002). Wanted: a definition of intelligence. *Studies in Intelligence* 46 (3): 15–22.

Welchman, G. (2017). Ultra revisited, a tale of two contributors. *Intelligence and National Security* 32 (2): 244–255. https://doi.org/10.1080/02684527.2016.125322.

Wheeler, D.L. (2012). A guide to the history of intelligence 1800–1918. *Intelligencer: Journal of U.S. Intelligence Studies* Winter/Spring: 47–50.

White House (1984). National Security Decision Directive Number 145. National Policy on Telecommunications and Automated Information Systems Security. https://fas.org/irp/offdocs/nsdd145.htm (accessed 13 January 2023).

White House (1998). Presidential Decision Directive 63. The White House. https://irp.fas.org/offdocs/pdd/pdd-63.htm (accessed 13 January 2023).

Yost, J.R. (2012). *Oral History Interview with Thomas Van Vleck*. Computer Security History Project, Charles Babbage Institute, University of Minnesota. https://conservancy.umn.edu/bitstream/handle/11299/144020/oh408tvv.pdf (accessed 13 January 2023).