

Design of Cybersecurity Model Based on Chinese and British Policies

Yifei Sun

April 2023

Contents

1	Abstract	4
2	Introduction	5
2.1	Study Purpose	7
2.2	Context	8
2.3	Rationale	10
2.4	Boundaries	10
3	Literature Review	11
3.1	UK Cybersecurity Governance Principles	11
3.1.1	Cyber Essentials	11
3.1.2	ISO/IEC 27001	11
3.1.3	Protection of National Infrastructure (CPNI)	12
3.1.4	NIST Cybersecurity Framework	13
3.1.5	CIS Controls	13
3.1.6	ITFL	14
3.2	Principles of China's cybersecurity governance	14
3.2.1	CERT-China	14
3.2.2	China's National Information Security Standard System	15
3.2.3	Cybersecurity Law of the People's Republic of China	16
3.3	Network security model	16
3.4	Model building tools	20
3.4.1	Threat modeling	20
3.4.2	Open source cyber attack and protection projects	22
4	Research Methodology	22
4.1	Introduction	22

4.2	Research Philosophy	23
4.3	Methodology	24
4.4	Research Approach	25
4.4.1	Deductive Approach	25
4.4.2	Inductive Approach	25
4.4.3	Qualitative Research	25
4.4.4	Quantitative Research	26
4.5	Ethical Statement	26
4.6	Research Methods	26
5	Time Horizon	28
6	Result	29
6.1	Methods of Data Collection	29
6.2	Experiments	29
7	Evaluation	30
8	Conclusion	31
9	Bibliography	32

1 Abstract

Cybersecurity has become an increasingly important focus in the era of the Internet, and countries around the world are taking measures to protect and enhance their online infrastructure. China and the UK are two countries with significant digital footprints, and their approaches to cybersecurity have attracted international attention. The proposal aims to analyze the cybersecurity measures and policies in China and the UK, highlight their similarities and differences, and design an effective cybersecurity model that will be applicable to the cybersecurity certification programs of both countries, and will be tested through penetration testing. The literature review section will mainly introduce the current cybersecurity frameworks and policies in the two countries, as well as the current cyber attack methods and threat modeling, and the tools and websites used in the penetration testing. The overall process of the project will be outlined on a timeline. The conclusion shows that if the penetration testing is passed, the project will provide a cybersecurity framework that can be used by both China and the UK. In order to ensure the smooth progress of the project, an ethical form will be provided in the appendix.

2 Introduction

With the rapid development of the Internet in recent years, cybersecurity has become increasingly important. Cyber attacks can result in significant financial losses for businesses and individuals, and can also pose threats to government and even military security. It has become a focus of research for many countries worldwide [1]. Figure 1 presents statistical data on cyber attacks over the past decade, compiled by the Center for Strategic International Studies (CSIS), showing a significant increase in the frequency of cyber attacks resulting in losses exceeding one million US dollars [2].

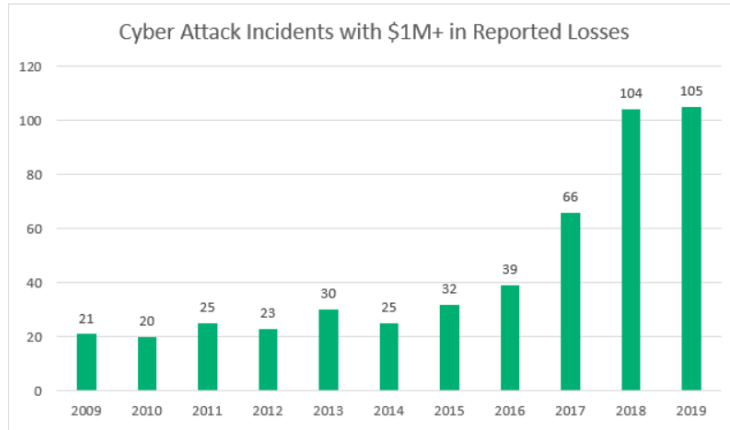


Figure 1: Over a million losses due to network attacks within a decade[2]

Between 2021 and 2022, the trend of cyber attacks was particularly fierce, with many of these attacks launched by small teams, targeting educational institutions and software for profit through ransom and other means. In 2022, the overall trend of cyber attacks increased by percentage 38, and there were also many new hackers conducting attacks in the medical field for profit. It is necessary to take measures and actions as soon as possible to prevent further cybersecurity incidents. Figure 2 shows the increase in cyber attack times in

each state in Check Point Research in 2022 compared to 2021, with the overall cyber attacks in the UK increasing by approximately 77 percentage[3]. In my opinion, due to the rise of ChatGPT and other similar tools such as Bing and various AI tools, 2023 may be the most stressful year for countries in terms of cybersecurity management. There is an urgent need to update the cybersecurity model and framework agreements to adapt to the rapid development of artificial intelligence.

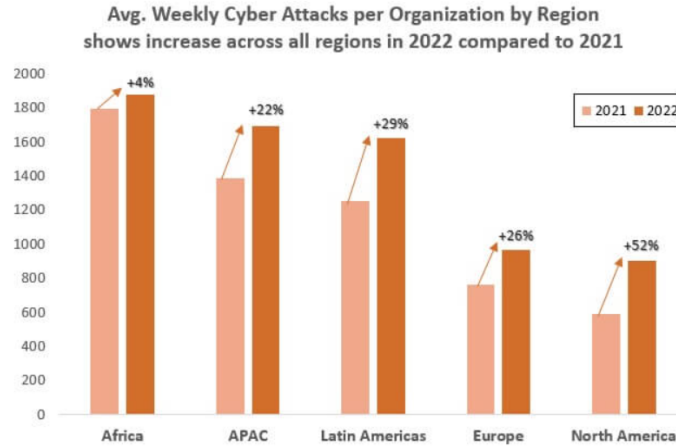


Figure 2: Trend of network attacks from 2021 to 2022[4]

In recent years, China's cybersecurity industry has rapidly expanded, with the industry's scale reaching 170 billion RMB from 2018 to 2022. In the future, China's cybersecurity industry product system will be further improved, innovation momentum will be further enhanced, and domestic demand will be further expanded. It is expected that by 2023, the overall industry scale will exceed 250 billion RMB, with a compound annual growth rate of over 15 percentage[5]. Although the growth rate of the cybersecurity industry in China is rapid, due to a significant shortage of cybersecurity professionals and relatively backward technology, a large number of cybersecurity practitioners will still be

needed in the future. Moreover, it is necessary to design firewalls that are better suited to the needs of current cyber attacks[6].

The COVID-19 pandemic has basically ended worldwide. During the pandemic, many enterprises and schools chose to work online, and working and studying from home became the primary choice for many people. This new way of working has greatly increased the demand for cybersecurity. During COVID-19, especially from 2019 to 2020, F5blog's data showed that the number of clients affected by cyber attacks increased by 220 percentage compared to the previous period[7]. After COVID-19, hacker organizations turned their attacks to the medical field, which has weaker network defenses, to profit from attacking medical organizations[1][8]. Today, with frequent cyber attacks and frequent data leaks, countries' enterprises and governments are actively introducing new cybersecurity models and treaties. In September 2022, the EU proposed a new network protection policy, which improved previous vulnerabilities and strengthened the defense against cyber attacks on the EU and its member states[9]. In recent years, there have been many updates to evaluation methods, including the proposal by Bokan et al. [10] of a threat-based network security architecture evaluation method. This method describes how to use threat-based assessment to identify network security threats and risks, and design and implement appropriate security solutions. In this paper, we will also revisit the issue of evaluation methods.

2.1 Study Purpose

The purpose of this study is to compare the development of network security in China and the UK and to design a model framework that meets the network security requirements of both countries.

2.2 Context

There are various means of network attacks, which can greatly impact businesses, politics, education, healthcare, and other industries. A network attack refers to the unauthorized access, interference, destruction, or theft of computer systems, network equipment, applications, or data through the internet or other network channels [11]. Such attacks can lead to severe consequences such as information leakage, system paralysis, business interruption, and property damage. There exist many different techniques for network attacks, and below are a few examples.

(1) Denial of Service (DoS) attack: An attack method that exhausts system resources by sending a large number of requests or malicious data packets to the target system, causing the system to be unable to respond to legitimate user requests, and rendering the service unavailable.

(2) Distributed Denial of Service (DDoS) attack: Similar to DoS attacks, but using multiple different computers or devices to simultaneously launch attacks against the target system, thereby increasing the scale and power of the attack. The first DDoS attack occurred in 1999, and in 2000, Yahoo's website was unable to be accessed for three hours due to a DDoS attack[12]. In recent years, major enterprises such as eBay and Amazon have also been subject to DDoS attacks to varying degrees, causing not only significant economic losses but also infringement upon the rights of the companies' customers[13].

(3) Malware attack: An attack involving malicious software, such as viruses, worms, Trojans, and spyware, that infects the target system or application and gains unauthorized access or steals sensitive information. During software development, multiple security tests are required to prevent harm to customer interests upon release, but some factors are still ignored in the current design

process, leading to software vulnerability to attacks[14]. In the future, the design of a more standard process requires significant data support and better testing and evaluation systems.

(4) Phishing attack: An attack method that uses forged legitimate websites, emails, or messages to induce users to provide personal or confidential information, resulting in unauthorized access or theft of information. Due to its ease of implementation, phishing attacks have a high success rate, affecting not only individuals but also many businesses. Spear phishing, a type of phishing attack, utilizes client information to steal contextual information from customers when using the internet, making network attacks easier to implement. In the UAV field, as they are connected via the internet, they are more susceptible to attacks, posing a great threat to military, commercial, and other areas[15].

(5) Internet fraud: Including false advertisements, false transactions, and false promotions, this type of online fraud deceives users into providing financial or personal information. Although many developers in the financial industry have developed preventive systems to prevent fraud in recent years, the systems still lack sufficient data and real-time updates, resulting in many people falling victim to various forms of online fraud[16].

In 2023, despite the existence of relatively sound frameworks for preventing network attacks, many problems still persist. Numerous large enterprises and governments around the world continue to suffer from network attacks each year, especially in recent years where inconsistent regulations on network security among different countries have led to many cross-border incidents. In 2018, the UK and its allies announced that a group called APT10, representing the Chinese Ministry of State Security, had launched a malicious network attack, stealing intellectual property and sensitive business data from Europe,

Asia, and the United States. The UK's National Cyber Security Centre (NCSC) concluded after assessment that this attack was most likely launched by the well-known APT10 group, which has a history of launching network attacks against major service providers[17]. In China, the situation regarding network attacks differs slightly from other countries due to the large population and political factors. The government plays a major role in regulating network security and has implemented many legal provisions and policies to protect Chinese people's network security. However, due to the country's massive population, the frequency of attacks from foreign sources is much higher than in other countries. In 2013, China, Russia, Kazakhstan, and Uzbekistan established the Shanghai Cooperation Organization (SCO) with the hope of improving cooperation in the area of network security[18].

2.3 Rationale

Based on the data presented by Check Point Research, the number of global cyber attacks in 2022 increased by 38 percentage compared to 2021[3]. This sharp increase in cyber attacks highlights the growing need for improved network security measures to address the rapid growth of cyber attack incidents. In this context, this article[19] discusses three major cyber attack models and critiques the existing network security measures, which are deemed inadequate for responding to current cyber attacks. Given the prevalence of cross-border cyber attacks, it is imperative to design network security models that comply with international treaties.

2.4 Boundaries

The network security model will not conduct the testing process under the connected state to prevent potential attacks on the internet during the testing.

3 Literature Review

3.1 UK Cybersecurity Governance Principles

3.1.1 Cyber Essentials

Cyber Essentials is a UK government certification program aimed at assisting organizations in protecting themselves against the impact of cyber attacks. The program outlines five fundamental security controls to mitigate the risk of network attacks[20]. In a study of 200 network vulnerabilities, JM Such et al.[21] concluded that patch management is the most effective control in mitigating the risk of remote attacks among the current five fundamental security controls. Anti-malware is also a significant measure in protecting against network attacks, but some organizations and individuals overly rely on it, which warrants further consideration. K Renaud et al.[22] suggested in a survey report that small businesses are particularly vulnerable to network attacks due to their limited resources in implementing protective measures, making it easy to overlook network security. Although Cyber Essentials can assist in protecting organizations and individuals, frequent network attacks still occur due to subjective factors.

3.1.2 ISO/IEC 27001

ISO/IEC 27001 is an international standard that provides a framework and best practices for organizations to establish, implement, maintain, and continually improve information security management. G. Culot et al. [23] summarized papers on ISO/IEC 27001 from 2005 onwards and concluded that the current structured approach to information and network security needs to integrate multiple standards, including differences between countries. In certifying ISO/IEC 27001, attention should also be paid to government policies and market demands of different countries. Alshar'e et al. [24] compared the NIST and ISO 27001

security frameworks and concluded that NIST is more suitable for supervising organizational security at critical moments of company operation, while ISO 27001 is more suitable for new companies to certify their network security risk maturity. Sussy et al. [25] analyzed the implementation process of ISO/IEC 27001 in public organizations in Peru, and determined the feasibility and success factors of the ISO/IEC 27001 security framework in this case study. The conclusion drawn from the results obtained is that in order to achieve successful information security management, not only technical, legal, and organizational issues should be considered, but also personnel-related factors such as training, knowledge, and awareness-raising. This has great reference value for the model design of this study.

3.1.3 Protection of National Infrastructure (CPNI)

The Centre for the Protection of National Infrastructure (CPNI) is a UK government agency that provides security advice to enterprises and organizations operating critical infrastructure. Petrakos et al. [26] analyzed the methods and strategies for protecting critical infrastructure in various countries. In the UK, CPNI serves as the responsible public institution and independently conducts its own research on the potential critical infrastructure (CI) based on cross-domain assessment criteria for social impact. The UK's assessment includes six levels of rating, ranging from CAT 0 to CAT 6, as detailed in Figure 3.

Level 0	Absence of any activity relevant to CIP	Croatia, Irland, Portugal
Level 1	Embodiment of Directive 2008/114 (EU Council, 2008) at national level. Nothing further	Greece, Bulgaria, Denmark, Malta
Level 2	Establishment of a national Strategy on Protection of CI	Belgium, Cyprus, Letonia, Lithuania, Hungary, Slovenia, Sweden
Level 3	Implementation of a National Protection Plan on CI	Austria, France, Germany, Switzerland, Estonia, Spain, G. Britain, Holland, Poland, Romania, Slovakia, Czech, Finland

Figure 3: Rating standards in the UK[27]

Weiss et al. [28] provided a survey of the UK, Germany, and the United States, analyzing the different policies and measures taken by these countries to protect critical national infrastructure. The authors suggest that governments of these countries need to adopt a more comprehensive and collaborative approach, strengthen cross-border cooperation, and develop more robust cybersecurity technologies to counter increasingly complex cyber threats.

3.1.4 NIST Cybersecurity Framework

In the article "What is the NIST Framework?"[29], the NIST Cybersecurity Framework is first introduced as a voluntary framework launched by the National Institute of Standards and Technology (NIST) in the United States, providing a consistent language, approach, and method for organizations to manage cybersecurity risk. The article then analyzes the prevalence of cyber threats in the world today, explains the applicability of NIST in enterprises, and discusses the increasing global adoption and popularity of the NIST cybersecurity framework.

3.1.5 CIS Controls

CIS Controls is a cybersecurity framework introduced by the Center for Internet Security (CIS) to provide organizations with a set of cybersecurity controls to protect them from common network attacks and threats. In the 16th International Conference on Telecommunications (ConTEL) in 2021, S. Groš et al. critically analyzed CIS Controls and explored their strengths and limitations under current network threats and trends. The paper also proposed some suggestions to modify and improve CIS Controls to enhance their effectiveness and relevance in today's rapidly changing cybersecurity environment [30]. Meanwhile, Eemani et al. [31] provided a detailed analysis, implementation, and monitoring of critical security controls through a case study of J B Group. The

paper discussed how to monitor the implementation effect of critical security controls and how to continuously improve the implementation process. The authors provided some practical tools and recommendations to help organizations effectively monitor and improve the implementation of their critical security controls.

3.1.6 ITFL

The Information Technology Infrastructure Library (ITIL) is a best practice framework for service management that provides a set of standardized IT service management processes and best practices to help organizations optimize their IT service management and improve the quality and efficiency of their IT services. Sheikhpour et al. [32] explored the best practices for integrating ITIL (Information Technology Infrastructure Library) and ISO/IEC 27001 services into information security management. They designed a five-step method to achieve service integration, which can help organizations better manage information security and ensure the reliability, availability, and security of their IT services. In this study, multiple security frameworks were also integrated to provide some ideas for the design of this article.

3.2 Principles of China's cybersecurity governance

3.2.1 CERT-China

CERT-China is a Chinese government organization responsible for responding, managing, and preventing domestic internet security incidents, issuing network security warnings and vulnerability information, as well as providing technical support and services for network security [33]. According to He Shiping et al. [34], in recent years, the Chinese government has taken a series of measures to strengthen network security, such as establishing a national internet emergency

response center and enacting the Cybersecurity Law, and has achieved certain results. However, the authors also emphasize the weak links in the security of Chinese websites, such as vulnerabilities in website code, personal information leakage, and phishing, which require enhanced prevention and response capabilities.

3.2.2 China's National Information Security Standard System

China Electronics Technology Group Corporation (CETC) led the development of four national standards in 2012, including "Basic Requirements for Information Security Level Protection", "Specification for Cryptographic Application Marks", "Guidelines for Network Security Level Protection Assessment of Information Security Technology", and "Testing Specifications for Network Security Level Protection of Information Security Technology". These standards cover various aspects of information security level protection, cryptographic application marks, network security level protection assessment and testing, providing important reference and guidance for the standardization construction of China's information security field. An et al. [35] proposed a complete framework for ICS (Industrial Control System) information security policies and standards. The framework includes five aspects: ICS information security policy, ICS information security management, ICS information security technology, ICS information security training, and ICS information security assessment. At the same time, they compared international standards such as ISO/IEC 27001 and ISO/IEC 62443, and explored the current situation and development trend of domestic ICS information security standardization. This provides some insights for the framework design of this study.

3.2.3 Cybersecurity Law of the People's Republic of China

In the conference report [37], it was pointed out that the promulgation of the Cybersecurity Law of the People's Republic of China is of great significance for strengthening network security management, protecting network security and national security in our country. However, the implementation process also faces many challenges, such as the popularization and interpretation of legal provisions, and the formulation and implementation of technical standards. The article believes that analysis of policy agenda can provide reference for relevant departments to better promote the implementation and landing of the Cybersecurity Law.

3.3 Network security model

(1) The PDR model, proposed by International Internet Security Systems (ISS), is one of the earliest network security models to embody the concept of active defense. Protection refers to using all possible measures to ensure the security of networks, systems, and information[38]. Protection typically employs techniques and methods such as encryption, authentication, access control, firewall, and antivirus. Detection allows for an understanding and evaluation of the security status of networks and systems, providing a basis for security protection and response. Detection technologies mainly include intrusion detection, vulnerability detection, and network scanning. Response occupies an important position in the security model and is the most effective way to solve security problems. Solving security problems means solving emergency response and abnormal processing problems. Therefore, establishing an emergency response mechanism and forming the ability for rapid security response is crucial for networks and systems. The PDR model defines protection time P_t , detection time D_t , and response time R_t and provides a calculation method for evaluating sys-

tem security. When $Pt > Dt + Rt$, the system is considered safe. In other words, if the attack behavior is discovered and prevented before the attacker breaches the system, the system is secure[39]. Figure 4 below shows a brief schematic of the PDR model.

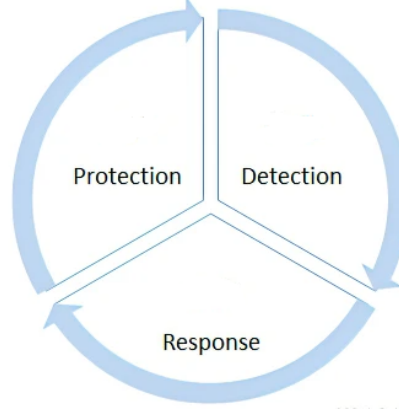


Figure 4: PDR model

(2) The P2DR model is a representative model of the dynamic network security system proposed by the US ISS company, and also the prototype of the dynamic security model. The security strategy generated based on risk analysis describes which resources in the system need protection and how to implement their protection, etc. The strategy is the core of the model, and all protection, detection, and response are implemented based on the security strategy. Network security strategy generally includes two parts: overall security strategy and specific security strategy [40]. (1) Strategy: Define the monitoring cycle of the system, establish the system recovery mechanism, formulate network access control strategy, and clarify the overall security planning and principles of the system. (2) Protection: Prevent security incidents by repairing system vulnerabilities, correctly designing and developing and installing systems; Find potential system vulnerabilities through regular inspections; Use education and

other methods to ensure that users and operators use the system correctly and prevent accidental threats; Prevent malicious threats through access control, monitoring, etc. The protection technologies adopted usually include data encryption, identity authentication, access control, authorization and virtual private network (VPN) technology, firewall, security scanning, and data backup, etc. (3) Detection: It is the basis for dynamic response and strengthening protection. By continuously detecting and monitoring the network system, new threats and weaknesses can be discovered, and effective responses can be made in a timely manner through feedback loops. When the attacker penetrates the protection system, the detection function comes into play and complements the protection system. (4) Response: Once the system detects an intrusion, the response system starts to work and event handling is initiated. The response includes emergency response and recovery processing, and the recovery processing includes system recovery and information recovery [41]. The following figure is a schematic diagram of the P2DR model:

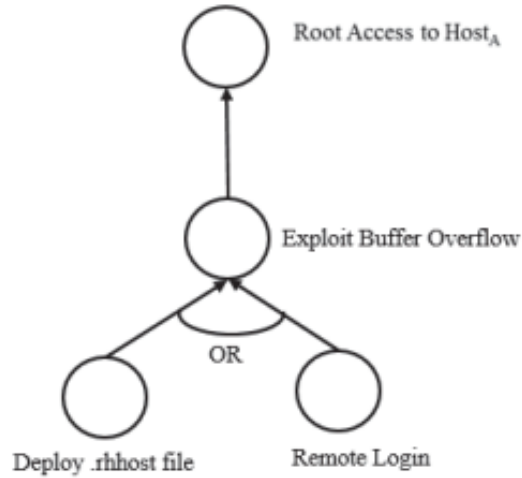


Figure 5: P2DR model

(3)The Adaptive Security Architecture (ASA) is a next-generation security framework proposed by Gartner in 2014 to address the security challenges faced in the era of cloud, big data, mobile, and IoT. The ASA emphasizes that security protection is a continuous, cyclic process that involves real-time dynamic analysis of security threats from a fine-grained, multi-angle, and continuous perspective. It adapts to the constantly changing network and threat environment and continuously optimizes its security defense mechanisms across four dimensions: prediction, prevention, detection, and response [42].

Prevention refers to a series of strategy sets, products, and services that can be used to defend against attacks. The key goal is to reduce the attack surface and intercept attack actions before being affected.

Detection is used to identify attacks that have bypassed the defense network. The key goal is to reduce the "downtime" and potential losses caused by threats. Detection capability is crucial because companies should assume that they are already in a state of being attacked.

Response is used to efficiently investigate and remedy transactions detected by analysis functions (or external services) to provide intrusion authentication and attack source analysis, generate new preventive measures to avoid future incidents.

Prediction optimizes the baseline system through the results of prevention, detection, and response, gradually predicting unknown and new attacks accurately. It actively locks down new attacks that threaten existing systems and information, prioritizes and locates vulnerabilities. This intelligence is fed back into the preventive and detection functions, forming a closed loop for the entire processing flow.

3.4 Model building tools

3.4.1 Threat modeling

Threat modeling is a structured process of identifying and assessing the security risks and threats of a product, and developing mitigation measures for these risks and threats. As the saying goes, "unknown threats, no defense." We should examine network security problems from the perspective of attackers, identify threats, and mitigate risks. Threat modeling is a structured theoretical framework that was developed by pioneers in the field of network security based on engineering practice. It constructs threat models from the perspectives of examiners and practitioners, and under the guidance of theoretical frameworks, helps to avoid confusion and helplessness in identifying constantly changing security threats [43].

(1) STRIDE threat modeling: STRIDE is the pioneer of threat modeling, created by Microsoft security researchers in 1999. From the perspective of attackers, threats are divided into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege [44]. By analyzing and evaluating each type of threat, potential security issues can be better identified and addressed. The STRIDE method is suitable for security assessment and threat modeling in various software development lifecycles, and can help developers better ensure the security of software.

(2) PASTA threat modeling: PASTA (Process for Attack Simulation and Threat Analysis) is a use case-based threat modeling method. PASTA threat modeling mainly includes six steps: planning threat modeling, defining scope, applying model, threat assessment, solution development, and evaluation improvement.

(3) VAST threat modeling: VAST (Visual, Agile, and Simple Threat modeling)

is a graphical and agile-based threat modeling method. Its goal is to quickly build visual threat models to support rapid response to threats. VAST threat modeling mainly includes five steps: defining scope, applying model, identifying threats, evaluating threats, and solving threats.

(4) Attack tree model: The attack tree was created by Bruce Schneier, a legend in information security, in the late 1990s. It provides a formal and clear method to describe the security threats that a system faces and the multiple attacks that a system may be subjected to. We use a tree structure to represent the attacks that the system faces, where the root node represents the target being attacked, and the leaf nodes represent the methods of achieving the attack goal. By exhaustive and in-depth analysis, the most clear attack methods and attack paths can be continuously identified[45].

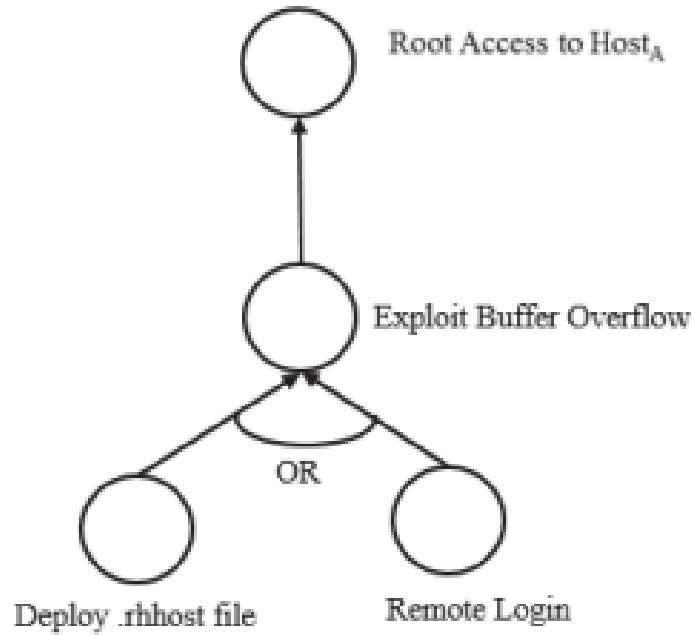


Figure 6: Attack tree model

3.4.2 Open source cyber attack and protection projects

Searching for information on GitHub, the following tools were found, including information gathering tools, vulnerability exploitation tools, internal network penetration tools, emergency response tools, and client-side operation and maintenance tools. These will be introduced in the following sections: First, the project by Ske, called ShuiZe 0x727, which only requires the input of the root domain name to collect relevant assets comprehensively and detect vulnerabilities. It can also input multiple domains, C-class IP addresses, etc [46]. This project uses the Python language. In this study, this project will be considered for testing.

It should be noted that some of the projects themselves contain viruses during actual testing, so precautions should be taken to prevent computer infection and avoid connecting to the internet. Furthermore, these projects are not intended for commercial use.

4 Research Methodology

4.1 Introduction

This chapter will elucidate the methods utilized by the researchers in conducting the study, and will closely examine the different techniques and approaches employed in this research. As defined by [47], research methodology outlines how to research, experimental methods, theoretical basis, model design and testing, data collection, and indicates the correct direction to achieve results. Research strategy and methods will be used for data collection and analysis. The sample selection will then depend on the selection made during the experiment, as depicted in Figure 7 of the Research Methodology [48].

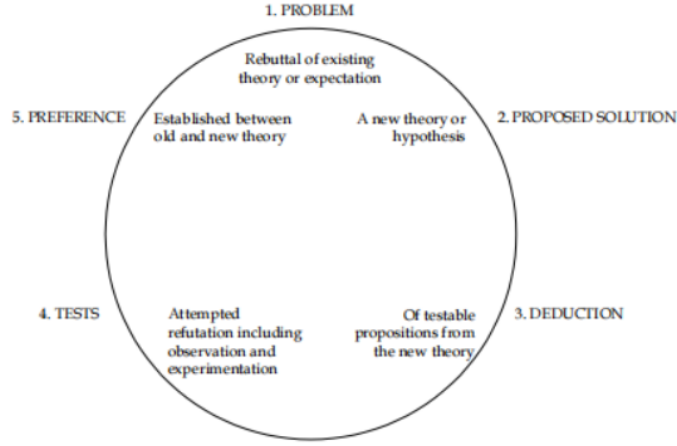


Figure 7: The Cycle of Scientific Research[48]

4.2 Research Philosophy

Research philosophy is the foundation for research design and methods, and it directly relates to the selection of research questions, the formulation of research methods, and the interpretation and explanation of research results. Common research philosophies include positivism, interpretivism, critical theory, and constructivism, among others [49].

Positivism's basic principle is that all knowledge of reality is based on positive information obtained from observable experience. Positivism involves the development of general laws from objective truth that can be used to predict behavior. Sanders et al. [50] found that in positivism, researchers adopt a philosophical attitude when dealing with observable social reality, where they develop a theory from observation.

Interpretivism believes that human behavior is meaningful and emphasizes the interaction, understanding, and interpretation of researchers and study subjects. By gaining a deep understanding and exploration of the internal phenomena and

processes of the research object, interpretivists believe that human behavior is complex and diverse, and therefore qualitative data must be used to understand phenomena.

Critical theory believes that research methods should be based on practical problems and the needs of researchers, emphasizing practicality and practical value. Based on practice-oriented methods, researchers tend to use a variety of research methods and techniques to solve practical problems and apply the results to practice.

Constructivism believes that humans jointly construct social reality through social interaction and communication. Constructivists focus on the meaning and significance of social reality and believe that understanding social phenomena requires a deep understanding of their historical and cultural background. They use qualitative data such as text and cultural symbols to study social phenomena.

4.3 Methodology

To understand the cybersecurity frameworks of China and the UK, as well as their response measures to cyber attacks, this research is conducted by searching relevant journals, books, and websites using highly reliable sources such as Science Direct, IEEE, and Springer, among others. The priority of literature search is mainly based on relevant keywords and content, followed by publication date, as recent journals are deemed more representative. Based on the literature, the current research status and conclusions on how to improve are obtained. The research areas include the network frameworks, cyber attacks, and threat models of China and the UK.

4.4 Research Approach

4.4.1 Deductive Approach

The deductive approach refers to the reasoning process from general to specific, also known as deduction. In deductive reasoning, we start with general principles or premises and use logical inference to reach a specific conclusion. This type of reasoning is a "top-down" method, which means the deduction process goes from general principles to specific cases. The deductive approach is widely applied in scientific research, mathematics, philosophy, and other fields.

4.4.2 Inductive Approach

Inductive reasoning is a method of inferring general principles or rules through observation and empirical evidence. In science and research, inductive reasoning is often used to study and understand complex systems or phenomena, by observing and analyzing commonalities and patterns among multiple specific instances to arrive at general conclusions. Unlike deductive reasoning, which derives specific conclusions from general rules, inductive reasoning derives general rules from specific conclusions.

4.4.3 Qualitative Research

Qualitative research is a research method that primarily relies on textual and visual data sources, with the aim of exploring human experiences, meanings, and perspectives. Compared to quantitative research, qualitative research pays more attention to the depth and diversity of phenomena, emphasizing understanding and interpretation rather than simple numerical measurement. Qualitative research typically employs open-ended research designs and data collection methods, such as in-depth interviews, focus group discussions, observation, and document analysis, to uncover and explore the essence and connotations of

research questions.

4.4.4 Quantitative Research

Quantitative research is a research method based on data analysis, which reveals quantitative relationships between phenomena by collecting, analyzing, and interpreting a large amount of numerical data. It emphasizes the objectivity and reproducibility of the research object, and usually uses statistical methods to analyze data, draw conclusions, and validate hypotheses. Quantitative research typically employs methods such as surveys, experiments, and observations to collect data, and is applicable to research in fields such as social phenomena, human behavior, and natural sciences.

4.5 Ethical Statement

For this project, preliminary model design is currently underway, and some data and websites have been collected for testing the model. If successful, the results will be submitted to the school. An ethics form will be completed and submitted for approval, with limited ethical implications expected. The ethical form for this project can be found in the attachment section of Turnitin.

4.6 Research Methods

Firstly, by examining the network framework of China and the UK, the network framework and threat model will be designed. Network attack testing will be conducted while ensuring computer security, and the feasibility of the model will be verified through network attack projects in open-source projects on GitHub. When designing the model, the network security protocols of both China and the UK will be considered comprehensively. During testing, websites from both countries will be selected for testing. It should be noted that this test will not

have any actual impact on the websites and will only be used to extract data, which will be treated confidentially.

5 Time Horizon

Time Horizon typically refers to the time span considered in planning and decision-making. It refers to the timeframe of a project, plan, or strategy, including the start and end dates. It can help individuals better plan and manage time resources, predict future outcomes and trends, and make more targeted and effective decisions. In project management, Time Horizon is a critical concept as it can help teams understand the project's time frame, develop more realistic time schedules, and make necessary adjustments throughout different project stages [51]. The following figure illustrates the time range for this project.

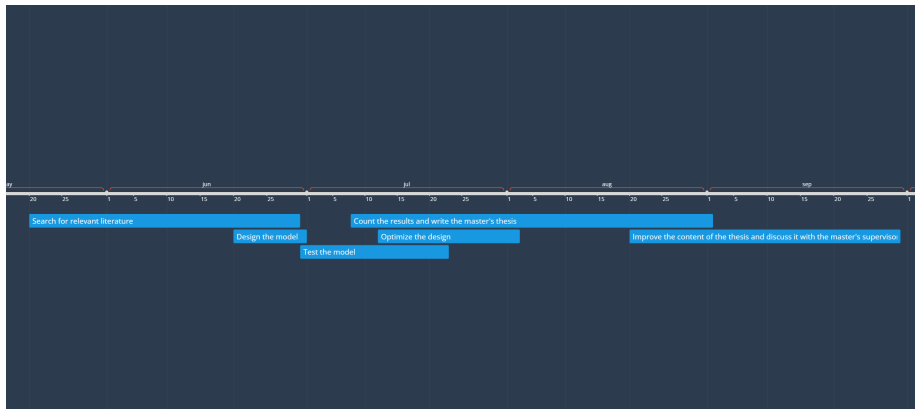


Figure 8: Time Horizon

6 Result

6.1 Methods of Data Collection

In order to ensure the authenticity and validity of the data, the main data searched in this study are collected by the researchers themselves, rather than from third-party websites or data from existing papers. The remaining auxiliary data comes from websites and literature verified by the researchers to ensure data applicability.

6.2 Experiments

The experiment will proceed as follows:

- (1) Design a framework for network security modeling.
- (2) Create a threat model and identify the website data that will be targeted for attack.
- (3) Check the computer to ensure that it is not at risk.

During the experiment, the following software and tools will be used, as well as other tools that may be needed: Microsoft Threat Modeling Tool, Threat Dragon: OWASP, Python, GitHub open-source projects.

In addition, some data will be obtained from websites, which is currently under investigation.

7 Evaluation

Currently, network security incidents are occurring frequently, and measures must be taken as soon as possible to prevent more cross-border cyber attacks. Enterprises, governments, and individuals should update their network security frameworks to counter new cyber attack methods.

If successful, this experimental project will first be executed by multinational enterprises, especially those in China and the United Kingdom, to prevent the experimental model from being leaked, which could lead to a cyber attack. It should be noted that there are some limitations to this experiment: firstly, due to the multiple types of security models available, there may not be enough time to research them all thoroughly. Secondly, the current testing methods for cyber attacks are limited to using open-source projects on GitHub. If data is obtained from some government or enterprise websites, legal issues may arise.

8 Conclusion

Currently, there are frequent incidents of network attacks in China and the UK, due to policy reasons and the inadequacy of existing models. This project aims to design a new security framework that meets the policies and requirements of both countries and is capable of addressing new types of attacks. The framework will be tested through network attack simulations.

9 Bibliography

- [1] Odebade, Adejoke T., and Elhadj Benkhelifa. "Evaluating the impact of government Cyber Security initiatives in the UK." arXiv preprint arXiv:2303.13943 (2023).
- [2] <https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/>
- [3] <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>
- [4] <https://www.eeas.europa.eu/eeas/factsheet-eu-policy-cyber-defence> en
- [5] Ministry of Industry and Information Technology. Three-year Action Plan for the High-quality Development of the Cybersecurity Industry (2021-2023) (Draft for Comments) [EB/OL]. (2021-07-12) 2021-09-23
- [6] LI Yaqi. Review of Computer Network Security System and Its Development Trend[J]. Interactive Software, 2020(3): 1293-1294.
- [7] Warburton, D., 2020. Phishing attacks soar 220cybercriminal opportunism intensifies. Last accessed: January 27, 2022
- [8] Muthuppalaniappan, Menaka, and Kerrie Stevenson. "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health." International Journal for Quality in Health Care 33.1 (2021): mzaa117.
- [9] Lallie, Harjinder Singh, et al. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers security 105 (2021): 102248.
- [10] Bokan, Branko, and Joost Santos. "Managing cybersecurity risk using

- threat based methodology for evaluation of cybersecurity architectures.” 2021 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2021.
- [11] Kim, Youngsoo, Ikkyun Kim, and Namje Park. "Analysis of cyber attacks and security intelligence." *Mobile, Ubiquitous, and Intelligent Computing: MU-SIC 2013*. Springer Berlin Heidelberg, 2014.
- [12] M. A. Saleh and A. Abdul Manaf, "Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks," 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, Malaysia, 2014, pp. 263-267, doi: 10.1109/ISBAST.2014.7013132.
- [13] Thapngam, T., Y. Shui, and Z. Wanlei. DDoS discrimination by Linear Discriminant Analysis (LDA). in *Computing, Networking and Communications (ICNC)*, 2012 International Conference on. 2012.
- [14] E. Iannone and F. Palomba, "The Phantom Menace: Unmasking Security Issues in Evolving Software," 2022 IEEE International Conference on Software Maintenance and Evolution (ICSME), Limassol, Cyprus, 2022, pp. 612-616, doi: 10.1109/ICSME55016.2022.00085.
- [15] M. S. Baig, F. Ahmed and A. M. Memon, "Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted," 2021 4th International Conference on Computing Information Sciences (ICCIS), Karachi, Pakistan, 2021, pp. 1-6,
- [16] W. Fang, X. Li, P. Zhou, J. Yan, D. Jiang and T. Zhou, "Deep Learning Anti-Fraud Model for Internet Loan: Where We Are Going," in *IEEE Access*, vol. 9, pp. 9777-9784, 2021, doi: 10.1109/ACCESS.2021.3051079.
- [17] <https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of->

chinese-cyber-campaign.zh

- [18] Kshetri, Nir. "Cybercrime and cyber-security issues associated with China: some economic and institutional considerations." *Electronic Commerce Research* 13 (2013): 41-69.
- [19] Al-Mohannadi, Hamad, et al. "Cyber-attack modeling analysis techniques: An overview." 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). IEEE, 2016.
- [20] Essentials, Cyber. "Cyber essentials scheme: Assurance framework." UK Government (2015).
- [21] Cyber Essentials Such, Jose M., et al. "Cyber security controls effectiveness: a qualitative assessment of cyber essentials." (2015).
- [22] Renaud, Karen, and Jacques Ophoff. "What is Preventing UK SMEs from taking Cyber Security Precautions?." (2021).
- [23] Culot, Giovanna, et al. "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda." *The TQM Journal* 33.7 (2021): 76-105.
- [24] Alshar'e, Marwan. "CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001." *Applied computing Journal* (2023): 245-255.
- [25] Sussy, Bayona, et al. "ISO/IEC 27001 implementation in public organizations: A case study." 2015 10th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2015.
- [26] Petrakos, Nikolaos, and Panayiotis Kotzanikolaou. "Methodologies and

Strategies for Critical Infrastructure Protection.” Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies (2019): 17-33.

[27] Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (2010) London: UK Cabinet Office. Retrieved from <https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards>

[28] Weiss, Moritz, and Felix Biermann. ”Cyberspace and the protection of critical national infrastructure.” Journal of Economic Policy Reform (2021): 1-18.

[29] Cockcroft, Steven. ”What is the NIST Framework?.” ITNOW 62.4 (2020): 48-49.

[30] S. Groš, ”A Critical View on CIS Controls,” 2021 16th International Conference on Telecommunications (ConTEL), Zagreb, Croatia, 2021, pp. 122-128.

[31] Eemani, Hareesh Reddy. ”Analyzing, Implementing and Monitoring Critical Security Controls: A Case Implemented in J B Group.” (2017).

[32] Sheikhpour, Razieh, and Nasser Modiri. ”A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management.” Indian journal of science and technology 5.2 (2012): 2170-2176.

[33] China National Internet Emergency Response Center: New Characteristics of Cybersecurity Threats [J]. Electronic Product Reliability and Environmental Test, 2011, (4):16.

[34] He Shipping, National Internet Emergency Response Center: Overview of

the development status and security of Internet websites in China[J]. China Education Network,2017(8):24-25.

[35] China Electric Power Research Institute takes the lead in formulating national standards in the field of information security[J]. China Information Security, 2012(1): 19-19.

[36] AN Feng, ZHU Changming, LEI Xiaofeng, et al. Research on Information Security Policy and Standard Architecture of Industrial Control System in China[J]. Information Security Research,2018,4(10):959-964.

[37] GUO Junmin. Policy Agenda Analysis of Cybersecurity Law of the People's Republic of China: Based on Multi-source Flow Analysis Framework [J]. Management Observation,2019(24):93-96.

[38] PDR Liu, Yingze, and Yuanbo Guo. "Towards Real-Time Warning and Defense Strategy AI Planning for Cyber Security Systems Aided by Security Ontology." Electronics 11.24 (2022): 4128.

[39] PDR Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity in big data era: From securing big data to data-driven security." IEEE Transactions on Services Computing 14.6 (2019): 2055-2072.

[40] Liu, Shaogang. "Research on Core Technology Based on Computer Information System Security Architecture." 2018 3rd International Conference on Mechanical, Control and Computer Engineering (ICMCCE). IEEE, 2018.

[41] Xu, Shi Ping, et al. "Design and application of a network security model." Applied Mechanics and Materials. Vol. 347. Trans Tech Publications Ltd, 2013.

[42] Shen Ping Ping, "An improved model of distributed network information se-

- curity,” 2010 International Conference on Educational and Information Technology, Chongqing, 2010, pp. V3-391-V3-393, doi: 10.1109/ICEIT.2010.5608347.
- [43] Xiong, Wenjun, and Robert Lagerström. ”Threat modeling—A systematic literature review.” *Computers security* 84 (2019): 53-69.
- [44] Straub, Jeremy. ”Modeling attack, defense and threat trees and the cyber kill chain, attack and stride frameworks as blackboard architecture networks.” 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020.
- [45] Haque, S., M. Keffeler, and T. Atkison. ”An evolutionary approach of attack graphs and attack trees: A survey of attack modeling.” *Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, 2017.
- [46] <https://github.com/0x727/ShuiZe> 0x727
- [47] Kothari, Chakravanti Rajagopalachari. *Research methodology*. 2004.
- [48] Baker, Michael J. ”Selecting a research methodology.” *The marketing review* 1.3 (2000): 373-397.
- [49] Crossan, Frank. ”Research philosophy: towards an understanding.” *Nurse Researcher (through 2013)* 11.1 (2003): 46.
- [50] Saunders, Mark, P.H.I.L.I.P. Lewis, and Thornhill. ”Research methods.” *Business Students 4th edition Pearson Education Limited, England* 6.3 (2007): 1-268.
- [51] Ebert, Ronald J., and DeWayne Piehl. ”Time horizon: A concept for

management.” *California Management Review* 15.4 (1973): 35-41.