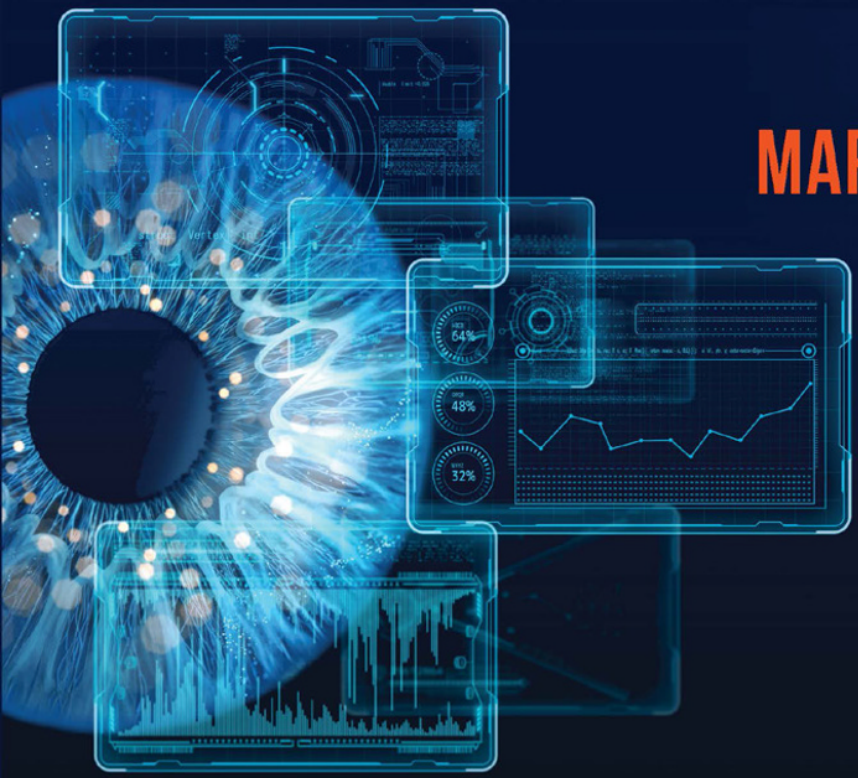
CYBER THREAT INTELLIGENCE



MARTIN LEE

WILEY

Cyber Threat Intelligence

Cyber Threat Intelligence

Martin Lee
Oxford, UK

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data

Names: Lee, Martin (Computer security expert), author.
Title: Cyber threat intelligence / Martin Lee.
Description: Oxford, UK ; Hoboken, NJ, USA : Wiley, 2023. | Includes bibliographical references and index.
Identifiers: LCCN 2022047002 (print) | LCCN 2022047003 (ebook) | ISBN 9781119861744 | ISBN 9781119861751 (adobe pdf) | ISBN 9781119861768 (epub)
Subjects: LCSH: Cyber intelligence (Computer security) | Cyberterrorism–Prevention. | Cyberspace operations (Military science)
Classification: LCC TK5105.59 .L47 2023 (print) | LCC TK5105.59 (ebook) | DDC 005.8/7–dc23/eng/20221205
LC record available at https://lccn.loc.gov/2022047002
LC ebook record available at https://lccn.loc.gov/2022047003

Cover Design: Wiley
Cover Image: © Yuichiro Chino/Getty images

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

Contents

Preface

Cyber Threat Intelligence describes the intelligence techniques and models used in cyber threat intelligence. It provides a survey of ideas, views, and concepts, rather than offering a hands-on practical guide. It is intended for anyone who wishes to learn more about the domain, possibly because they wish to develop a career in intelligence, and as a reference for those already working in the area.

The origins of this book lie in an awkward dinner conversation. I was on one side of the table, a software engineer who had fallen into the domain of cyber security more or less by accident. On the other was a uniformed senior military intelligence officer. A shared professional interest in cyber threat intelligence led to our being invited to the same event.

Keen to learn how better to analyse the attacks that I was encountering, I tried to learn all that I could about intelligence techniques from my neighbour. Naively, I had hoped that there might be a text book that set out the approaches that I could try to apply to identify attackers. At the very least, I was certain that there must be conceptual models, which I could adapt from the intelligence world to make better use of my data.

Instead, I discovered that military intelligence officers do not impart their knowledge to civilians easily, nor do they particularly appreciate lengthy questioning about the details of their profession. My conclusion was that I would have to develop my own body of knowledge regarding intelligence techniques and learn how to apply these to the emerging issue of cyber security.

This book is the result of that dinner. It is the book that I had hoped to discover when I started working in the nascent domain of cyber threat intelligence. It is the book that outlines the concepts and theories, which serve as the foundation of sound professional practice and the development of new practical applications.

Cyber threat intelligence is so much more than feeds of technical indicators relating to current cyber attacks. It is a discipline that is distinct from forensic cyber analysis, or malware analysis, seeking not necessarily to supply raw information detailing attacks, but to enrich such information to provide understanding.

Many working in the domain of cyber threat intelligence have been formally trained in intelligence through having followed careers in the military or law enforcement. However, professional obligations to protect sensitive operational details mean that it is often difficult to share knowledge and competences developed over long careers.

As a civilian working in the private sector, I have learned what I can about traditional threat intelligence theories and techniques from declassified or open-source material under the mentorship of formally trained senior colleagues. The nascent domain of cyber security has also had to develop its own specialised techniques and vocabulary derived from a large community of people working together to solve new problems.

This book is a collection of the techniques and theories that underpin the practice of cyber threat intelligence. The domain continues to evolve rapidly. The day-to-day tools and analyses performed by threat intelligence teams may change frequently, but the theory and frameworks in which these activities take place are well developed. It is these mature, evolved disciplines that this book seeks to describe.

This book approaches cyber threat intelligence from a perspective that is western and predominantly that of NATO and EU countries. Although the book is not partisan in nature, the reader should be aware that there are other perspectives.

I am indebted to a long line of people with whom I have worked over the years, who have helped me discover resources and techniques, and who have given me support and encouragement. This book has benefitted from the wisdom and oversight of Dr. Herb Mattord, Dr. Jonathan Lusthaus, Vanja Svajcer, Paul King, Wendy Nather, Don Taggart, and Natasha King who helped in the preparation of the manuscript.

About the Author

As EMEA Lead of the Strategic Planning and Communication team within Talos, Cisco's threat intelligence and security research organisation, Martin Lee researches the latest developments in cyber security and endeavours to ensure that organisations are aware of emerging threats and how to mitigate them.

Having worked in the field of detecting cyber threats since 2003, he has established and led threat intelligence teams on three continents. A Certified Information Systems Security Professional (CISSP) and a Chartered Engineer, Martin holds degrees from the Universities of Bristol, Cambridge, Paris-Sud, and Oxford. He is a member of the technical advisory board to Europol, and has delivered lectures on threat intelligence to students at the Universities of Oxford, Warwick, Kennesaw State, and l'Ecole Polytechnique, Paris.

An England Athletics licenced leader in running fitness, when not sat in front of a screen, Martin is often found running in the countryside or encouraging others to run for pleasure.

Abbreviations

$(ISC)^2$	Information System Security Certification Consortium
ABS	Anti-lock Braking System
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BCE	Before the Common Era
CAPEC™	Common Attack Pattern Enumeration and Classification
CE	Common Era
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordinating Center
CIA	Central Intelligence Agency
CIDR	Classless Inter-Domain Routing
CISA	Cybersecurity and Infrastructure Security Agency
CISSP	Certified Information Systems Security Professional
COE	Council of Europe
COMINT	Communications Intelligence
COMSEC	Communications Secrecy
CPU	Central Processing Unit
CREST	Council of Registered Ethical Security Testers
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE™	Common Weakness Enumeration
D3A	Decide, Detect, Deliver, Assess
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name System
DoS	Denial of Service

DPRK	Democratic People's Republic of Korea
EDRPOU	Unified State Registration Number of Enterprises and Organizations of Ukraine
ELINT	Electronic Intelligence
ENISA	European Network Information Security Agency
EU	European Union
F2T2EA	Find, Fix, Track, Target, Engage, Assess
F3EAD	Find, Fix, Finish, Exploit, Analyse, and Disseminate
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FTP	File Transfer Protocol
GB	Gigabytes
GDPR	General Data Protection Regulation
GIAC	Global Information Assurance Certification
HSE	Health Services Executive (of Ireland)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning
ICAO	International Civil Aviation Organization
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESBA	International Ethics Standards Board for Accountants
IoCs	Indicators of Compromise
IODEF	Incident Object Description Exchange Format
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
JSON	JavaScript Object Notation
KGB	Committee for State Security (of Soviet Union)
MAEC	Malware Attribute Enumeration and Characterization
MIDI	Musical Instrument Digital Interface
MIME	Multipurpose Internet Mail Extensions

MISP	Malware Information Sharing Platform
MPEG	Motion Picture Experts Group
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre (of the United Kingdom)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSDD	National Security Decision Directive
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OSI	Open System Interconnection
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standards
PDD	Presidential Decision Directive
PMI	Project Management Institute
PPP	Point-to-Point Protocol
RAM	Random Access Memory
RAT	Remote Access Trojan
RC4	Rivest Cipher 4
RCE	Remote Code Execution
RJ45	Registered Jack 45
RS-232	Recommended Standard 232
SANS	SysAdmin, Audit, Network, and Security (Institute)
SCADA	Supervisory Control and Data Acquisition
SFIA	Skills Framework for the Information Age
SGAM	Structured Geospatial Analytical Method
SIGINT	Signals Intelligence
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMBv1	Server Message Block version 1
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOCKS	Socket Secure
SQL	Structured Query Language
STIX	Structured Threat Information eXpression
SVR	Foreign Intelligence Service of the Russian Federation
SWIFT	Society for Worldwide Interbank Financial Telecommunication

TAXII	Trusted Automated eXchange of Indicator Information
TCP	Transmission Control Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
UDP	User Datagram Protocol
UEBA	User and Entity Behaviour Analytics
UEFA	Union of European Football Associations
UK	United Kingdom
UN	United Nations
URL	Uniform Resource Locator
USA / US	United States of America
USAF	United States Air Force
USB	Universal Serial Bus
UTC	Universal Time Coordinated
VERIS	Vocabulary for Event Recording and Incident Sharing
VoIP	Voice over Internet Protocol
WMIC	Windows Management Instrumentation Command
XML	eXtensible Markup Language

Endorsements for Martin Lee's Book

"Martin takes a thorough and focused approach to the processes that rule threat intelligence. But he doesn't just cover gathering, processing and distributing intelligence. He explains why you should care who is trying to hack you. And what you can do about it when you know."

—Simon Edwards, Security Testing Expert, CEO SE Labs Ltd., Chair AMTSO

"I really enjoyed this engaging book, which beautifully answered one of the first questions I had coming into the profession of cyber security: "What is Cyber Threat Intelligence?"

It progressively walked me through the world of cyber threat intelligence, peppered with rich content collected through years' of experience and knowledge. It is satisfyingly detailed to make it an interesting read for those already in cyber security wanting to learn more, but also caters to those who are just curious about the prevalent cyber threat and where it may be headed.

One of the takeaways from this book for me is how finding threats is not the most important thing but how the effective communication of it is equally important so that it triggers appropriate actions at appropriate timing.

Moreover, as a penetration tester, we are used to looking at the little details so it was refreshing and eye-opening to learn about the macro view on cyber threat landscape."

—Ryoko Amano, Penetration Tester

"Cyber threats are a constant danger for companies in the private sector, which makes cyber threat intelligence an increasingly crucial tool for identifying security risks, developing proactive strategies, and responding swiftly to attacks. Martin Lee's new book is a comprehensive guide that takes the mystery out of using threat intelligence to strengthen a company's cyber

defence. With a clear and concise explanation of the basics of threat intelligence, Martin provides a full picture of what's available and how to use it. Moreover, his book is packed with useful references and resources that will be invaluable for threat intelligence teams. Whether you're just starting in cybersecurity or a seasoned professional, this book is a must-have reference guide that will enhance your detection and mitigation of cyber threats."

—Gavin Reid, CISO VP Threat Intelligence at Human Security

"Martin Lee blends cyber threats, intel collection, attribution, and respective case studies in a compelling narrative. Lee does an excellent job of explaining complex concepts in a manner that is accessible to anyone wanting to develop a career in intelligence. What sets this book apart is the author's ability to collect related fundamentals and applications described in a pragmatic manner. Understandably, the book's challenge is non-disclosure of sensitive operational information. This is an excellent reference that I would highly recommend to cyber security professionals and academics wanting to deepen their domain expertise and broaden current knowledge. Threats indeed evolve and we must too."

—Dr. Roland Padilla, FACS CP (Cyber Security), Senior Cyber Security Advisor – Defence Program (CISCO Systems), Army Officer (AUS DoD)

"Cyber Threat Intelligence by Martin Lee is an interesting and valuable contribution to the literature supporting the development of cyber security professional practice. This well researched and thoroughly referenced book provides both practitioners and those studying cyber threats with a sound basis for understanding the threat environment and the intelligence cycle required to understand and interpret existing and emerging threats. It is supported by relevant case studies of cyber security incidents enabling readers to contextualise the relationship between threat intelligence and incident response."

—Hugh Boyes, University of Warwick

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)*