

Міністерство освіти і науки України  
Харківський національний університет радіоелектроніки

Факультет \_\_\_\_\_ Інфокомунікацій \_\_\_\_\_  
(повна назва)  
Кафедра \_\_\_\_\_ Інфокомунікаційної інженерії імені В.В. Поповського \_\_\_\_\_  
(повна назва)

**КВАЛІФІКАЦІЙНА РОБОТА**  
**Пояснювальна записка**

Рівень вищої освіти \_\_\_\_\_ другий (магістерський) \_\_\_\_\_

Дослідження методів оцінки кібернадійності інфокомунікаційних систем  
Study of methods for estimating cyber reliability of infocommunication systems  
(тема)

Виконав:  
студент 2 курсу, групи \_\_\_\_\_ АМС3Ім-20-1 \_\_\_\_\_  
\_\_\_\_\_ Майкл Ннамді Нвезе \_\_\_\_\_  
(прізвище, ініціали)

Спеціальність: \_\_\_\_\_ 125 Кібербезпека \_\_\_\_\_  
(код і повна назва спеціальності)  
Тип програми: \_\_\_\_\_ освітньо-наукова \_\_\_\_\_  
(освітньо-професійна або освітньо-наукова)  
Освітня програма: \_\_\_\_\_ Адміністративний менеджмент \_\_\_\_\_  
\_\_\_\_\_ у сфері захисту інформації \_\_\_\_\_  
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського \_\_\_\_\_  
\_\_\_\_\_ Коваленко Т. М. \_\_\_\_\_  
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри

\_\_\_\_\_  
(підпис)

\_\_\_\_\_ Лемешко О. В. \_\_\_\_\_  
(прізвище, ініціали)

2022 р.

*Кваліфікаційна робота не містить відомостей, що заборонені до відкритого друку*

Студент 2 курсу

групи АМСЗІм-20-1.

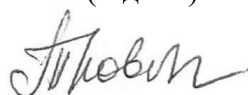


(підпис)

Майкл Ннамді Нвезе

(ініціали, прізвище)

Керівник



(підпис)

Т. М. Коваленко

(ініціали, прізвище)

## Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій  
(повна назва)  
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського  
(повна назва)  
Рівень вищої освіти другий (магістерський)  
Спеціальність 125 Кібербезпека  
(код і повна назва)  
Тип програми освітньо-наукова  
(освітньо-професійна або освітньо-наукова)  
Освітня програма Адміністративний менеджмент у сфері захисту інформації  
(повна назва)

ЗАТВЕРДЖУЮ

Зав. кафедри \_\_\_\_\_  
(підпис)

« \_\_\_\_ » \_\_\_\_\_ 2022р.

## ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Майкл Ннамді Нвезе  
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів оцінки кібернадійності інфокомунікаційних систем

затверджена наказом по університету від «24» березня 2022 р. №409 Ст.

2. Термін подання студентом роботи до екзаменаційної комісії 16.05.2021р.

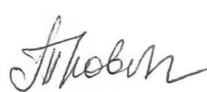
3. Вихідні дані до роботи: методи оцінки кібернадійності та кількісного розрахунку кібернадійності інфокомунікаційних систем та мереж і їх елементів, структура мережі для проведення оцінки кібернадійності телекомунікаційної мережі шляхом розрахунку надійності її вузлів

4. Перелік питань, що потрібно опрацювати в роботі:

- 1) Кібербезпека та кібернадійність інфокомунікаційних систем
- 2) Вразливості в інфокомунікаційних системах та мережах
- 3) Оцінка кібернадійності інфокомунікаційних систем та мереж
- 4) Кількісні розрахунки кібернадійності

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

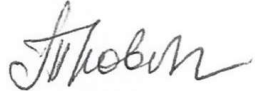
Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Коваленко Тетяна Миколаївна		29.06.2022

### КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	24.03.2022	Виконано
2	Збір матеріалів для дослідження	14.03.2022	Виконано
3	Розробка 1 розділу	21.03.2022	Виконано
4	Розробка 2 розділу	04.04.2022	Виконано
5	Розробка 3 розділу	18.04.2022	Виконано
6	Розробка 4 розділу	02.05.2022	Виконано
7	Оформлення кваліфікаційної роботи	16.05.2022	Виконано

Дата видачі завдання 24 березня 2022 року

Студент  Майкл Ннамді Нвезе  
(підпис) (прізвище, ініціали)

Керівник роботи  доцент Коваленко Т. М.  
(підпис) (посада, прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка – 92 с., кількість таблиць – 6, кількість рисунків – 15, кількість посилань – 14.

### ІНФОКОМУНІКАЦІЙНА СИСТЕМА, КІБЕРНАДІЙНІСТЬ, ТЕСТ НА ВРАЗЛИВІСТЬ, ОЦІНКА КІБЕРНАДІЙНОСТІ, КРИТИЧНІ ВУЗЛИ, КРИТИЧНІ ДУГИ

Об'єкт дослідження – процес оцінки кібернадійності інфокомунікаційних систем та мереж.

Предмет дослідження – методи й засоби оцінки кібернадійності інфокомунікаційних систем та мереж.

Мета роботи – аналіз методів оцінки вразливостей інфокомунікаційних систем та мереж та кількісного розрахунку кібернадійності сучасних інфокомунікаційних систем та мереж ті їх елементів.

Методи досліджень – емпіричний аналіз, формалізація, методи теорії графів, теорії ігор, стохастичного аналізу.

У цей час завдання кількісної оцінки кібернадійності інфокомунікаційних систем та мереж є надзвичайно важливим етапом забезпечення та підвищення рівня інформаційної безпеки.

У цій роботі наведено класифікацію атак на інфокомунікаційні системи та мережі, розглянуто основні стандарти щодо забезпечення інформаційної безпеки із зазначенням їх особливостей. Розглянуто підходи до оцінки вразливостей та кількісного розрахунку кіберстійкості інфокомунікаційних систем та мереж і їх елементів. Проведено розрахунок для телекомунікаційної мережі із заданою структурою.

## ABSTRACT

The explanatory note – 92 p, number of tables – 6, number of figures – 15, number of references – 14.

INFOCOMMUNICATION SYSTEM, CYBER RELIABILITY, ASSESSMENTS, VULNERABILITY TEST, CYBER RESILIENCE ASSESSMENT, CRITICAL NODES, CRITICAL ARCS

The research object is the process of assessing the cyber reliability of infocommunication systems and networks.

The subject of research is methods and means of assessing the cyber reliability of infocommunication systems and networks.

The purpose of the work is the analysis of methods for assessing the vulnerabilities of infocommunication systems and networks and quantitative measurement of cyber resilience of modern information communication systems and networks and their elements.

Research methods – empirical analysis, formalization, methods of graph theory, game theory, stochastic analysis.

Currently, the task of quantitative assessment of cyber reliability of infocommunication systems and networks is an extremely important step in ensuring and improving the level of information security.

This work provides a classification of attacks on infocommunication systems and networks, considers the main standards for ensuring information security and indicates their features. Approaches to vulnerability assessment and quantitative measurement of cyber resilience of the infocommunication systems and networks and their elements are considered. The calculation was carried out for a telecommunication network with a given structure.

## TABLE OF CONTENTS

LIST OF ABBREVIATIONS .....	8
INTRODUCTION .....	9
1 CYBERSECURITY AND RELIABILITY OF INFOCOMMUNICATION SYSTEMS AND NETWORKS .....	10
1.1 Cyber Security .....	10
1.2 Cyber Security assessment in infocommunication systems and networks .....	11
1.3 Importance of regular assessments .....	19
1.4 Governance and risk management .....	21
1.5 Real-life example of cyber-attack operations .....	23
2 VULNERABILITIES IN INFOCOMMUNICATION SYSTEMS AND NETWORKS .....	25
2.1 Graph theory and its importance .....	27
2.2 Problem definition .....	31
2.3 Node importance metrics .....	32
2.4 Critical node identification .....	34
2.5 Critical node detection problem .....	37
2.6 General cyber security metrics .....	40
3 CYBER RESILIENCE ASSESSMENT IN INFOCOMMUNICATION SYSTEMS AND NETWORKS .....	52
3.1 Cyber resilience assessment breakdown .....	52
3.2 System resilience under disruptions .....	54
3.3 Methods for assessing resilience.....	55
3.3.1 Game theory applications .....	55
3.3.2 Stochastic approach .....	58
3.3.3 Decision making algorithm.....	62
3.4 Experimental analysis.....	64

3.5	Conclusive statements .....	66
3.6	Risk mitigation and control for organizations.....	67
4	QUANTITATIVE MEASURES OF CYBER RESILIENCE.....	74
4.1	Factors of network resilience.....	74
4.2	Resilience evaluation model based on DBN.....	79
4.3	Numerical discussion and extension of personal experiment.....	82
4.4	Numerical analysis .....	84
	CONCLUSIONS .....	90
	LIST OF REFERENCES .....	91



## LIST OF ABBREVIATIONS

APL	– Average path length
CI	– Computer infrastructure
CRI	– Component resilience index
CVSS	– Common vulnerability scoring system
DBN	– Dynamic Bayesian network
DSS	– Data security standard
IDS	– Intrusion detection system
IOC	– Indicators of compromise
IAAS	– Infrastructure as a service
MTTD	– Mean time to defend
MTTR	– Mean time to respond
NST	– Network security toolkit
PAAS	– Platform as a service
SAAS	– Software as a service
SAR	– Secure architecture review
SDN	– Software defined network
VAPT	– Vulnerability assessment and penetration testing
WSN	– Wireless sensor network

## INTRODUCTION

The purpose of this research is to ensure the discovery of an advanced and efficient model or method for assessing the cyber reliance of info-communication systems. With a suitable model/method, a network infrastructure can identify its cyber weaknesses and strengths and develop an appropriate roadmap to prioritize, resolve and bolster them. A strategized assessment helps the network infrastructure in being proactive.

It is important for infrastructures to foster the security with proper security measures and a better understanding of risk and threats by evaluating the following components:

- Current assets (includes application, network, systems, data, etc.)
- Vulnerabilities present in the assets
- Identify the attack surface.
- Potential threats and risks on assets
- Assets' cyber resiliency
- Assets prevention cost with proportion to assets cost

The assessment can be done internally with a dedicated cyber security team or third-party cyber security services provider.

This study includes proof of research and experimentation carried out on several already existing models for assessment of cyber resilience, analysing their process of operation as well as their advantages and disadvantages and methods for improving the security of networked systems.

According to the aim of the research, an experiment as carried out that takes into account the behaviour of a telecommunication network, the importance and criticality of each node present in the infrastructure and how these values dictate the general resilience of the system. This study also proposes the game theory as the most efficient model.

# 1 CYBERSECURITY AND RELIABILITY OF INFOCOMMUNICATION SYSTEMS AND NETWORKS

## 1.1 Cyber Security

An efficient and well performing cyber security system is one of resilience with the inept ability to prevent, mitigate and adjust to attacks and threats. There are various methods and models currently in the market used for the analysis and evaluation of resiliency in networks. The main importance of this practice is to ensure total safe-keeping and protection of assets and or recovery, if lost. General evaluation of cyber systems helps bolster security and reduce the risk

An effective cybersecurity method will have many layers of defence spread across the networks, computers, programs, or information it aims to remain non-toxic. Technology is essential in providing individuals and organizations with the system security tools they want to protect against cyberattacks. Three main objects should be at risk: the policies of endpoints such as personal computers, portable devices, and routers; systems; and the cloud. Shared technologies used to protect these objects include next-generation firewalls, DNS pass-through filtering, malware prevention, antivirus tools, and email security scores. The cyber may differ in that it is connected to the workstation collection or to the network in some way. At the same time, security means the mechanism to protect everything. Therefore, the terms cyber and security define how the user's defensive information is organized on or after malicious attacks that could indicate vulnerability. This is the time that was covered for a while after the internet evolved as it always has. Cybersecurity allows any business or user to protect their critical data from hackers. Although he had concerns about hacking at one point, he actually used ethical hacking to invent cybersecurity in every structure.

This could be defined as the procedure to assuage security issues to protect reputational damage, business loss, or financial loss to all groups. The term cybersecurity obviously required it to be a security measure that we offer to the organization that frequent users can contact through the internet or through a network. There are many tackles and

techniques that are thrown to deploy it. The most important fact about information protection is that it is not a one-time event, but an ongoing process. The owner of the organization must upgrade the materials to keep the risk low.

## 1.2 Cyber Security assessment in infocommunication systems and networks

Different types of assessments help reduce the cost of breaches and improve defence capabilities. In the age of highly sophisticated cyberattacks, organizations of all sizes need to take precautionary measures to mitigate risks and improve overall resilience. Below are some types of cybersecurity assessments with different approaches that serve different goals under one goal, namely to prevent cyber-attacks [11].

1. Vulnerability Assessment: Vulnerability Assessment is the most commonly performed security test in the cybersecurity industry. VA is an automated test and is performed in a limited scope to detect the security bug or flaws in assets (assets can be applications, network, infrastructure, code, data, etc. depending on the purpose of the assessment). In it, the defects are classified according to the risk to the company. It is often done to track open paths and vulnerabilities in software, network, etc. and to release patches or updates.

2. Penetration tests: Penetration testing involves exploiting classified security holes found in the vulnerability assessment. This is an in-depth method of exploiting vulnerabilities to test an organization's security posture from the attacker's perspective. Classified vulnerabilities and bugs are mostly chained or often used alone to validate how the organization can be hacked or breached or how an attacker can launch an attack if they find the vulnerabilities open.

Pen testing can be performed from three approaches:

1. Black-box Pentesting: It involves breaking into the assets testing from a malicious hacker perspective who has no internal knowledge, access, or data.

2. White-box Pentesting: It involves testing the assets with most of the internal information and access

3. Grey-box Pentesting: It involves testing of assets with partial internal information and accesses.

The cybersecurity industry offers a variety of penetration testing based on the assets categories. The pentest types include:

- Web-application Penetration Testing
- Mobile Application Penetration Testing
- Network Penetration Testing (It can be performed separately on the external network and internal network)
- Cloud security penetration testing
- Embedded devices penetration testing
- IoT/IIoT Penetration Testing
- Thick client Penetration Testing
- Thin client Penetration Testing
- Virtual Appliances Penetration Testing

1. Compromise Assessment: Compromise Assessment is a high-level security test performed to identify traces of a breach. This is done by evaluating the infrastructure and logs, traffic and activities of the connected endpoints to discover Indicators of Compromise (IoC). In particular, the impairment assessment helps identify the attacker who has been active in recent history or lived in the current environment. It is also performed prior to the merger for compliance and regulatory compliance and often annually as a proactive approach to security.

2. Social Engineering Assessment: Unlike any technical or technological security testing, social engineering assessment involves manipulating the human mind through misleading or deceptive information. In social engineering, the security professionals impersonate themselves in order to push individuals or employees to perform specific tasks such as download any attachment. This assessment aims to check security awareness and identify missing security components, security education, and culture within the company. Social engineering assessment offers a broad spectrum to test organization security culture, employees, or individual training and awareness.

3. Red Teaming or Red-Team Assessment: Red Teaming is a step forward in identifying and exploiting vulnerabilities and beyond penetration testing. It is a large-scale attack that involves simulating cyberattacks, including lateral movements, to gain a foothold in the internal and external environment and elevate privileges without being detected. In the red team, an attack campaign is strategically designed to test the defensive capabilities of the organization. To analyse the organization's overall offensive and defensive security posture, Red Teaming examines the security culture perspective by testing employees through physical and virtual social engineering attacks, network resiliency testing, and applications through various penetration tests. It also manipulates defence and detection tools to circumvent security measures while remaining opaque. It includes targeting the people (i.e., employees), facilities, and the organization's safety culture to validate how well defence controls stand up to and protect against a real opponent in all respects.

4. Cloud Security Assessment: A cloud security assessment is performed to assess the state of the cloud according to the best practices of the cloud service provider. This focuses on identifying vulnerabilities in cloud infrastructure and mitigating them through various access control administrations and appropriate layers of security and governance. Specifically, cloud security assessment is used to identify risks and threats to all cloud-based assets. It helps to determine weak ingress and access point to cloud infrastructure. The cloud security rating is absolutely for companies that use SaaS (Software as a Service), IaaS (Infrastructure as a Service) or PaaS (Platform as a Service) models for their day-to-day operations.

5. Third-party Risk Assessment: A third-party risk assessment or vendor risk assessment is performed to quantify the associated risk that the organization's third-party relationship can impose. It is usually done while outsourcing any services or product to evaluate risk based on the shared information.

6. Risk Assessment: A cybersecurity risk assessment is a process of mapping risks and threats on vulnerabilities identified through penetration testing, vulnerability assessment, social engineering assessment, and other cybersecurity assessments. Risk assessment solely evaluates the critical, non-critical assets and risk surfaces that can be potentially affected through cyber-attack or any other cyber incident. It helps to verify

security measures and safeguard the internal and external environment against security threats and attacks. With a proactive approach, risk assessment can help organizations prepare incident response plans and outline risk remediations.

7. Security Audit: A security audit is the technical assessment of organization policies and controls. Where other security assessments focus on finding vulnerabilities and strengthening security and defensive possession, the audit focuses on mapping an organization's current security posture with security industry standards according to business and security requirements. It is conducted annually to meet security compliances and company policy requirements such as HIPAA, SOX, PCI DSS, etc., and occasionally to keep track of business security status.

8. Bug Bounty: A bug bounty is considered an ongoing security assessment and is commonly misinterpreted as a substitute for application penetration testing. Many organizations and software development companies are adopting it. In Bug Bounty, bug hunters or independent security researchers discover exploitable vulnerabilities and bugs in open company software, websites or other assets and report them to the relevant/affected organization in exchange for recognition and financial compensation.

9. CIS Control Assessment: CIS Controls and benchmark assessment helps organizations of all sizes to follow and incorporate security industry best practices. It allows the businesses to assess, compare and track their documentation, implementation, and missing security configuration to improve the overall security presence. It is performed to evaluate the assets from the inventory stage to incident readiness and response.

10. Application Security Program Assessment: This assessment manages to implement security in the overall application or software development to reduce the security skill gap, manage resources, and integrate security into the software development life cycle (SDLC). This is specifically a handful in sustaining extensive application development and designing from the initial requirement gathering stage to the final delivery stage. It helps software and app-development businesses to build secure applications/software from scratch through Secure Architecture Review (SAR) to Threat Model and Secure Coding Practices.

11. **Ransomware Simulation Assessment:** Ransomware simulation assessment helps organizations analyse the impact of a ransomware attack, i.e., how far the consequences of a successful ransomware attack the organization would have to face, what is the Mean Time To Detect (MTTD), and what's the Mean Time To Respond (MTTR). It evaluates the defence capability to prevent, detect, respond and contain ransomware. Ransomware simulation assessment is usually carried by third-party resources to test the organization's blue team readiness and employees' security awareness level.

12. **Incident Response Readiness Assessment:** An incident response readiness assessment is performed to evaluate how well an organization is prepared to combat the cyber-attack and depreciate the damage. It provides a technical and fundamental attack-driven analysis to calculate the response capabilities to stand against the malware, viruses, and other attack vectors upcoming from advanced threat actors and state-sponsored attackers. Similar to ransomware simulation assessment, this is also carried out by third-party resources to evaluate the organization's preparedness, current security controls, and defensive abilities.

13. **Table Top Exercises (TTX):** Unlike other cybersecurity assessments, tabletop exercise does not include any type of real cyberattacks or exploitation. Instead, it is a theoretical cybersecurity assessment meant to prepare the organization and security team for potential cyber threats under different realistic risks and security event scenarios. It helps determine the organization's readiness and how effective their current plan is to respond to any real cyber.

Steps taken in estimating and assessing in a system can be represented in a flow chart as seen in Figure 1.1

There are generally 2 categories of assessments:

1. **Quantitative assessments:** assessments that focus on numbers and percentages, can help you determine the financial impacts of each risk.
2. **Qualitative assessments:** help you assess the human and productivity aspects of a risk.



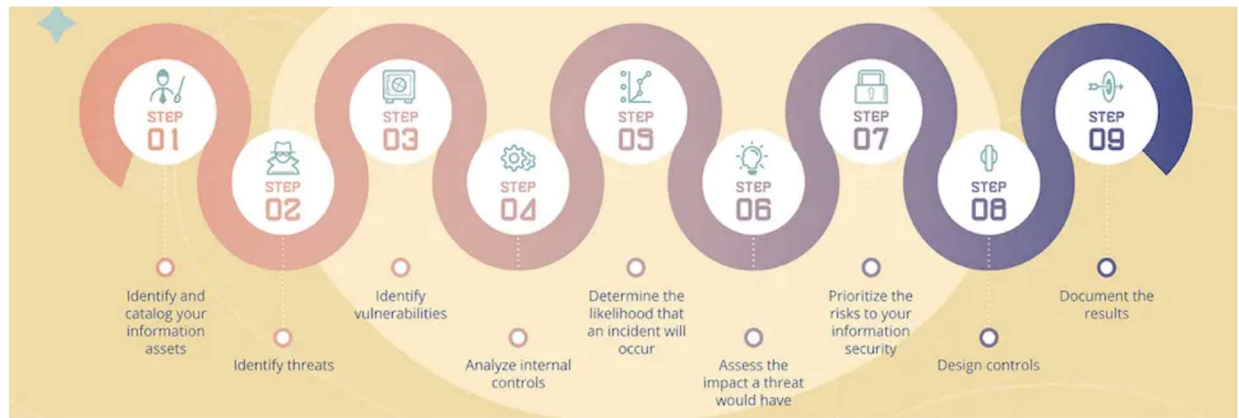


Figure 1.1 – Flow cycle of steps taken in estimation and assessment

Both of these categories have value, and both of them will allow you to communicate risk with different types of people. For example, your legal and financial teams will likely be most interested in the numbers, while your operations teams, such as sales and customer service, will be more concerned about how a security event would affect their operations and efficiency.

Steps for conducting a basic assessment of the cyber reliability of information communication systems [1]

- Identify and catalogue your information assets: The first step in a risk assessment is to make sure that you have a comprehensive list of your informational assets. It's important to remember that different roles and different departments will have different perspectives on what the most important assets are, so you should get input from more than one source here. For salespeople, the most important information asset might be your company's CRM, while IT likely sees the servers they maintain as a higher priority. Once you have identified all of your information assets and key stakeholders within all departments, you'll need to classify these data assets based on their sensitivity level as well as the strategic importance of the asset to the organization.

- Identify threats: When thinking about threats to data security, hackers are usually top of mind, but threats to your business's information security come in many different forms. You can see from this list of 2019 data breaches that while hackers exploiting weaknesses in a business' firewalls or website security programs has been very common, a

lot of different threat types contributed to data breaches in 2019. You need to take into account many different threat types when compiling a list of all the unique threats your business faces. For example, you also have to take into account not just malicious human interference, but also accidental human interference, such as employees accidentally deleting information or clicking on a malware link. Depending on the quality of your hardware and your information systems.

- Identify vulnerabilities: A vulnerability is a weakness in your system or processes that might lead to a breach of information security. For example, if your company stores customers' credit card data but isn't encrypting it, or isn't testing that encryption process to make sure it's working properly, that's a significant vulnerability. Allowing weak passwords, failing to install the most recent security patches on software, and failing to restrict user access to sensitive information are behaviours that will leave your business's sensitive information vulnerable to attack. During the coronavirus health crisis, another vulnerability you may face is the lack of staff.

- Analyse internal controls: After identifying the vulnerabilities in your systems and processes, the next step is to implement controls to minimize or eliminate the vulnerabilities and threats. This could be either a control to eliminate the vulnerability itself or a control to address threats that can't be totally eliminated. Controls can be technical, such as computer software, encryption, or tools for detecting hackers or other intrusions, or non-technical, such as security policies or physical controls. Controls can also be broken down into preventive or detective controls, meaning that they either prevent incidents or detect when an incident is occurring and alert you. Creating effective controls requires experience and skills.

- Determine the likelihood that an incident will occur: Using all the information you have gathered – your assets, the threats those assets face, and the controls you have in place to address those threats – you can now categorize how likely each of the vulnerabilities you found might actually be exploited. Many organizations use the categories of high, medium, and low to indicate how likely a risk is to occur. So, if, for example, a core application you use to run your business is out-of-date and there's no process for regularly checking for updates and installing them, the likelihood of an incident involving that system

would probably be considered high. On the other hand, if you handle a large volume of personal health information, have automated systems for encrypting and anonymizing it, and regularly test and check the effectiveness of those systems, the likelihood of an incident could be considered low.

- Assess the impact a threat would have: This step is known as impact analysis, and it should be completed for each vulnerability and threat you have identified, no matter the likelihood of one happening.

Your impact analysis should include three things:

The mission of the system, including the processes implemented by the system

The criticality of the system, determined by its value and the value of the data to the organization.

1. Prioritize the risks to your information security: Prioritizing your security risks will help you determine which ones warrant immediate action, where you should invest your time and resources, and which risks you can address at a later time. For this step, it might help to utilize a simple risk matrix that helps you use the information you already have about each vulnerability/threat pair you've identified and plot it on the matrix. Risks that are both likely to happen and would have severe consequences would be mapped as a high priority, while risks that are unlikely to happen and would have marginal consequences would be mapped as the lowest priority, with everything else falling somewhere in between. You can make your risk matrix as simple or as complex as is helpful to you. If you're a large organization with a lot of risks competing with each other for time and attention, a more in-depth 5×5 risk matrix will likely be helpful.

2. Design controls: Once you've established priorities for all risks you've found and detailed, then you can begin to make a plan for mitigating the most pressing risks. To determine what controls, you need to develop to effectively mitigate or eliminate the risks, you should involve the people who will be responsible for executing those controls. Senior management and IT should also be heavily involved to ensure that the controls will address risks and align with your organization's overall risk treatment plan and end goals. You'll also need to develop a plan for implementing all of the new controls.

3. The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and so on. For each threat, the report should describe the corresponding vulnerabilities, the assets at risk, the impact to your IT infrastructure, the likelihood of occurrence and the control recommendations. The risk assessment report can identify key remediation steps that will reduce multiple risks. For example, ensuring backups are taken regularly and stored offsite will mitigate both the risk of accidental file deletion and the risk from flooding. Each step should detail the associated cost and the business reasons for making the investment.

### 1.3 Importance of regular assessments

In particular, it enables them to:

- identify and re-enforce IT security gaps;
- stop data breaches;
- choose appropriate protocols and controls to control and minimize risks;
- prioritize the protection of the asset with the highest value and highest risk;
- eliminate unnecessary control measures;
- evaluate potential security partners;
- establish, maintain and prove compliance with regulations;
- accurately predict future needs.

We can understand risk using the following equation [2]:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset} \quad (1.1)$$

Where threat, vulnerability, asset – variable expectation, although risk is represented here as a mathematical formula, it is not about numbers; it is a logical construct. For example, suppose you want to assess the risk associated with the threat of hackers compromising a particular system. This isn't strictly a mathematical formula; it's a model for understanding the relationships among the components that feed into determining risk:

- Threat is short for “threat frequency,” or how often an adverse event is expected to occur. For example, the threat of being struck by lightning in a given year is about 1 in 1,000,000.

- Vulnerability is shorthand for “the likelihood that a vulnerability will be exploited and a threat will succeed against an organization’s defences.” What is the security environment in the organization? How quickly can disaster be mitigated if a breach does occur? How many employees are in the organization and what is the probability of any given one becoming an internal threat to security control?

- Cost is a measure of the total financial impact of a security incident. It includes hard costs, like damage to hardware, and soft costs, such as lost business and consumer confidence.

Other costs can include:

- Data loss – theft of trade secrets could cause you to lose business to your competitors. Theft of customer information could result in loss of trust and customer attrition.

- System or application downtime – if a system fails to perform its primary function, customers may be unable to place orders, employees may be unable to do their jobs or communicate, and so on.

- Legal consequences – if somebody steals data from one of your databases, you can incur fines and other legal costs because you failed to comply with the data protection security requirements of various compliances.

The risk assessment factors in the relationship between the three elements. For example, suppose you want to assess the risk associated with the threat of hackers compromising a particular system. If your network is very vulnerable (perhaps because you have no firewall and no antivirus solution) and the asset is critical, your risk is high. However, if you have robust perimeter defences that make your vulnerability low, your risk will be medium, even though the asset is still critical. Note that all three elements need to be present in order for there to be risk – since anything times zero equals zero, if one of the elements in the equation is not present, then there is no risk, even if the other two elements are high or critical.

Individuals or Organizations tasked and or authorised to make assessments: A comprehensive approach is essential for identifying all areas of cyber vulnerability. Instead of relying on a few IT team members, a thorough risk assessment should involve representatives across all departments where vulnerabilities can be identified and contained. Look for individuals who know how data is used within the company. Depending on the size of your organization, assembling a complete IT risk assessment team may be a difficult task. While larger organizations might want to have their internal IT teams lead the effort, businesses that lack an IT department might need to outsource the task to a company specializing in IT risk assessment.

#### 1.4 Governance and risk management

Organizations and businesses need to establish and implement a cybersecurity governance framework that supports informed decision making and escalation across the organization to identify and manage cybersecurity risks. The framework should include defined risk management policies, processes and structures, along with relevant controls adapted to the nature of the cybersecurity risks the enterprise faces and the resources the enterprise has at its disposal. Effective practices include: establishing a governance framework to support decision-making based on risk appetite; ensure the active involvement of senior management and, if appropriate for the company, at the management level in IT security matters; identify frameworks and standards for addressing cybersecurity; use metrics and thresholds to inform governance processes; use resources to achieve the desired risk attitude; and conducting cyber security risk assessments. An effective business practice is to define and maintain a governance framework for managing cyber security risks and related controls that are appropriate to the size of the organization and the nature of the cybersecurity risk exposure. The governance framework should articulate the roles and responsibilities of organizational units and individuals within those units. As used in this report, "governance" and "governance framework" generally refer to the definition of "policies, procedures and processes to manage and monitor the regulatory, legal, risk, environmental and operational requirements of the organization".

Within the organization and informing management about IT security risks. "Management" generally refers to the implementation of such control measures. The governance framework should enable organizations to become aware of relevant cybersecurity risks, assess their severity, and decide how to manage each risk (i.e., accept, mitigate, pass on or avoid the risk). Most of the companies' time will be devoted to mitigation, including identifying, selecting, implementing, monitoring performance, and updating the controls that companies use in their cybersecurity programs. The risk management function, on the other hand, can provide standards and objective monitoring of the implementation of these controls. Finally, an appropriate independent function, such as internal or external audit, can evaluate the implementation and effectiveness of the company's cybersecurity program. This may include reviewing a company's cybersecurity controls and processes to determine if they are performing as intended and assessing whether the controls are appropriate for the company's risk appetite.

Observation on Firm practices: Some companies have pointed out the important role the board of directors plays in their company's cybersecurity efforts. In these companies, the board of directors has been actively involved in approving the company's overall cybersecurity strategy and overseeing its implementation. This engagement, offered by companies, has had a strong positive effect in attracting attention and providing cybersecurity resources. FINRA stresses the importance of actively involving executives in prioritizing and monitoring the implementation of companies' responses to cyber security threats. The board's reporting practices varied among the companies rated by FINRA. In some companies, the board receives annual cybersecurity reports, while others report on a quarterly basis. A number of offices also provide ad hoc reports to the board on major cybersecurity events. The management of some companies reports to the board of directors, while the management of others depends on a sub-committee of the board. In addition to the benefits of proactively engaging senior management in cybersecurity initiatives, companies also need to be aware of the drawbacks of under-engagement. This includes the obvious risk that the company is more vulnerable to successful cybersecurity attacks. A case study is presented: In one case where FINRA took enforcement action, hackers used a SQL injection attack on a company's database server to obtain sensitive customer information from over

200,000 customers, including names, account numbers, social security numbers, addresses and dates of birth. The company stored the data on a computer with an internet connection and did not encrypt the information. The company only became aware of the breach when hackers attempted to extort money from the company. In fact, these violations were visible in the company's web server logs. The case demonstrates governance failures in multiple ways. Overall, the company does not have adequate safeguards in place to protect customer data. Specifically, the law firm stored confidential client data in plain text in an Internet-connected database without effective password protection. Although the company conducted penetration testing, it did not include any assets containing sensitive customer information as part of this testing. Additionally, the company has not established procedures to review web server logs that would reveal the data theft. And the company did not respond to an earlier recommendation from an auditor to purchase an intrusion detection system. Finally, the company had not established written procedures for its information security program to protect confidential customer information.

### 1.5 Real-life example of cyber-attack operations

Many nation-states' actors are committing cyber-attacks against one another including the United States, United Kingdom, Ukraine, North Korea, and Russia. That said, China and the US have the two most sophisticated cyber warfare capabilities. Outside of nation-states, there are also non-nation states entities that perform cyber terrorism to shut down critical national infrastructures like energy, transportation, and government operations or to coerce and intimidate the government or civilian population. For example, in February 2020 the Iranian telecommunications infrastructure suffered from a distributed denial of service (DDoS) attack that led to national connectivity falling to 75% of usual usage. This is part of the reason why China and the United States have invested heavily in cyber warfare programs.

China's Cyber Warfare Program: The People's Liberation Army (PLA) has a cyberwarfare strategy called "Integrated Network Electronic Warfare" that guides computer network operations and cyber warfare tools. The strategy links network warfare tools and



electronic warfare weapons against an opponent's information systems during the conflict. The PLA believes that seizing control of an opponent's information flow and establishing information dominance is fundamental to warfare success. By focusing on attacking infrastructure to disrupt transmission and information processing gives the PLA cyber dominance over their enemies. The PLA may use electronic jammers, electronic deception and suppression techniques to achieve interruption. They may also use more traditional techniques like viruses or hacking techniques to sabotage information processes. The key focal point is to weaken the enemy's cyber abilities to maximize the physical offensive. Additionally, it is suspected that the Chinese government gathers data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning.

**The United States' Cyber Warfare Program:** The United States focuses on security plans in response to cyber warfare, acting in defence rather than attacking. The responsibility for cybersecurity is divided between the Department of Homeland Security (Homeland Security), the Federal Bureau of Investigation (FBI) and the Department of Defence (DOD). Recently Cyber Command was formed as a dedicated department to tend to cyber threats to ensure the President can navigate and control information systems via the Internet. Cyber Command is a military subcommand under US Strategic Command and is responsible for protecting military cyberinfrastructure. Cyber Command is made up of Army Forces Cyber Command, Twenty-fourth Air Force, Fleet Cyber Command, and Marine Forces Cyber Command. Both state and non-state actors target the United States in cyber warfare, cyber espionage, and other cyber-attacks, so Cyber Command was designed to dissuade potential adversarial attacks by conducting cyber operations of its own.

## 2 VULNERABILITIES IN INFOCOMMUNICATION SYSTEMS AND NETWORKS

The complexity of the systems increases day by day. This leads to more and more vulnerabilities in systems. Attackers use these vulnerabilities to exploit the victim's system. It is best to discover these vulnerabilities in advance before attackers do. The power of vulnerability assessment is usually underestimated. While vulnerability assessment and penetration testing can be used as a cyber defence technology to provide proactive cyber defence. In this article, we have demonstrated vulnerability assessment and penetration testing (VAPT) as a cyber defence technology, how we can provide active cyber defence using vulnerability assessment and penetration testing. We have described the entire life cycle of vulnerability assessment and penetration testing on systems or networks and the proactive action taken to correct that vulnerability and stop potential attacks. In this article, we have described common vulnerability assessment techniques and some well-known premium / open source VAPT tools. We have described the entire process for using vulnerability assessment and penetration testing as a powerful cyber defence technology. Vulnerability assessment and penetration testing are a gradual process.

Vulnerability Assessment is the process of scanning your system or software or network for weakness and loophole. This loophole can provide the attacker with a back door to attack the victim. A system may have an access control vulnerability, boundary condition vulnerability, import validation vulnerability, authentication vulnerability, configuration. Penetration tests attempt to exploit this system in an authorized manner to discover possible exploits in the system. In penetration tests, the tester has: the authority to perform penetration tests and intentionally exploit the system and discover possible exploits. The vulnerability scan and penetration test consist of a total of 9 steps. These steps are illustrated in the following image. First, the tester must specify the scope of the mission (black / grey / white box). After determining the size, the tester receives information about the operating system, network, and IP address during the Explore step. After This Tester Use various vulnerability assessment techniques (explained later) on the test object to find

vulnerabilities. The tester then analyses the well-founded vulnerability and makes a plan for the penetration tests.

The tester uses this plan to: Break into the victim's system. After logging into the system, the tester increases the privilege on the system. In the results analysis phase, the tester analyses all the results and makes recommendations to correct the weaknesses of the system. All of these activities are documented and reported to management for appropriate action. After all these steps, the victimized system and its program are affected and modified. In the clean-up step, we restore the system to the previous state before the VAPT process started. VAPT can be represented as a lifecycle of ordered stages, as shown in Figure 2.1 [3]

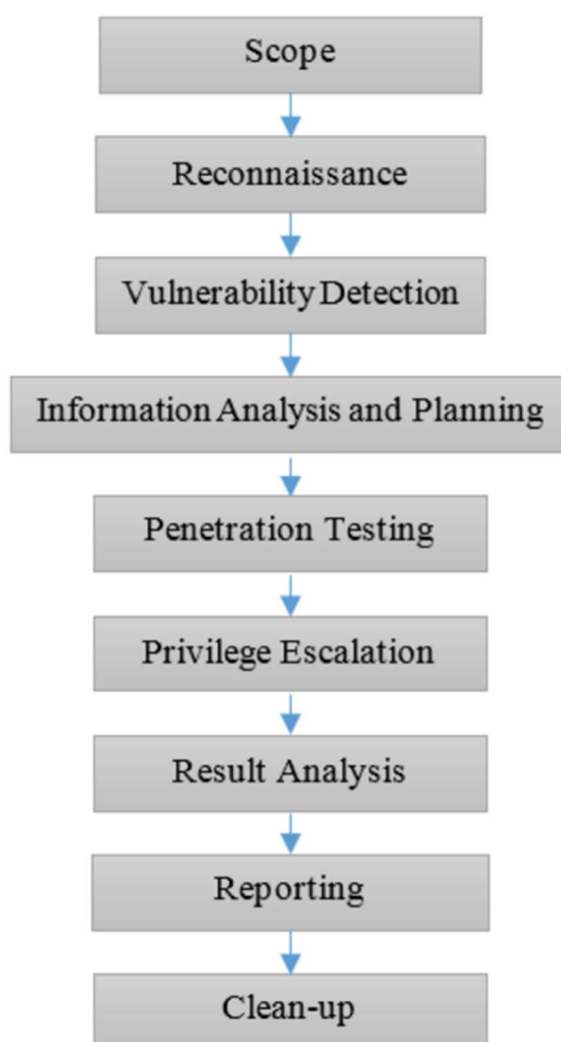


Figure 2.1 – Vulnerability assessment and penetration testing life cycle

## 2.1 Graph theory and its importance

The set of vertices of a graph  $G$  is denoted by  $V(G)$  and the set of edges is denoted by  $E(G)$ . We can simply call these sets  $V$  and  $E$  if the context makes the particular graph clear. For simplification we do not denote  $\{u, v\}$ , but simply  $uv$ . The order of a graph  $G$  is the cardinality of its set of vertices and the magnitude of a graph is the cardinality of its set of edges. Given two vertices  $u$  and  $v$ , if  $uv \in E$  then  $u$  and  $v$  are adjacent. In this case,  $u$  and  $v$  are called endpoints of edge  $uv$ . If  $uv \notin E$ , then  $u$  and  $v$  are not adjacent. Also, if an arc  $e$  has a vertex  $v$  as its extremity, we say that  $v$  is incident with  $e$ . The neighbourhood (or open neighbourhood) of a node  $v$ , given by  $N(v)$ , is the set of neighbouring nodes of  $v$ :

$$N(v) = \{x \in V \mid vx \in E\} \quad (2.1)$$

Where the closed neighbourhood of a vertex  $v$ , denoted by  $N[v]$ , is simply the set  $\{v\} \cup N(v)$ . Given a set  $S$  of vertices, we define the neighbourhood of  $S$ , denoted by  $N(S)$ , to be the union of the neighbourhoods of the vertices in  $S$ . Similarly, the closed neighbourhood of  $S$ , denoted  $N[S]$ , is defined to be  $S \cup N(S)$ . The degree of  $v$ , denoted by  $\deg(v)$ , is the number of edges incident with  $v$ . In simple graphs, this is the same as the cardinality of the (open) neighbourhood of  $v$ .

$$\Delta(G) = \max \{\deg(v) \mid v \in V(G)\} \quad (2.2)$$

Where maximum degree of a graph  $G$ , denoted by  $\Delta(G)$ , is defined to be

$$\sigma(G) = \min \{\deg(v) \mid v \in V(G)\} \quad (2.3)$$

Where the minimum degree of a graph  $G$ , denoted by  $\delta(G)$ , is defined to be

The importance of graph theory was first recognized by Euler in 1736. He used it to identify a suitable route that would allow a single person in the city of Königsberg to cross exactly seven bridges and return to the starting point. Euler not only proved the existence of such a path, but also provided a general solution that could be applied to any arbitrarily arranged land mass and bridge structure. He also noted that the physical distance and geographical position of the bridges are not important in determining the correct solution and that the geometric position of the bridges is important. A graph is a mathematical representation of a network made up of interconnected components called nodes, with the connections between these nodes called edges. A graph can be represented in several ways: an undirected graph does not show directional information at the connections, while a directional graph shows the direction of information flow through the links. Furthermore, in binary graphs, the presence of an edge is indicated by one and the absence of an edge by a zero, while in a weighted graph the connection force is quantified as the weight of the connections. Furthermore, connection density can vary from fully connected graphs, also known as fully connected graphs, to very sparse graphs.

In a graph theory view, network components are represented as nodes and edges connecting those nodes. In a transport geography, most networks have a clear spatial basis, namely road and rail networks, which are defined more by their links than by their nodes. This is not necessarily the case for all transport networks. For example, sea and air networks are generally defined more by their nodes than by their connections, as connections are often not clearly defined. A telecommunications system can also be represented as a network, while its spatial expression can have limited meaning and would actually be difficult to represent. Mobile telephone networks or the Internet, perhaps the most complex graphs to consider, are relevant cases of networks with a structure that is difficult to symbolize. However, cell phones and antennas can be represented as nodes, while connections can be individual phone calls. Routers, the heart of the Internet, can also be represented as nodes on a diagram, while the physical infrastructure between them - fibre optic cables - can act as links. Therefore, all transport/communication networks can be represented by graph theory in one way or another. Each graph differs from the others based on the properties of each node and edge. These individual components of a network affect their individuality

relative to others, allowing researchers to carefully analyse the properties of a network by monitoring only a set of components, nodes, or edges. The interconnection of these individual components determines the structure of a network and much research has been done in the past to identify important / vital network structures. For example, in a multi-hop wireless sensor network (WSN), nodes can be connected using different edges, each of which is shorter in length than a conventional WSN, to reduce the transmission power for the network. Nodes in a network are evaluated based on both their geographic location and the combined influence of all edges connected to that node. The geographic location of a node helps to approximate the speed of traffic flow through nodes, as it has been found that nodes near the centre of the network will experience more traffic flow than nodes near the edge of a network. The latter, on the other hand, is so important that a node with a greater number of arcs is in proximity to a greater number of nodes in the network and is therefore essential to ensure network connectivity. Further elaboration of this phenomenon is explained later in this work. The combined effect of the above two attributes define the importance of a node in a network. Due to these characteristics, some nodes in a network, when removed, will cause part of the network to become disconnected and hence degrade the performance of a network. These nodes are called points of articulation; Figure 2.2 explains the difference between hinge nodes and critical nodes [4].

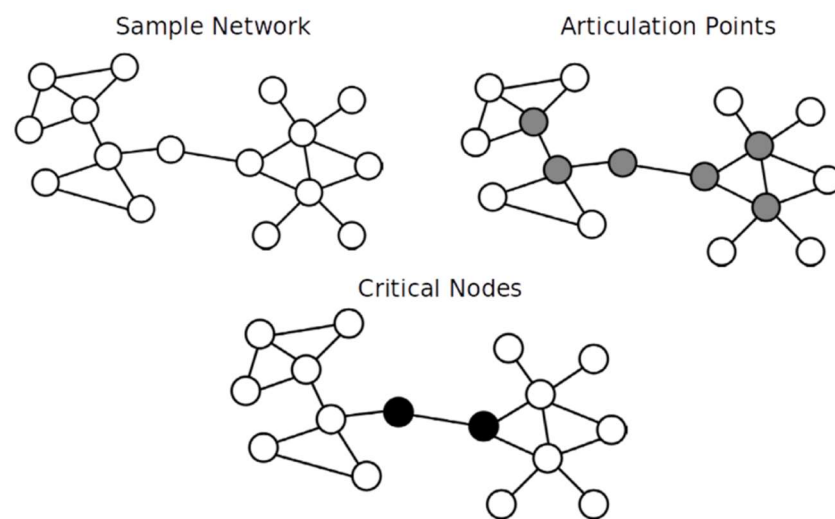


Figure 2.2 – Difference in articulation points and critical nodes

We represent the points of articulation in grey colour. As can be seen in the Figure, removing one of these articulation points makes the network disconnected, where we use the term disconnected for a network where each node is not accessible to all other nodes in the network. Some of these articulation points have been shown to signal greater network performance degradation, and these black-coloured points are called the critical nodes of a network. The example above is a special case where the critical nodes are also hinge points. Researchers have defined critical nodes in different ways in the literature [13].

### Optimization problems

An Integer Linear Programming problem is composed by a linear objective function and same constraints, moreover the solutions belong to the set of dimensional vectors  $n$  having integer components,  $\mathbb{Z}^n$ . An ILP problem is defined adopting the general form [4]:

$$\begin{aligned} z &= \min(c^T x), \\ Ax &\leq b, \\ x &\in \mathbb{Z}^n \end{aligned} \tag{2.4}$$

Where  $z$  is the cost of the solution computed by the objective function  $\min(c^T x)$ ,  $c \in \mathbb{R}^n$  represents the vector of the costs associated to each decision variable  $x_i$ . The expression  $Ax \leq b$  - constraints.  $A$  is an  $m \times n$  matrix whose entries  $a_{ij} \in \mathbb{R}$  and  $m$  is the number of the constraints. The constraints in an integer program form a polytope. However, the feasible set is given by the set of all integer-valued points within the polytope, and not the entire polytope. Therefore, the feasible region is not a convex set. Moreover, the optimal solution may not be achieved at an extreme point of the polytope; it is found at an extreme point of the convex hull of all feasible integral points. The naive way to solve an ILP problem is to simply remove the constraint that  $x$  is integer, solve the corresponding LP, that is the relaxation of ILP by neglecting the presence of the integer constraint, and then round the entries of the solution to the LP relaxation. But, not only may this solution not be optimal, it may not even be feasible, that is it may violate some constraints.

## 2.2 Problem Definition

Identifying critical nodes plays a crucial role in accessing network vulnerabilities, and there are several approaches in the literature that can be used to identify critical nodes in a network. Some of the existing algorithms are based on intuition, while others are based on mathematical abstractions of networks of arbitrary topology and are therefore characterized by properties that can be verified analytically before implementation.

Most of these approaches identify critical nodes based on a node's impact on the traffic flow pattern of the network or use the topological structure of the network to identify these critical nodes. To our knowledge, there is no such algorithm in the literature that identifies critical nodes based on both the topological structure and the traffic flow pattern of the network. To solve this problem, this work proposes two metrics, the first one is based on intuition and uses a newly defined node diversity metric that includes node weighted degree and link length variation of a node to deal with the topological properties of a network. The weighted degree of nodes metric is a minor variant of the well-known degree of centrality metric, the main difference being the assessment of the degree of a node based on the number of new nodes introduced by a given node over time. as it is in the network is accessible. The variation in the link length metric results from evaluating the effect of the average path length (APL) of a network. The variation in link length metric assesses the diversity of a network by exploiting the difference in path length maintained by a node.

The idea behind this approach is that a node connecting multiple nodes at different distances most likely acts as a bridge node between different network nodes, so removing this node is likely to result in higher performance degradation. The traffic flow model, on the other hand, is included in this metric for evaluating critical nodes using Banzhaf's performance index, is a subvariant of the well-known average centrality metric, and was previously used for weighted voting games. The second metric is based on a purely mathematical abstraction, where we formulate the problem of identifying critical nodes as an optimization problem, where the goal is to identify a node which, after being removed, has the greater impact on the connectivity of the two networks. algebraically than the maximum traffic flow of the whole network [5].



### 2.3 Node importance metrics

Connection-based approaches identify the criticality of a node based on the information flow pattern of a network. The information flow model in a network emphasizes the speed of data flow through each individual node and also helps to identify the node that could be causing a potential bottleneck in the network. Both parameters play a key role in identifying node criticality and there are many approaches in the literature that use the information flow model of a network to identify node criticality.

Average path metric length:

The average path length metric is one of the most common metrics and is also referred to as the characteristic path length metric of a network. This metric uses the sum of the shortest path from each node to all other nodes in the network to identify the most critical node in the network. In a graph  $G = (V, E)$ , where  $V$  is the set of vertices and  $E$  is the set of arcs, the characteristic length of the path is defined by:

$$l = \left( \frac{1}{N(N-1)} \right) \sum_{v \in V} \sum_{w \neq v \in V} d(v, w) \quad (2.5)$$

Where  $d(v, w)$  is the geodesic distance between  $v$  and  $w$  with  $v, w \in V$ , i.e., the cumulative distance of all edges that lie on the shortest path between the two nodes, and the factor  $1/N(N-1)$  is that over the total number of pairs of nodes. In such a network, a larger value of  $l$  represents a relatively longer time for the message to propagate through a network, while a smaller value of  $l$  indicates a tightly connected network in which nodes are placed close to each other. The average path length metric identifies such a node as the most critical node that has the greatest impact on the average path length of the entire network. It is easy to associate that the node with the shortest path length matches all other nodes in the network.

Closeness Centrality Metric:

This metric identifies the criticality of a node by analysing the total distance of a node with all nodes in the network, and therefore a node is considered critical which has the

lowest total distance and is therefore closer to all nodes of the network. The phenomenon behind using this metric is that a node which is closer to all other nodes in the network will end up having the highest network traffic through it because it can reach the maximum number of nodes in the network with the shortest distance. To calculate a node's proximity centrality, researchers use the inverse of the total distance from a given node to all other nodes in a network.

$$CC(v) = \frac{1}{\sum_{u \in V} d(v, u)} \quad (2.6)$$

Where,  $d(v, w)$  is the geodesic distance between  $v$  and  $w$  with  $v, w \in V$ , i.e., the cumulative distance of all the edges that lie in the shortest path between the two nodes. Unlike the average shortest path metric which is defined as the average distance of the whole network, the closeness centrality metric is a node specific metric, it identifies how close each individual node is to the rest of the network nodes.

**Betweenness Centrality metric:** This is also a metric based on the shortest path and identifies the most critical node based on the number of shortest paths a node participates in, a node that participates in the highest number of shortest paths will have the highest influence on the performance of the network upon its removal and it is considered as the most critical node.

**Ego Centrality metric:** The ego centrality metric is designed for a special class of graphs known as centred graphs, these graphs are in a star structure, thus limiting the nodes of a direct neighbour link or a 2-hop path between any two nodes in the net. The ego centrality metric uses this graph structure and determines the criticality of a node based on the number of times a node participates in the formation of this path with two jumps between any two nodes. This definition is consistent with the previously defined betweenness centrality metric, but the main difference lies in the type of network structure. Since the ego centrality metric was mainly defined for the star network, the maximum length between two nodes of a graph cannot exceed two hop counts.

## 2.4 Critical node identification

Identifying critical nodes in complex networks is important for studying network survivability and robustness. Previous studies on the structure hole theory have revealed that structure holes are gaps between a set of indirectly connected nodes and intermediaries that fill the holes and act as intermediaries for the exchange of information. We exploit the property of structural holes to design a heuristic algorithm based on local network topology information to identify the importance of nodes in undirected and unweighted networks whose adjacency matrix is symmetric. In the algorithm, a node with a higher degree and a larger number of structural holes connected to it gets a higher importance ranking. Six real networks are used as test data. The experimental results show that the proposed method not only has low computational complexity, but also has degree centrality, k-shell method, map entropy centrality, collective influence algorithm, DDN algorithm based on the degree of node and its neighbours and outperforms the random ranking method to determine the importance of nodes for network connectivity in complex networks. An unweighted and undirected network  $G(V, E)$  with  $N = |V|$  nodes and  $M = |E|$  Edges taken into account.

The network could be described by an adjacent matrix  $A(a_{ij})$  where  $a_{ij} = 1$  means there is a link connecting node  $i$  and node  $j$ , and otherwise  $a_{ij} = 0$ . The degree value of node  $i$  is represented by  $k_i$ . We begin our analysis by introducing a theory for the study of competitive relationships in social networks based on so-called structural holes. From a sociological perspective, structural holes are gaps between a group of indirectly connected nodes, and some individuals who act as structural hole keys to fill the hole receive more network benefits than their neighbours. Take the following figure as an example: There are three structural holes, marked with dotted arrows, associated with the intermediate node Ego. Compared to its neighbours A, B, C and D, Ego gets more network advantages than its neighbours because there is no alternative communication channel between them. Obviously, the ego node plays an important role in maintaining network connectivity, and we can conclude that the higher the value of a node, the higher the number of structural holes associated with the node, the greater the node is tall. The relationship between the ego knot and the structural holes is shown in Figure 2.3 [3].

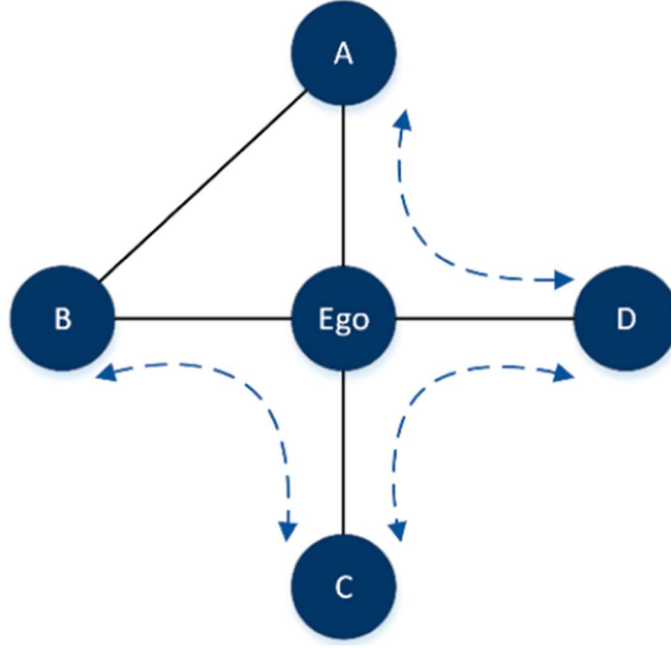


Figure 2.3 – Concept of structural hole

In view of the analysis above, we leverage the property of structural holes to design an intuitive algorithm for quantifying node importance in maintaining the network connectivity, based on degree algorithm for quantifying node importance in maintaining the network connectivity, based on degree and structural hole count, expressed by

$$DSHC_i = \sum_{j \in \Gamma_i} \left( \left( \frac{1}{k_i} + \frac{1}{k_j} \right) * \frac{1}{1 + \Delta_{ij}} \right)^2 \quad (2.7)$$

Where  $\Gamma_i$  is an expression of neighbour set of nodes  $i$  and  $\Delta_{ij}$  is the number of structural holes formed between node  $i$  and  $j$  with node  $i$  as the intermediary. According to Equation (2.7), the larger the degree of a node and its neighbours, and the higher the number of structural holes between the node and its neighbours, this means that the stronger the irreplaceability of nodes in the structure, the smaller the value of DSHC will be. We use several popular heuristic methods that are also based solely on the network topology to investigate the performance of the proposed method. These measures include:

- Degree centrality is a basic ranking algorithm to evaluate the importance of nodes.

The degree of node  $i$  can be defined as

$$k_i = \sum_{j=1}^N a_{ij} \quad (2.8)$$

Where  $i$  and  $j$  are individual nodes of the arc

- The  $k$ -shell decomposition algorithm categorizes the nodes into core nodes and fringe nodes. The algorithm steps are as follows: First, delete all nodes that have only one connection and assign those nodes to the 1-shell. In this process, there may be new nodes with  $k = 1$ , and then pruning is repeated until all nodes with  $k = 1$  are removed. The removed nodes will be classified using a 1-shell. Next, this process continues in a similar way for nodes with degree  $k = 2$  and gets the 2-shell of the network. The pruning is repeated until all network nodes are assigned to one of the shells.

- The DDN method believes that the importance of a node is determined by the degree of the node and the degree of its neighbours, which is defined as

$$DDN_i = \sum_{j \in \Gamma_i} w_{ij} \quad (2.9)$$

Where  $i$  and  $j$  are individual nodes

- The ME centrality is based on local neighbourhood information, which is defined as

$$ME_i = -k_i \sum_{j=1}^P \log k_j \quad (2.10)$$

## 2.5 Critical node detection problem

A lot of approaches have been devoted to discover the presence of critical nodes in the networks. The authors of present a mathematical model based on the ILP approach which provides optimal solutions for the classical critical node detection problem (CNP). Given an undirected graph  $G = \{V, E\}$  and an integer  $k$ , the aim is to find a subset  $VC \subseteq V$  of the network's nodes such that  $|VC| \leq k$ , whose deletion minimizes the connectivity among the nodes in the induced subgraph  $G(V \setminus VC)$ . The problem admits the following ILP formulation:

$$\text{Min} \sum_{i,j \in V} U_{ij} \quad (2.11)$$

Where  $U_{ij} = 1$ , if  $i$  and  $j$  are in the same component of  $G(V \setminus A)$  and 0 if otherwise. The objective function of the proposed problem is related to the minimization of the nodes able to communicate via an undirected path among the induced subgraph  $G(V \setminus VC)$ .

Cardinality constrained critical node detection problem: Another formulation based on the optimization approach is presented in which a slightly modified problem is tackled, namely the cardinality-constrained critical node detection problem (CC-CNP). In this perspective, a maximum allowed component size  $L$  of a connected graph is specified, and the goal is to minimize the number of attacked nodes required to satisfy this constraint. Given an integer  $L$ , the goal is to find a subset  $VC \subseteq V$  such that the largest connected component of the induced subgraph  $G(V \setminus VC)$  does not contain more than  $L$  nodes. The problem is therefore limited to the minimization of  $|VC| : |V_i| \leq L, 1 \leq i \leq T$ , where  $T$  is the total number of connected components in the induced subgraph  $G(V \setminus VC)$ . To describe this particular version of the problem, a Boolean variable is introduced.

$$\text{Min} \sum_{i \in V} v_i \quad (2.12)$$

Where  $v_i$  is 1 if the node is deleted in the optimal solution and 0 if otherwise

**$\beta$ -Vertex Disruptor:** A different ILP approach known as  $\beta$ -vertex disruptor is introduced in. The problem consists in the research of subset  $VC \subseteq V$  with the minimum cardinality, such that the connectivity in  $G(V \setminus VC)$ , obtained by removing the nodes in  $VC$  from  $V$ , is not more than. As introduced in the definitions of CNP and CC-CNP approaches, the decisional variables are  $u_{i,j}$  and  $v_i$ . The objective function consists in the minimization of removed nodes in  $VC$

**Large partition minimization:** The critical node detection approach presented in differs slightly from previous approaches. In this formulation, the objective function is a linear combination of two sub-objectives. More specifically, this model represents the perspective of an attacker who wants to remove nodes from the network to divide the network into a fixed number of partitions  $m$  while minimizing the size of the largest connected partition. In this way, the proposed model tends to provide a solution characterized by balanced partitions in terms of the number of nodes. As for the decision variables, the proposed approach requires  $O(mn)$  Boolean variables. More specifically, the variables  $x(1), \dots, x(m), c \in \{0, 1\}^n$ , so that  $x(i) = 1$  when the  $i$ -th node is assigned to the  $i$ -th partition and zero otherwise. the  $j$  input  $c_i = 1$  if the node is involved in the attack, zero otherwise. More precisely, the target function consists of two sub-goals as described: minimize the largest partition and minimize the weighted attack cost (i.e., the number of nodes attacked). According to the proposed formulation, the nodes that belong to the same partition are not necessarily connected each other. In more details the problem provides that, as described in the classical CNP, each node has to be assigned to just one set, and the nodes assigned to a partition  $V_i$  are not directly connected to the nodes in the others partitions

$$\sum_{i=1}^m x^{(i)} \leq 1_n \quad (2.13)$$

**Partition number and size minimization:** Another optimization problem for the discovery of network vulnerabilities. Here, the attacker aims at divide the network by

maximizing the number of partitions, by keeping the attack cost to the minimum, and by reducing the size of the largest partition. Similarly, the proposed problem requires  $O(n^2)$  Boolean variables. The decision variables are defined according to the following scheme:  $x^{(i)}_j = 1$  if node  $v_j$  is assigned to the partition  $V_i$ , moreover  $c_j$  is defined as a vector of Boolean variables such that  $c_j = 1$  if  $v_j$  is involved in the attack and  $c_j = 0$  otherwise. In more details, the objective function is a linear combination of three sub-objectives

**Multi objective optimization approach:** An innovative approach for the research of critical nodes. Differently from the previous approaches, in this case the problem is approached as Multi Objective Optimization problem. Indeed, it considers two conflicting objectives: the minimization of the network connectivity ( $f_1$ ) and the reduction of the total cost of the attack ( $f_2$ )

$$\min f(x) = \min[f_1(x), f_2(x)]^T \quad (2.14)$$

Where  $f_1$  is the minimization of the network connectivity and  $f_2$  is the reduction of the total cost of the attack. Note that the proposed approach requires  $n$  Boolean decision variables  $x_i$ , such that,  $x_i = 1$  if the  $i$ -th node is involved in the attack, 0 otherwise.

$$\begin{aligned} f_1 &= \text{PWC}(G(V \setminus V_c)) \\ f_2 &= \frac{\mathbf{c}^T \mathbf{x}}{\mathbf{1}^T \mathbf{c}} \end{aligned} \quad (2.15)$$

Where  $V_c$  is the set of nodes involved in the attack. In the attack cost ( $f_2$ ), the vector  $\mathbf{c} \in \mathbb{R}^n$  is introduced to describe the removal cost for each node of the network. Due to the conflicting nature of the two objective functions, the proposed schema is unable to find a unique optimal solution. Instead, each solution that belongs to the Pareto front is characterized by an attack cost and a connectivity value as defined in (2.15). In this way, it is possible to consider a set of multiple attackers' classes each one characterized by different preferences in terms of budget and attack strategy. Thanks to the analysis of each solution



in the Pareto front, it is possible to recognize those nodes of the network which more often appear as targets in the different attack strategies, i.e., in attack plans with different objectives and budgets [3].

## 2.6 General cyber security metrics

Metrics are tools to facilitate decision-making and improve performance and accountability. A cybersecurity metric contains the number of reported incidents, any fluctuations in these numbers as well as the identification time and cost of an attack. Thus, it provides stats that can be used to ensure the security of the current application. Organizations get the overall view of threats in terms of time, severity, and number. It is important today when this data keeps fluctuating. This way the organizations can maximize protection from threats in the future. Cybersecurity metric is the optimal way to monitor applications for cybersecurity.

Use of a Cybersecurity Metric: A Cybersecurity metric assists the organization in the following ways: It facilitates decision-making and improves overall performance and accountability, It helps in setting quantifiable measures based on objective data in the metric, It helps in making corrections in an efficient way, It brings together all the factors like finance, regulation, and organization to measure security, It maintains the log of every individual system that has been tested over the years

Some Cybersecurity Metrics: Here is a list of some important cybersecurity metrics that portray the current threat scenario really well.

A number of systems have vulnerabilities: A very important cybersecurity metric is to know where your assets lag. This helps in determining risks along with the improvements that must be taken. This way the vulnerabilities can be worked upon before anyone exploits them.

Mean detection and response time: The sooner a cybersecurity breach is detected and responded to, the lesser will be the loss. It is important to have systems that reduce the mean detection and response time [5].

Data volume over a corporate network: Employees having unrestricted access to the company's internet may turn out into a disaster. If they use the company's resources to download anything, it might lead to the invasion of malware.

Incorrectly configured SSL certificates: Company's digital identity can be used to extract critical information if proper authentication measures are not in place. Thus, it is important to keep track of SSL certificates that are not correctly configured.

Deactivation time of credentials of a former employee: The employees no longer a part of the organization must not be given access to the company's resources. Moreover, their previous rights must be immediately terminated otherwise sensitive information might be put at risk.

The number of users having higher access levels: There are individuals that have a wider range of data access as compared to others. However, this all must be efficiently monitored by the company. Also, unnecessary access should be minimized.

Open communication ports during a time period: Communication occurs both ways. The ports for inbound and outbound traffic must be individually monitored.

Access to systems by third parties: Some systems of a company are more critical to others. For the critical ones, proper mapping of third parties using them should be monitored.

Review of frequency of third-party access: Third parties might have to access the network of a company to complete any project or activity. Thus, monitoring their access is important to identify any suspicious activity that might be undergoing at their end.

Partners with effective cybersecurity: A company may have full control over its cybersecurity policies but you never know if the other business partners are as conscious as you. Thus, the higher the number of partners with strict cybersecurity policies, the lesser the chances of cyberattacks.

Main three reasons that validate the advantage of using metrics: For learning: To Figure out different information pertaining to a system, we have to start by asking questions. These questions will lead us to answers and then in turn to information. This becomes easier with the help of a metric and thus the understanding of cybersecurity risks improves, For Decision Making: When we use a metric to gain information about a system,

we can extend its use even further by gaining insight into previous decisions. This way, we can better manage the decisions that have to be taken with respect to current cybersecurity risks, For Implementation of Plans: After analysing the loopholes in the system and making decisions on how to go about rectifying them, it is time to take action. This implementation can be supported further by referring to previous records and assessments in the cybersecurity metric.

Cyber resiliency metric: Metrics are tools to facilitate decision-making and improve performance and accountability. Metrics are quantifiable, observable, and objective data that supports metrics. Operators can use metrics to apply corrective actions and improve performance. Regulatory, financial and organizational factors drive the need to measure IT security performance. Potential security measures cover a wide range of measurable characteristics, from individual system security audit logs to the number of systems within an organization tested in a year. Effective security measures should be used to identify vulnerabilities, determine trends for better use of security resources, and assess the success or failure of implemented security solutions. Cybersecurity metrics and measures can help organizations (i) verify that their security controls conform to a policy, process, or procedure; (ii) identify their security strengths and weaknesses; and (iii) identify security trends inside and outside the organization's control. By examining trends, an organization can monitor its security performance over time and identify changes that require adjustments in the organization's security posture [5].

At a higher level, these benefits can be combined to help an organization achieve its mission by (i) assessing its compliance with laws and regulations, (ii) improving the performance of its implemented security controls, and (iii) targeting high level goals. Activities. responds to security-related questions that facilitate strategic decision-making at the highest management level of the organization. A few terms then the current state of security metrics, with an emphasis on measuring operational security using existing data collected at the information systems level. This section explains the importance of selecting metrics that support specific metrics, then examines several issues with current practices related to the accuracy, selection, and use of metrics and metrics. The chapter also provides an overview of security metrics research efforts to illustrate the current state of metrics

research and suggests additional research topics. The term metric is often used to refer to performance measurement, but it is clearer to define metrics and measures separately. A metric is a concrete and objective attribute, such as the percentage of systems within an organization that are fully patched, the time between the release of a patch and its installation on a system, or the level of access to a system that might have a security vulnerability in the system.

A metric is an abstract, somewhat subjective attribute, e.g. For example, the level of protection of an organization's systems against external threats or the effectiveness of the organization's incident response team. An analyst can estimate the value of a metric by collecting and analysing sets of metrics, as described below. In the past, many metrics efforts have focused on collecting individual metrics, and little or no thought has been given to how those metrics might be combined into metrics. Ideally, organizations should first select their own metrics and then determine what measures they can take to support those metrics.

An organization should also have multiple levels of measurement, each targeting a specific type of audience. For example, security engineers may be interested in lower-level metrics related to the effectiveness of certain types of security controls, such as: B. Malicious code detection capabilities. Security management can address higher-level metrics related to the organization's security posture, such as: B. The overall effectiveness of the organization's incident prevention and management capabilities.

Lower-level metrics facilitate more tactical decision making, while higher level metrics facilitate more strategic decision making. Lower-level metrics are often used as input data for higher level metrics. Businesses can use ratios and metrics to set goals, also called benchmarks, and use benchmarks to determine success or failure. Suppose an organization finds that 68% of its systems comply with a specific policy. The organization could set a benchmark of 80%, make changes to its practices to improve compliance, and then measure compliance again in six months to see if the benchmark has been met. Benchmarks are organization-specific and are typically based on the baselines of an operating environment. Once an organization has identified its metrics, it needs to determine what actions can be collected to support those metrics. Organizations should favour measures that can be collected by automated means, as they are more likely to be more

accurate than manual collection (e.g., self-assessment surveys) and can also be collected whenever needed. Organizations should also look for opportunities to use existing data sources and automated collection mechanisms due to the costs of implementing and maintaining new systems and software for data collection purposes only. When metrics are collected, organizations need a way to analyse them and generate reports for the metrics they support. Organizations can analyse measures and metrics in many ways, such as grouping them by geographic location, logical organization within the organization, type of system, criticality of the system, and so on. Some organizations use products that aggregate measures into measures and present them in a security dashboard format, where the measures underlying each measure are available through drill-down. This allows a dashboard user to see the values of the metrics presented and the changes in those metrics over time, as well as to review the metrics and measures that comprise those metrics.

Problems with accuracy of metrics: The accuracy of a metric depends on the accuracy of the metrics that comprise it. Organizations are currently facing several problems related to measurement accuracy. One problem is that measurements are often inaccurately defined. Look at the percentage of fully patched systems: Does it only contain patches for the operating system or also patches of services and applications? Does this simply mean that the patches have been installed or that the subsequent actions necessary to activate the patch (such as rebooting the system or changing configuration settings) have also been performed? Another issue with defining metrics is the terminology itself, such as B. measuring the number of port scans performed. What is the minimum number of ports that must be scanned during a port scan? If an attacker scans ports on 100 hosts, is that 1 port scan or 100 port scans? If the attacker performs the same scan but scans only one host per day, it is a port scan or 100 port scans. Port scanning measurement is also a good example of a similar common problem: inconsistent measurement methods. Port scans are often identified by intrusion detection systems (IDS), but each IDS uses its own proprietary algorithms to identify port scans, so activity identified by an IDS as port scanning may not be identified by another IDS be identified as such. This leads to measurement inconsistencies if your company uses multiple IDSs or if only one product is used but the sensors have different port scan settings (e.g., minimum number of ports in a scan or

maximum trace time of an analysis). Another example is system patch status - one operating system may only report operating system patches, while another operating system may also have application patches. In such a case, an organization could use multiple metrics instead of just one, with each metric corresponding to a different measurement method, and then combine the metrics into a single metric that approximates the collective values of the metrics. There have been numerous reports of inaccurate policy-making problems in the security community, but to date there has been no concerted effort to collect, document, and make them available to the security community. Safety. information on these topics. Identifying the factors organizations need to consider when defining their metrics would be much more helpful than trying to provide a unique definition for each metric.

The best definition for an organization is determined by what the organization is trying to achieve. For example, in the patch example mentioned above, an organization might attempt to understand general patch installation and deployment practices to verify that all applications that the organization deems critical have been patched or to verify that organization patches are working fine. Another common problem with measurement accuracy is the use of qualitative measurements.

Data collection methods such as self-report surveys often produce inaccurate or biased results depending on the types of questions asked. For example, if users or administrators are asked if their systems comply with company policies, they likely will. Instead, it would be more accurate to use quantitative measures that assess system compliance. Qualitative measurements without clearly defined scales or units of measurement can be particularly problematic in terms of accuracy. For example, if you ask a user to rate the reliability of their computer on a scale of 1 to 5, where 1 is simply defined as "poor" and 5 as "excellent", this is subjective and inaccurate. A qualitative measure can be useful when each rating is well-defined and there is no overlap between ratings, so that different people with the same information would likely give the same rating. An objective scale might be 5 - no crashes or hangs in six months, 4 - one crash or hang, 3 - two or three occurrences, 2 - four to six occurrences, and 1 - more than six occurrences. However, the rating can be somewhat subjective because it is based on user recall or because "crash" and "hang up" are undefined. However, this qualitative measure is more accurate than poor to

excellent. Some metrics are also considered qualitative because they provide absolute numbers without context, standard, or purpose. For example, an action that claims to have performed 100 attacks has no context. Which 100 point is a lot or a little? A statistic showing that 100 attacks were attempted out of 1,000,000 incoming web server connections adds context. Context is very important for measurements and statistics. Most of the measures individually have little significance. Even the example above (attempts per million incoming web server connections) doesn't make much sense on its own. Is the number of attack attempts increasing, decreasing or stable? Have there been any changes to the organization's security controls that could alter the effectiveness of the attacks, or has the number of attacks really changed? Do the changes in attack attempts match observations of attack trends reported by other organizations? It may be necessary to analyse a single metric along with many other metrics, as well as individual events such as security audit changes and external trends, to determine their true meaning. It would be useful for organizations to collect additional information on the relationships between actions and between actions and individual events, especially when empirical information is included based on analyses of real operating environments. Because computer technology is so dynamic, the meaning of statistics changes over time. Problems with selecting statistics. Most organizations have a number of security measures that are automatically generated by corporate security measures, such as antivirus and antispyware software, intrusion detection systems, firewalls, patch management systems, and vulnerability scanners. Despite the accuracy issues, these measures can be a good starting point for selecting measures to use in an organization. Organizations could also implement additional measures, such as tools to extract information from security logs, but this can be costly and may require the creation of entire systems to collect such measures.

Problem with the use of measures: In addition to issues with measure accuracy and selection, many organizations also face challenges involving the use of measures. Some of these challenges, such as ensuring that the selected measures support the determination of the chosen metrics, have been discussed earlier. Another common challenge is determining how to combine the values of the measures into a metric. The measures may use different units of measurement, have different scales, and have varying precision; these issues can be

addressed through careful creation of equations to combine the values. Also, some of the measures may be more important than others in the scope of the metric. Empirical research in this area could provide organizations with a factual basis for weighting measures instead of either guessing or weighting each measure equally. Organizations need to recognize that over time, they will need to alter their measures and metrics. Although high-level metrics may stay the same, low-level metrics need to change over time as the security posture of the organization changes.

Common vulnerability scoring system (cvss): To better illustrate the current state of research on security metrics, we will examine an ongoing research effort on metrics that indicate the importance of vulnerabilities in systems. The Common Vulnerability Scoring System (CVSS) is a standard for rating the severity of vulnerabilities in operating systems and application software. CVSS consists of three sets of metrics: Base metrics, which are constant over time, Time metrics, which change over time but are the same for all environments, and Environmental metrics, which can be different for each environment. There is a different equation for each set of metrics, and the result of each equation is a score (a base, time, or ambient score) which is essentially a metric. Metrics relate to the specific characteristics of each vulnerability, e.g., B. whether it can be operated remotely (over a network) and to what extent a target's confidentiality, integrity and availability could be compromised. The score metric is intended to provide a general indication of the relative severity of the vulnerability. The first version of the CVSS measurements, equations and metrics was published in 2005. Gaps in the CVSS standard were identified based on feedback from its practical use, particularly expert review of empirical measurements and metric data sets. Measurements, equations, metrics, and related documentation have all been revised to make measurements more consistent and improve the accuracy of metric values. Version 2 of the CVSS standard was released in mid-2007. CVSS is most commonly used by organizations to prioritize their vulnerability mitigation activities, such as applying patches to systems. However, researchers are investigating other uses for CVSS. For example, work has been done at the National Institute of Standards and Technology (NIST) on using CVSS to determine metrics for security-related software configuration settings. Researchers at Veracode are looking at using CVSS to rate software



weaknesses. There is also interest in bringing CVSS scores down from the enterprise level to the individual system level so that CVSS could be used to help assess the overall vulnerability of individual systems. To accomplish this, considerable research and empirical validation are needed for applying CVSS to software configuration settings and weaknesses, as well as a new way of measuring the strength of security controls on individual systems. Stages of cyber resiliency can be visualised as seen in Figure 2.4 [6].

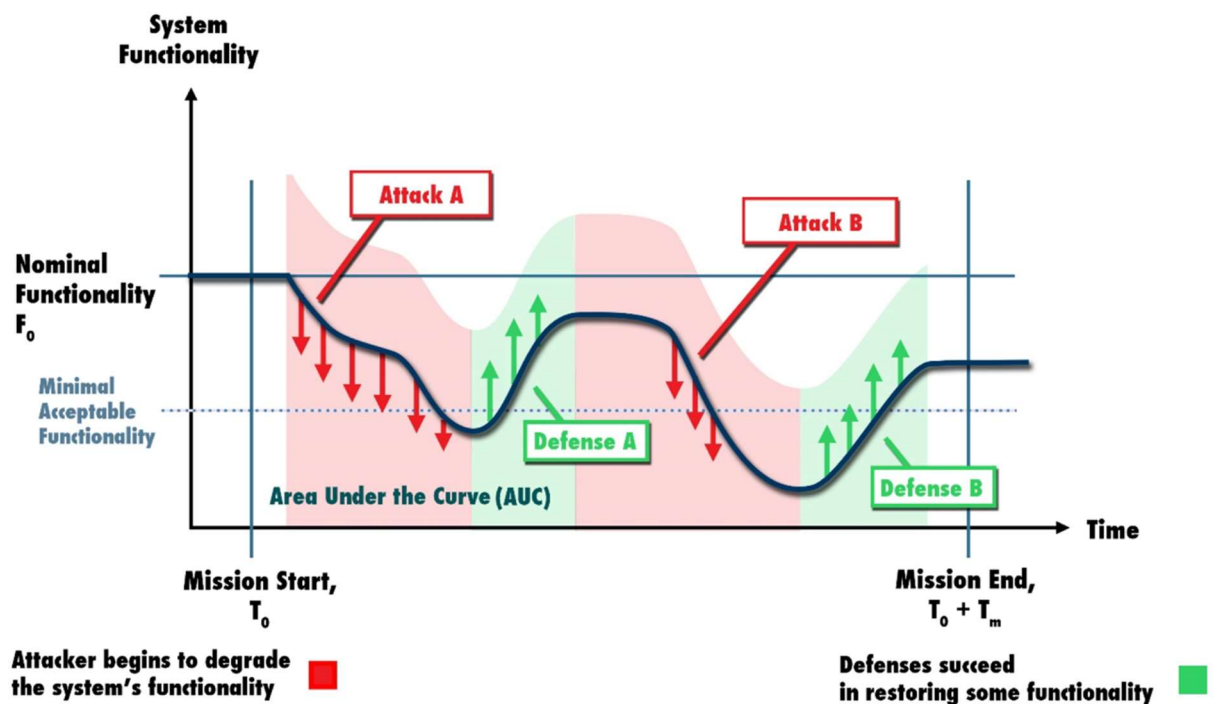


Figure 2.4 – Stages of cyber resiliency

When a cyber incident occurs, specialized organizations such as security operations centres, managed security service providers, incident response providers become agents of resilience. They identify the type of compromise, isolate and mitigate the compromise, use redundant computing resources, wipe affected devices, reinstall software, and restore data from backups. All these steps require significant and costly human skills. Worse still, these processes can take up valuable time, often hours or even weeks. Other situations require much faster reactions, and the resiliency that depends on human rescuers can be prohibitive for certain categories of use cases. Criminals or irresponsible pranksters can take control of

high-speed cars or flying planes, posing a deadly threat to vehicle occupants and others communicating with these systems. In these cases, waiting for a Human Incident Response Team is not enough. On the contrary, such systems require an intelligent autonomous agent on board capable of performing the necessary response and repair actions with response times on the order of seconds or even less. The need for fast superhuman endurance is even more pressing in warfare, especially the highly automated warfare that is likely to define the foreseeable future.

To maintain a significant measure of effectiveness, a missile defence system may only have seconds to react and recover from a cyber compromise. Or consider tactical mobile ground installations in future active ground combat. This could include tanks, combat robots, smart sensors, smart munitions, etc. These means will generally operate in relatively close proximity to enemy forces, which in turn will require relatively easy physical and electromagnetic access with some likelihood of physical capture of people and soldiers by the enemy. In other words, the likelihood of a cyber compromise – severe enough to reduce system functionality below acceptable levels – is relatively high.

Another approach might be a Cyber Operations centre with well-trained Cyber Warriors who would cope with such compromises remotely. However, this can be unlikely to succeed: the battlefield of the long run will see heavily contested networks, intermittent connectivity and therefore the have to minimize radio emissions. Therefore, we cannot depend upon remote recovery. The remaining solution is that resilience must rely upon artificially intelligent agents located aboard battlefield facilities, enabling real-time response and recovery during the mission. Yet accepting even decisions recommended through such systems, including enabling automated response to major trade-offs, requires the power to instil grade of trust related to AI-based interventions to be actionable, which successively requires good measurements and metrics. Let's take a glance at some samples of efforts to extend cyber resilience. The U.S. National Institute of Standards and Technology has published an in-depth catalogue of possible techniques for improving the cyber resilience of systems a number of these techniques are already contributing to the cyber resilience of business products. For example, micro segmentation may be a common approach that improves resilience by slowing down cyber invaders as they try to navigate the system.

Computer deception is a lively topic of educational research. RHIMES may be a research program funded by the Office of Naval Research (ONR) that uses a variety of detection and recovery techniques to safeguard cyber-physical systems against cyberattacks (Pomerleau, 2015). A NATO research group has proposed a reference architecture for an Autonomous Intelligent Cyber Defence Agent (AICA) that resides on a system, continuously assesses adversary activity on the system, and autonomously plans and executes mitigation and recovery actions.

Better resilience calls for measurements: Here by measure (in accordance with the prevailing literature on measures) we mean the quantification, objectively and empirically, of a specific characteristic of a real phenomenon experienced by a system of real (or representative) interest. Measurements should be as empirical and "physical" as possible, even in a cyber world. Some methods and measures are often confused with measurements. For example, great progress has been made in modelling and simulating computer phenomena. But these are not measurements. We perform qualitative assessments and have checklists and metrics for these assessments - suitable and necessary for decision making, but require underlying measurements. We use Red Teams - very important, but again these are not measurements. When looking for possible approaches to measuring cyber resilience, it may be useful to consider a well-developed measurement process in another field, physics: measuring the properties of materials. These measurements (tests) often involve the application of a destructive effort (for example, a cyclic load of some magnitude) applied to a sample of material that performs an abstract form of a useful task (for example, withstanding a large number of bending cycles in case of fatigue property measurement). Such tests can also involve the variation of the load and the quantification of the measure (for example the number of cycles tolerated before destruction) in which the sample can perform its task under load. Exploring this process in materials science can provide insight into possible characteristics of cyber resilience measurement techniques.

First, it is necessary to define an abstract but representative mission of the system and the critical functions necessary to support the mission being measured. Second, find a way to execute a cyber-attack of a certain type (a targeted or random attack) and vary its magnitude (of course, research on how to measure the magnitude of cyber pressure is also

needed). Third, to develop the means by which the system performs its prescribed mission while undergoing cyberloading. Fourth, quantify the extent to which the system can accomplish its mission. For example, the mission time averaging can be a way to quantify resilience. However, research is needed to quantify "functionality" and understand how to account for time-varying computing load and system response. Finally, provide tools and processes that ensure that such experiments, combined with simultaneous modelling and simulation, can be repeated in a consistent and objective way to obtain sufficient evidence for safe decision making. For example, after measuring fatigue strength, engineers can use this measurement to predict if and when a particular part will fail. In somewhat similar fashion, although such analogies are never perfect, cyber resilience measurements help designers or operators estimate a system's suitability (along with its resilience mechanisms) for a given mission [6].

Confidence in measurements and metrics: Unlike precise measurements in physics, the measurement of cyber resilience is still in its infancy. Decisions about translating knowledge and insight into correcting and adapting information systems in response to threats into management decisions and policies will depend on a growing number of increasingly diverse measures. These measurements can be collected in various ways, supplemented with experiments or models, and can indicate different directions regarding the functionality of the system. How can IT professionals make confident decisions about the right course of action given the consistency of multiple individual measures related to system absorption, recovery and adaptation in response to cyber threats? a series of criteria to evaluate the confidence of assuring decision makers the reliability of the methodology used to obtain a meaningful measurement [6].

### 3 CYBER RESILIENCE ASSESSMENT IN INFOCOMMUNICATION SYSTEMS AND NETWORKS

#### 3.1 Cyber resilience assessment breakdown

The AD model can be used to assess the resilience of interdependent CI systems to the worst-case disruptions. Before that, we should carefully define the constraints on  $\mathbf{z}$ , to avoid that the obvious “absolute worst-case” turns out to be that with the simultaneous loss of all system components that leads to complete failure of the systems. A straightforward idea would be to limit the maximum number of lost components by a cardinality constraint, as follows [7]:

$$\sum_{K \in \mathbf{k}} \sum_{I \in L^k} (1 - Z_I^k) \leq B_A \quad (3.1)$$

Where  $B_A$  characterizes the "magnitude" of attack disruption in terms of the maximum number of connections that can simultaneously fail in the attack and where  $\mathbf{z}$  characterizes the failure probabilities of system components, the constraint on  $\mathbf{z}$  allow us avoid the absolute worst case scenario of simultaneous loss. This parameterisation makes sense because it allows to take into account different levels of interference and to evaluate the best possible worst-case functionality of CI systems as a function of the disturbance variable  $B_A$ , thus obtaining the so-called "curve of resilience" ". Additionally, the cardinality constraint can be generalized to any "budget" concept by specifying the costs associated with attacking each component of the system. Additionally, any available information about the attack intent attacker's or disruptor's threat profile for systems, can be carefully formulated in terms of additional constraints on  $\mathbf{z}$  to reduce the space  $\mathbf{z}$ . For example, the impact of a natural hazard such as a hurricane on the components of the CI system is usually probabilistically quantified based on the physical model of the hurricane threat (e.g., wind speed) and the vulnerability models of the system components. The

resulting failure probabilities of system components can be related to their binary damage state variables  $z$  via Shannon information theory.

**Resilience Improvement:** The usefulness of resilience assessment is limited unless it is used to guide the planning for the resilience improvement of interdependent CIs: to build and enhance resilience of the CI systems is the ultimate goal. In the context of the AD model, this means improving the functionality of CI systems under the worst-case simultaneous losses of system components. Nevertheless, doing so will require investment on certain actions, e.g., hardening and upgrading weak system components to increase their chances of survival under disruptions. To quantify this pre-disruption decision.

**Optimization-Based system operation model:** The functioning of modern infrastructural systems is fundamentally guided by the demands placed on their functionality. The system as a whole must "work", i.e., provide services to its users, which are often seen as objectives (for example, to minimize the unsatisfied demand for services) and therefore measured in terms of system functionality. Furthermore, the operation of the CI system is limited as far as is possible, due to physical, economic or regulatory constraints, for example the amount of electrical energy carried by a transmission line cannot exceed its capacity. In this regard, bounded optimization is ideal for modelling this type of decision problem: system administrators make optimal decisions about system behaviour in pursuit of these goals (what we want the system to do), while being subject to its limits (what the system can do). In the constrained operations optimization models of the CI system, possible actions are modelled by decision variables and the solution to a given problem indicates the decisions to be made to optimally reconcile objectives and constraints with respect to the specified objective.

Importantly, this modelling technique is inherently suitable for representing perturbations of CI systems as changes in the input data. For example, the operation of an electricity transmission network can be modelled using linear programming (LP) based on direct circuit representation (DC), taking available generation units, transmission lines and buses and identifying the series of power flows that source unsatisfied demand. If the system loses a transmission line in the event of a failure, we just have to leave the damaged transmission line "out" of the model (for example, using an indicator variable to show the

unusable status) and resume the same business model (or a slightly modified model). I unload. for example, by attributing more weight to the quality of the system service than to the operating costs of the system in the objective function in the event of a disruption); then the solution to this modified problem will indicate the best possible system response. To illustrate, a common network flow-based approach is used here to model the operation of interdependent ICs, where each IC is modelled as a network and their interdependencies are represented through interconnections. Formally, the set of CI of interest is indicated by  $\kappa$ . For CI network  $k \in \kappa$ , its resilience to a disruptive event is regarded as the system functionality level immediately after the event, normalized by the total satisfied demand level

### 3.2 System resilience under disruptions

In practice, CI systems deal with various types of internal / external shocks, such as technical failures, accidents, natural disasters and deliberate attacks. The study of failures in technical systems has produced an extensive literature on system reliability and probabilistic risk analysis. However, the concept of resilience is usually discussed in the context of high impact and low probability events (HILP), i.e., risks that are difficult or even impossible to predict (e.g., due to a lack of statistically evident historical data of the event).; therefore, probabilistic assessment may not be applicable in this case. Furthermore, the probabilities of intentional threats posed by an intelligent and targeted terrorist may not be appropriate for modelling the adversary's behaviour. Brown and Cox show that probabilistic estimation of terrorism risk can even lead to misleading results. Instead of focusing on the source of a disturbance, we look at the problem from the perspective of system functionality. More specifically, we consider disturbances as simultaneous losses of one or more system components and evaluate the performance of ICs in the worst case of disturbances. To identify worst-case breaks, it is assumed that a hypothetical intelligent adversary (an attacker) has perfect knowledge and is able to use limited resources to intentionally damage ICs. From the system operator's point of view, the attacker is not necessarily a real person. Instead, it could be Mother Nature, a terrorist, just plain bad luck, or anything else causing the simultaneous loss of components; Operators strive to maintain the functionality of ICs

as best they can after the loss of these components. We emphasize that the purpose of assuming a custom attacker here is simply to identify worst-case disruptions, not to model the actual behaviour of any given adversary. Formally, damage to IC systems in the event of failure is represented by the state variables of system components, e.g.,  $B_{zlk}$  for trunk  $l \in L_k$  with  $zlk = 0$  if link  $l$  is attacked;  $zlk = 1$  otherwise, as explained in the constraint. It should be noted that we are only considering the failure of network connections here, since the failure of a node in the network corresponds to the simultaneous failure of all the connections connected to it. Then, the impact of disturbances on interdependent CI systems is represented by the following attacker-defender (AD) model [8].

### 3.3 Methods for assessing resilience

#### 3.3.1 Game theory application

In game theory, each "game" consists of two or more rational players whose actions are determined according to any strategy in order to maximize the payoffs they can expect from the game. A "player" can be an individual, but to explore the principles of game theory related to cybersecurity, we can also think of a player as a team or collective of individuals united in their efforts to achieve a common goal. Let's look at an example game where Player 1 is Team Defence, cybersecurity professionals from a legitimate company (Company X) tasked with protecting the organization's information assets, and Player 2 is Team Offense, a corporate crime aimed at destroying the same compromising assets. We can visualize this game with a simple matrix showing Player 1's strategies as rows and Player 2's strategies as columns, as shown in Table 3.1. At the intersection of each player's strategies, payoffs ( $E$ ) are shown with player 1's value on the left and player 2's value on the right:

Each player in our example game has two strategies to choose from. Team Defence must choose whether to implement a security check to protect an information asset (Strategy A) or simply accept the risk of an attack (Strategy B). Team Attack must choose to attack that same resource (Strategy C) or leave it alone (Strategy D). For the purposes of our example game, let's assume that if Team Defence chooses to defend the asset, it will be



successful. Likewise, we assume that an attack by Team Offense on an undefended asset will be successful. Thanks to our knowledge of the players in the game, we can make assumptions about the different types of trade-offs that each player can take into account when choosing their strategy [6].

Table 3.1 – Example of game theory strategy options

		TEAM OFFENSE	
		Strategy C	Strategy D
TEAM DEFENCE	Strategy A	E1, E2	E1, E2
	Strategy B	E1, E2	E1, E2

We can summarize the factors that Team Defence will consider when choosing its strategy as follows:

- value of the asset to the organization;
- building and maintaining consumer trust;
- legal and regulatory compliance;
- resources required for implementation and maintenance.

Similarly, we can summarize some of the factors Team Offense will consider when choosing its strategy:

- value of the asset if compromised;
- resources required to execute an attack;
- specialized skills required to plan and execute an attack;
- importance of keeping their custom-built exploits (TTP) a secret;
- risk of being caught (fines, incarceration, etc.).

While this is an extremely simple example of how cyber war games play out in real life, the logic of how game theory principles can be helpful in making strategic decisions is starting to take shape. Now that we've defined our players and strategies. Table 3.2 lets us start exploring what the pay-outs for each player might look like in our sample game:

Table 3.2 – Possible outcomes of the game

		TEAM OFFENSE	
		Attack	Don't Attack
TEAM DEFENCE	Defend	50, -5	25, 0
	Don't Defend	-100, 25	50, 0

We can use the row and column names of our matrix to refer to each of the possible outcomes of this game. In the game (Defend, Attack), Team Defence chooses to implement a check to protect an information asset and Team Offense chooses to attack it. As a result of these strategies, Team Defence gains 50 points, while Team Offense suffers a loss of -5. Using our summaries of how each player determines the value of possible outcomes, we can see how this result makes sense. Team Offense's defence strategy is beneficial as it prevents these resources from being compromised. Implementing this security control has the added benefit of meeting one or more compliance requirements. The outcome of the game (defence, attack) is less favourable for Team Offense, which spent a significant number of resources trying to attack, but ultimately failed. The game (defending, attacking) is therefore the worst-case scenario for Team Offense. In our example game, the payoffs for the game (defence, not offense) are 25 for team defence and 0 for team offense. In this game, Team Defence again chooses to implement a security check to protect an information asset, but Team Offense chooses not to attack it.

The security review made it difficult for legitimate Company X users to use the resource, but met one or more compliance requirements. For Team Attack, this (defending, not attacking) costs them nothing but earns them nothing. The game (Don't Defend, Attack) is the worst-case scenario for a team's defence. In this game, Team Defence abstains from performing a security check to protect an asset and Team Offense is able to perform a successful cyberattack to compromise it. After this match, the pay-out for Team Defence is -100. Team Attack, on the other hand, exits the game (Don't Defend, Attack) and celebrates its pay-out of 25. Play (Don't Defend, Attack) is the best scenario for a team attack. In the game (Don't Defend, Don't Attack), Team Defence chooses not to perform a security check to defend the asset and Team Offense chooses not to attack it. Team Defence will receive

50 points for saving the time, money and effort required to perform the security check and for not unnecessarily disrupting the normal activities of Company X users. Team Offense leaves with a win of 0 because, once again, it's a game that costs them nothing, but in return they get what they pay for: nothing. As the cyber landscape changes, we can expect pay-outs for cyber war games to be dynamic. The value of information assets will fluctuate as new technologies come to market and existing systems become obsolete. Changes in the economy, political landscape, consumer trends, and legal and regulatory compliance requirements may affect players' calculations of the expected value of playing these games. In order for Team Defence to stay ahead, it must implement a continuous improvement process. An accurate inventory of all information assets, classified according to their value to the organization, is essential to assess the seriousness of the risks to which it is exposed. Applying the principles of game theory, cybersecurity professionals must implement controls that reduce risk to their information assets to acceptable levels while maximizing return on investment [12].

### 3.3.2 Stochastic approach

The comparison between cyberattacks and defence is a complex problem, but given the level of strategy selection, it can be described as a stochastic game problem. Let's take the DDoS attack that exploits the Sadmin vulnerability of the Soloris platform as an example. The attack is performed through multiple steps including IP sweeps, Sadmin ping, Sadmin exploit, installation of DDoS software, and execution of DDoS attacks. Each phase of the attack can lead to a change in the security state of the network as seen in Figure 3.1

Taking the first step as an example, the initial state of the network is indicated with S0 (H1, none). This means that the attacker Alice has no privileges from the H1 host. Next, attacker Alice implemented an IP sweep attack on H1 on open port 445 and gained H1 user privileges. This network state is called S1 (H1, User). After that, if Defender Bob selects and implements a defence strategy from the candidate strategy {Reinstall Listener Program, Install Patches, Close Unused Port}, the network state is reset to S0; otherwise, the network

may continue to evolve into another more dangerous state  $S_3$ . The continuous time axis is divided into time intervals and each time interval contains only one network state [6].

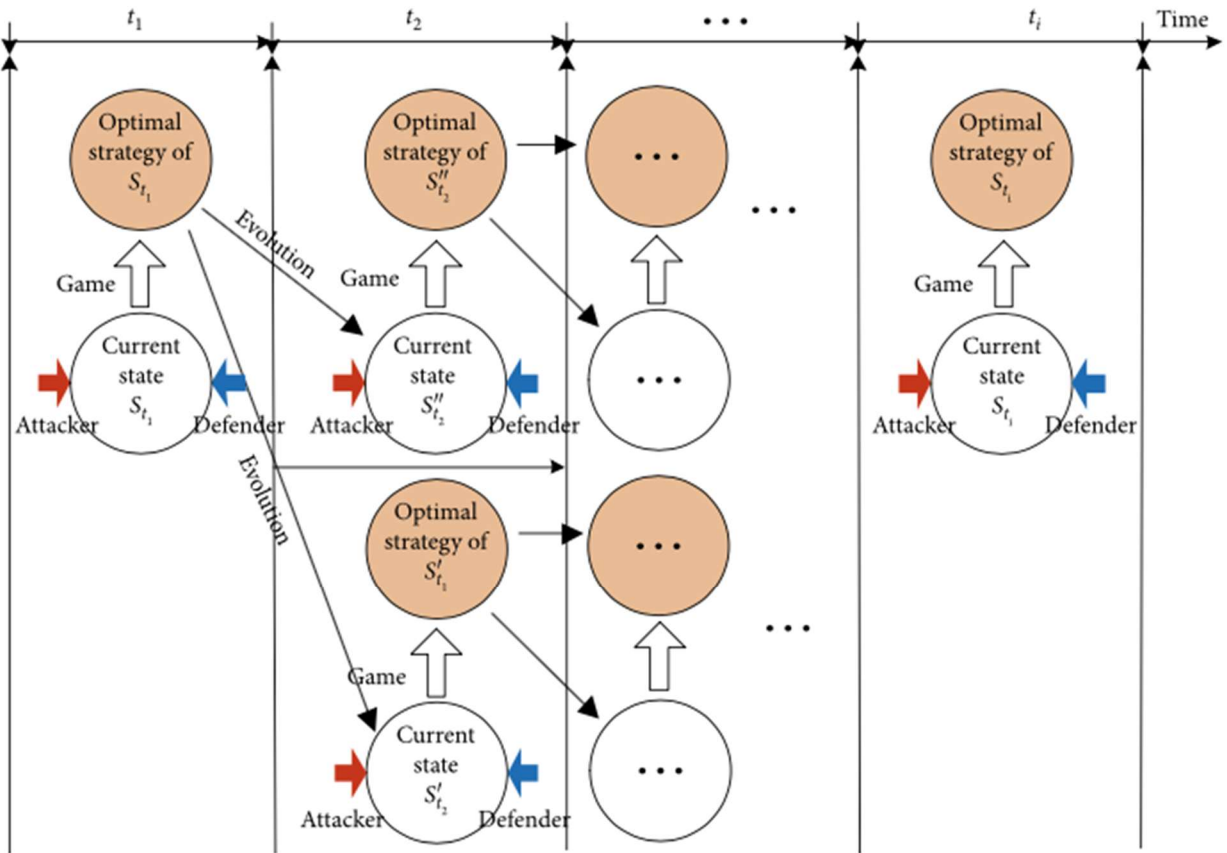


Figure 3.1 – Game process and strategy selection

The state of the network can be the same in different time segments. Each time frame is an offensive defence game. Both sides detect the current state of the network, then select attack defence actions based on strategy and get immediate feedback. Attack defence strategies are tied to network health. The network system switches from one state to another under the candidate action of the attacking side and the defending side. The transition between network states is affected not only by counterattack actions, but also by factors such as the system's operating environment and the incident's external environment.

The purpose of this 59ce59ionn is to enable defenders to achieve higher long-term advantages in the stochastic attack-defence game. Both sides of the defence can predict the existence of a Nash equilibrium, so the Nash equilibrium is the best strategy for both sides.

From the description of total rationality in the introduction, we can see that the requirement of total rationality for both attacker-defender sides is too strict, and both attacker and defender sides are constrained in practice by bounded rationality. Bounded rationality means that at least one of the attacking and defensive teams will not use a Nash equilibrium strategy at the start of the game, which means that it is difficult for both sides to find the optimal strategy at the start of the game. Game and they constantly customize and adjust the strategy to improve their opponents. This means that the balance of the game is not the result of choice, but the two sides of the attack-defence side are constantly learning to achieve during the attack-defence confrontation, because the influence of the learning mechanism can also then deviate again when equilibrium is reached. From the above analysis, we can see that the learning mechanism is the key to winning the game of bounded rationality. For the defence decision-making process, the learning mechanism of the attack-defence stochastic game under conditions of bounded rationality must satisfy the following two requirements:

1. Convergence of the learning algorithm: the strategy of the attacker in conditions of bounded rationality has characteristics of dynamic change and due to the interdependence of the attack-defensive strategy, the defender must use the corresponding optimal strategy learned in the face of different attack strategies to ensure that he is invincible.

2. The learning process does not need too much information about the attacker: both sides of the cyber-attack defence have objective opposition and non-cooperation, and both sides will intentionally hide their most important information. If too much opponent information is needed in the learning process, the practicality of the learning algorithm will be reduced.

The WoLF PHC algorithm is a typical smart strategy gradient learning approach that allows defenders to learn through network feedback without sharing too much information with attackers. The introduction of the WoLF mechanism ensures the convergence of the WoLF PHC algorithm. Once the attacker has learned to adopt the Nash equilibrium strategy, the WoLF mechanism allows the defender to approach the corresponding Nash equilibrium strategy while the attacker has not yet learned the Nash equilibrium, and the WoLF mechanism allows defenders to approach the appropriate optimal defence strategy. The

relationship and similarities between the cyber-attack defence model and the stochastic game model is seen in Figure 3.2 [14]

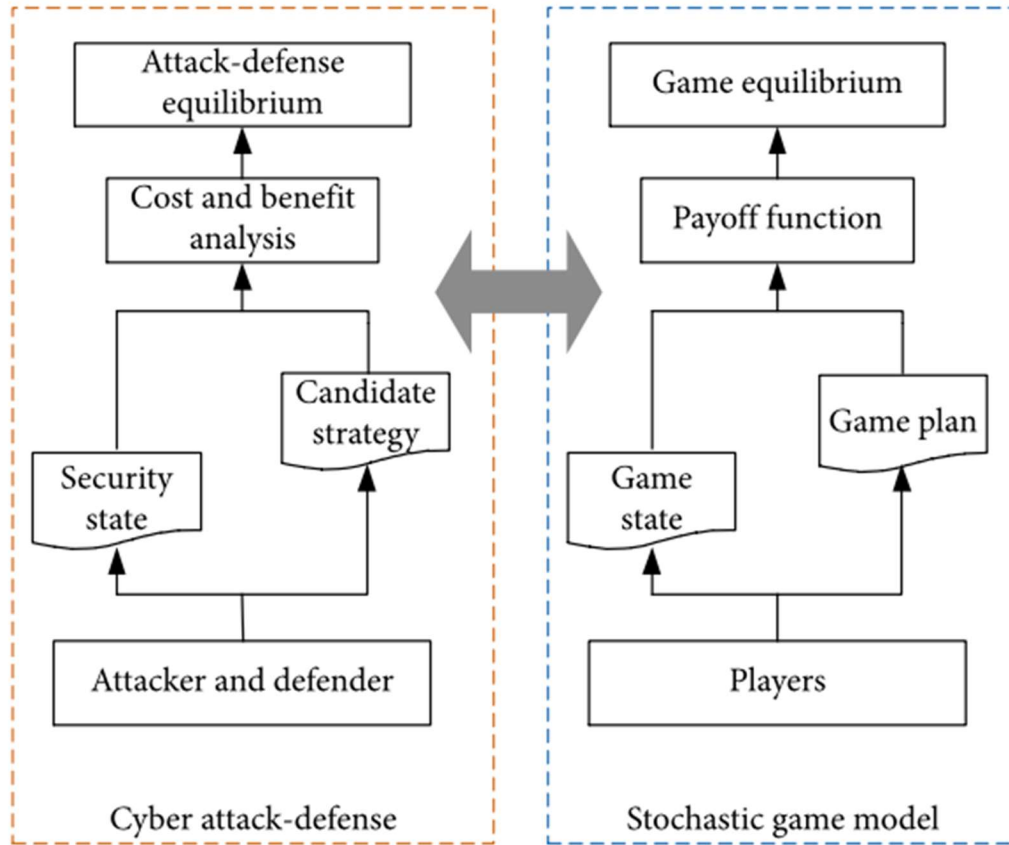


Figure 3.2 – Relationship between cyber-attack-defence and stochastic game model

The protection status in this case corresponds to S0 (H1, None) and S1 (H1, User). The possible strategy against DDoS attacks is {Reinstall Listener Program, Install Patch, Close Unused Port}. The state of the network is common knowledge of both parties. Due to the non-cooperation between the attacking and defending parties, the two parties can observe each other's actions only through the detection network, which will slow down the execution time for at least an interval of time, so the attacking-defence parties take action at the same time in each time interval. The "simultaneous" here is a concept of information rather than a concept of time; that is, the choice of attack-defence factions should not be based on the concept of time. At the same time, since the attacking-defending sides do not

know the choice of the other side when choosing the action, they are considered to be simultaneous actions.

Stochastic Game Analysis and Strategy Selection: Cyber-attack-defence is described as a bounded rational stochastic game problem, and an attack- defence stochastic game model AD-SGM is constructed. In this section, reinforcement learning mechanism is introduced into finite rational stochastic game, and WoLF- PHC algorithm is used to select defence strategies based on AD-SGM.

Principle of WoLF-PHC: Q-learning algorithm – is the basis of WoLF-PHC algorithm and a typical model-free reinforcement learning algorithm. Agent in Q-learning obtains knowledge of return and environment state transfer through interaction with environment. Knowledge is expressed by payoff  $Q_d$  and learned by updating  $Q_d$ .  $Q_d$  is:

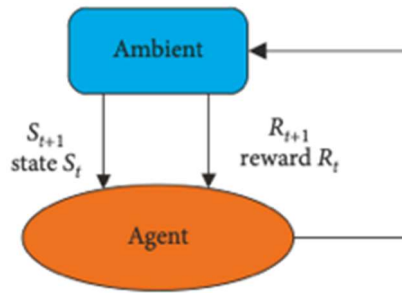
$$Q_d(s, d) = Q_d(s, d) + \alpha \left[ R_d(s, d, s') + \gamma \max_{d'} Q_d(s', d') - Q_d(s, d) \right] \quad (3.2)$$

Where  $\alpha$  is payoff learning rate and  $Q_d$  is updated with new information gotten over time as the attacker makes attempts to penetrate the system. This new information is called a discount factor and is classified as  $c$  in  $\alpha[c]$  in reference to (3.2) and consists of components such as defence of current and changing state.

### 3.3.3 Decision making algorithm

The general process of the decision-making approach can be broken into ordered and specific steps that help decide how to defend an attack, this can be seen in Figure 3.3.

All these pieces of evidence come from real-time intrusion detection systems. After decision making, the optimal security strategy is determined against detected intrusions. In order to improve the learning speed of WoLF-PHC algorithm and reduce the dependence of the algorithm on the amount of data, the eligibility trace is introduced to improve WoLF-PHC.



Q-learning mechanism

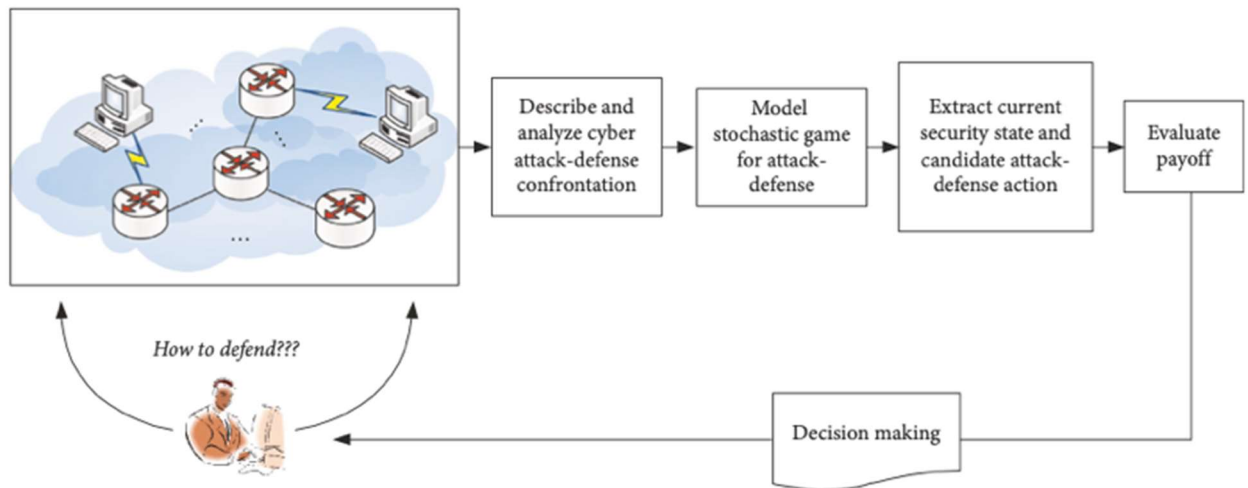


Figure 3.3 – process of decision-making approach

The eligibility trace can track specific state-action trajectories of recent visits and then assign current returns to the state-action of recent visits. WoLF- PHC algorithm is an extension of Q-learning algorithm. At present, there are many algorithms combining Q-learning with eligibility trace. WoLF-PHC algorithm is an extension of Q-learning algorithm, which belongs to off-policy algorithm. It uses greedy policy when evaluating defence actions for each network state and occasionally introduces nongreedy policy when choosing to perform defence actions in order to learn. In order to maintain the off-policy characteristics of WoLF- PHC algorithm



### 3.6 Experimental analysis

In order to verify the effectiveness of this approach, a typical enterprise network is built for experiment. Attacks and defences occur on the intranet, with attackers coming from the extranet. As a defender, network administrator is responsible for the security of intranet. Due to the setting of Firewall 1 and Firewall 2, legal users of the external network can only access the web server, which can access the database server, FTP server, and e-mail server as seen in Figure 3.4.

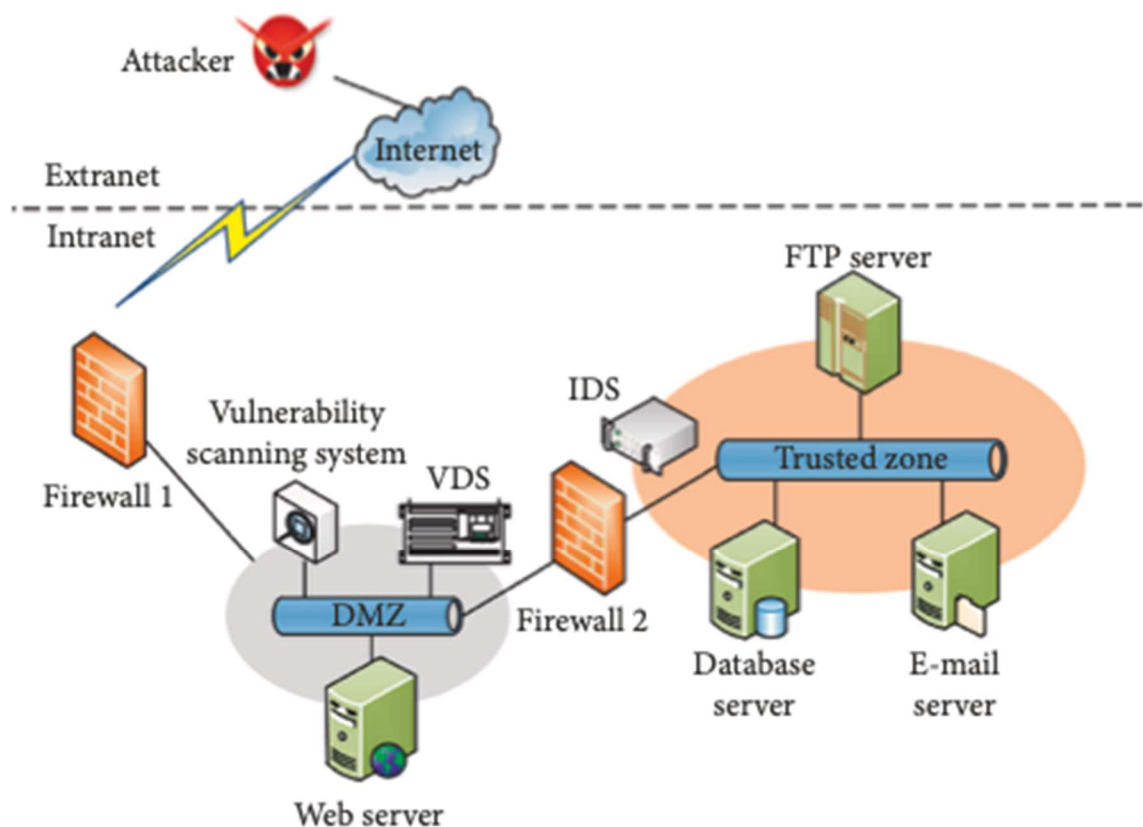


Figure 3.4 – Network topology for experiment

The network vulnerability information is viewable and displays information on the attacker, host and the target privilege amongst other things, as seen in Table 3.3

Table 3.3 – Network vulnerability information

Attack Identifier	Host	CVE	Target privilege
Tid <sub>1</sub>	Web server	CVE-2015-1635	User
Tid <sub>2</sub>	Web server	CVE-2017-7269	Root
Tid <sub>3</sub>	Web server	CVE-2014-8517	Root
Tid <sub>4</sub>	FTP server	CVE-2014-3556	Root
Tid <sub>5</sub>	E-mail server	CVE-2014-4877	Root
Tid <sub>6</sub>	Database server	CVE-2013-4730	User
Tid <sub>7</sub>	Database server	CVE-2016-6662	Root

Figure 3.5 graphically visualises the mode of attack by each attacker identifier

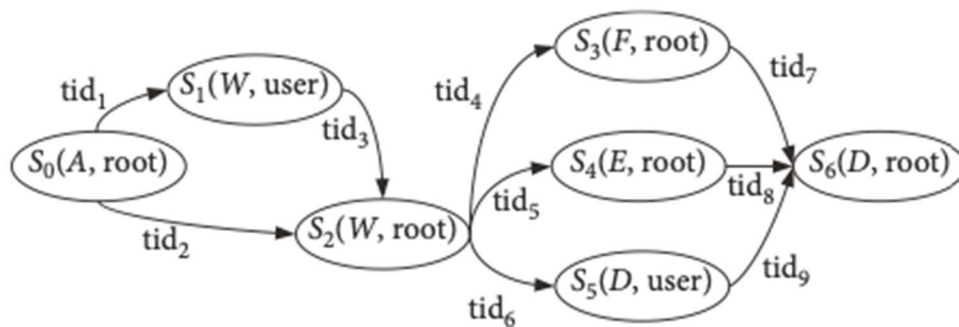


Figure 3.5 – Attack graph

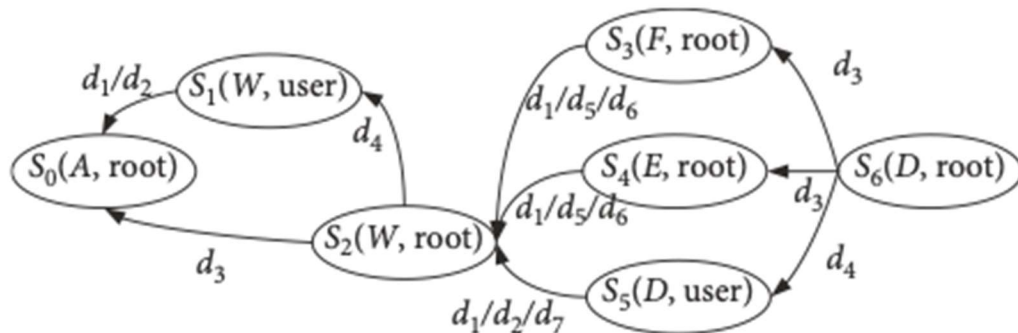


Figure 3.6 – Defence graph

Table 3.4 entails information on defensive action for each defence identifier according to the atomic defence action presented

Table 3.4 – Network Vulnerability Information

Atomic defence action	D <sub>1</sub>	D <sub>2</sub>	D <sub>3</sub>	D <sub>4</sub>	D <sub>5</sub>	D <sub>6</sub>	D <sub>7</sub>
Renew root data	-		-		-	-	
Limit SYN packets		-					
Install oracle patches	-						-
Reinstall listener program	-				-		
Uninstall delete trojan		-				-	
Limit access to MDSYS		-		-			
Restart database server			-	-	-		
Delete suspicious account		-					-
Add physical resource	-			-	-	-	
Repair database			-	-			-
Limit packets from ports	-	-	-			-	

### 3.6 Conclusive statements

The comparison between cyber-attack and defence is abstracted as a stochastic game problem under the constraint of bounded rationality. A host-canted attack defence graph model is proposed to extract the network state and attack defence action, and an algorithm to generate an attack defence graph is designed to effectively compress the game state space. To solve this problem, the defensive decision-making approach based on WoLF-PHC is proposed, which allows defenders with limited rationality to make optimal decisions in front of different attackers. The grid improves the WoLF PHC algorithm, accelerates the learning speed of the defenders and reduces the dependency of the algorithm on data.

### 3.6 Risk mitigation and control for organizations

Technical checks: The selection of specific controls is highly dependent on the circumstances of an individual company. A specification of all possible cybersecurity controls, or the recommendation of a specific method of selecting controls, is beyond the scope of this document. However, given the recent cybersecurity events that have affected companies, it is useful to highlight a general approach to cybersecurity controls that companies have found effective, as well as some critical and illustrative cybersecurity practices.

Defence in depth: Many organizations use a defence-in-depth strategy. As part of such a strategy, organizations strategically overlay several independent security controls on their IT systems. A successful defence-in-depth strategy relies on the selection and effective implementation of cybersecurity practices and controls that match an organization's risk profile. Defence-in-depth strategies are promoted by organizations such as the National Security Agency. Organizations can conceptualize defence in depth from a variety of perspectives that are not mutually exclusive. For example, one perspective is to view the components of an organization's technical infrastructure in layers, and then apply security checkpoints to each layer. A basic decomposition might consider the technical environment as having the following layers: applications, perimeter, servers, databases, and the data itself.

The Cyber Kill Chain (reconnaissance, armament, delivery, exploitation, installation, command and control, and actions on targets) – or similar models – offer a different perspective for conceptualizing a defence in depth strategy. By looking at the defence-in-depth challenge from multiple angles, such as those described above, organizations can better understand the controls that can maximize the effectiveness of the strategy. The list of candidate controls can be long. These practices are listed and categorized in various ways by standards such as ISO 27002 and NIST SP 800-53, and by industry organizations such as SANS. The recently released NIST framework also provides helpful guidance for selecting controls that match an organization's risk appetite. The success of a defence-in-depth strategy depends on both the organization's overall control architecture

and the effectiveness of the individual controls deployed. With the increasingly sophisticated nature of cybersecurity threats, organizations must continually identify and remediate potential vulnerabilities in both areas. For example, some attacks may involve custom malware that traditional antivirus programs cannot detect. Other attacks can hijack an application or process beyond detection by traditional security measures. Participation in information-sharing organizations can help companies become aware of potential new threats to their systems, learn how other companies are dealing with these threats, and discuss general cybersecurity approaches.

**Identity and Access Management (IAM)** Establishing appropriate controls to limit user access to an organization's systems and data – identity and access management – is one of the key challenges faced by system operators. This challenge involves many aspects, including how to set it up, restrict it appropriately, and terminate access when no longer needed. This applies to external parties – customers and suppliers – and internal parties. The increasing use of mobile devices by customers and employees contributes to this challenge – by creating several new devices whose access to the system must be carefully managed. Additionally, internal issues can arise when user-facing applications are granted excessive privileges on back-end systems such as databases. Controls that restrict access of a user-facing system to a back-end system provide an additional layer of control behind other controls that can be implemented in the user-facing application. These backend system credentials must also follow a least privilege policy.

This is an example of defence in depth. In the event that an insider finds a vulnerability in a user-facing system, applying a least-privilege policy to this back-end system account will reduce the impact. As a specific example, if a user-facing application has no requirements regarding sensitive fields in a database table, the backend system account should be explicitly denied access to those fields. Three key principles should underpin the policies, processes and technical measures that together ensure effective access controls throughout a user's lifecycle: least privilege policy, separation of duties and transparency of rights.

**Authorization scheme:** If permissions are allowed to be granted in a distributed manner, other controls, such as enforcing segregation of duties or monitoring and

terminating unnecessary permissions, will become much more complex and costly. Authorization responsibilities can be delegated; However, the underlying rights system must be centrally organized and controlled. When permissions for operating systems, applications, databases, or utilities are granted independently, it is extremely difficult to maintain a complete inventory of possible permission sources and therefore extremely difficult to confirm that all granted permissions are checked. Organizations should consider maximizing the use of role-based authorizations in their authorization systems. Access requirements for employees are generally tied to their role in the organization. Additional rights can also be applied based on specific project assignments, but where possible basing the rights on a person's characteristics pays off in terms of ensuring consistency across the board. 'Internal organization, minimizing the opportunities to acquire rights as people move between roles and departments and drastically simplify the tasks of designing and maintaining proper separation of duties. Businesses must review the business justification for any rights granted, and the requirements for accessing sensitive information must be challenged. Business necessity rather than convenience should guide access to sensitive data and systems. Before granting access to such data or systems, enterprises should consider whether a change to an underlying business process would enable the business goal to be achieved without exposing sensitive data to that role. Businesses should compartmentalize sensitive data and processes as much as possible. The wider the access of a single role, the greater the negative impact on the company in case of misuse or abuse of the access of that role (by accident, malicious intent by the right holder or theft of credentials from part of another insider). Again, companies should consider whether adapting an underlying business process can contribute to better compartmentalization. Businesses must ensure that for every role with access to sensitive data, there is at least one other control that prevents (or at least detects) abuse or abuse of that right. Claims relating to that other control cannot be attributed to the previous control. For example, permissions to start, stop, or modify logs should not be granted to a role that also uses those logs as a means of monitoring the actions of members of that role.

Using monitoring: Businesses should introduce controls to detect violations of sensitive rights. For example, there may be nothing unusual in having a member of a

function with appropriate privileges access a client's sensitive data; however, it may be unusual for a member with that role to access 10,000 customer records within a one-hour period. Companies should seek to establish business rules that distinguish between normal and abnormal use of sensitive rights and to create controls to quickly detect and investigate abnormal behaviour.

**Maintenance of Rights / Access Revisions:** Businesses need to establish triggers for entitlement updates. For example, it might be possible to set up a human resources process that reminds managers to review rights in the event that a person's title or department changes. In a more advanced model, the entitlement would be automatically updated based on the permissions schedule. Regardless of the degree of automation, it is imperative that companies conduct regular access assessments and that these assessments are thorough. It is not enough to ask the managers to carry out this assessment. There should be a mechanism to provide the reviewer with an inventory of roles a user is assigned to (or an inventory of specific permissions if role-based permissions are not used). The reviewer should then be prompted to explicitly indicate whether a role assignment or permission should be retained or terminated. Releases marked for completion should be tracked to completion. It may also be advisable to review these access reviews, perhaps through spot checks, to confirm that the access review process is effective.

**Revoke access:** Organizations should put mechanisms in place to immediately terminate employee access to systems and information they no longer need to access. Where automation is not available, policies and procedures related to permissions management and access review should be in place to ensure that role assignments and permissions identified as no longer required are terminated in a timely manner. In the event that a user account is fully terminated, some companies implement two levels of access termination for departing employees: end-of-day termination for departing employees in good standing and immediate termination for departing employees for a valid reason.

**Cryptography:** Cryptography is an extremely important practice in a company's cybersecurity audit arsenal. Encryption has the distinct advantage of protecting data confidentiality by ensuring that only approved users (users who have the decryption key) can view the data. Less obvious benefits include providing a means of ensuring information

integrity (if the encrypted data cannot be read, it cannot be significantly changed) and irrefutability (if a message is encrypted with a key held only by that source cannot renounce the source of having sent it Message). Depending on how it is applied, encryption can also be used to enable a strong separation of duties policy by limiting access to keys to employees with a company-defined need to access protected information. In some ways, cryptography can be seen as the last line of defence in a defence-in-depth strategy. Encryption is a control applied to the data itself. When all higher-level checks fail and data is exposed, encryption can protect that data from being read or modified. While encryption is ultimately a control applied to data, control can be implemented at multiple layers of a defence-in-depth strategy, with different security benefits and operational trade-offs at each layer. The application of encryption should be considered on both workstations and servers, at rest and in transit, and at different technology layers, from storage media to the application layer.

**Data at rest (data saved)** Data is stored in many locations within an organization, including file servers, workstations, and portable media such as USB sticks. An effective practice is to encrypt this inactive data. Enterprises need to have a strategy in place to ensure that portable media, including but not limited to USB drives, backup tapes, and end-user portable terminal drives such as laptops, are encrypted. There are many examples of organizations losing sensitive data due to the loss of portable media and computing devices. It is a widely accepted best practice that these devices should be encrypted, as they present a much higher risk of loss and theft than fixed storage media in offices and data centres. Additionally, organizations must encrypt data stored in formal systems. To this end, organizations should consider the options and relative advantages of applying encryption at different levels of the organization's technology systems. Placing sensitive data in a cloud service carries the same risks as data stored in private systems, and organizations must deal with the risk of disclosure to insiders of the cloud service provider. A guiding principle is to encrypt all sensitive data before it is placed in the cloud, using encryption that the business controls and is never shared with the cloud service provider. Any decision to deviate from this guiding principle should be based on a thorough third-party risk analysis of the cloud service provider and informed acknowledgment of the risks by relevant stakeholders.



Third-party Penetration Testing: Penetration Testing (also known as “Pen Testing”) is an effective practice that simulates a real- world attack against a firm’s computer systems. The goal of a third-party penetration test is to get an attacker’s perspective on security weaknesses that a firm’s technology systems may exhibit.

Penetration tests are valuable for several reasons:

- determining the feasibility of a particular set of attack vectors;
- identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence;
- identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software;
- assessing the magnitude of potential business and operational impacts of successful attacks;
- testing the ability of network defenders to successfully detect and respond to the attack; and providing evidence to support increased investments in security personnel and technology.

Penetration Tests can take different forms depending on a firm’s specific objectives for the test. Each of these contributes in its own way to an overall defence-in-depth strategy.

Broad vs. Targeted: Penetration testing may be scoped to encompass all accessible systems, or may be scoped to target a specific system or application. In the former case, it is common to provide the tester with little more than a range of IP addresses. In the latter case, URLs and an appropriate set of application credentials may be provided, along with guidance on how to exercise the functionality of the application. There are cost and risk trade-offs to be made in balancing the depth and breadth of the work.

Find vs. Exploit: Testing can be limited to finding apparent vulnerabilities, or can include the demonstrated exploitation of vulnerabilities to achieve a particular security objective (e.g., obtain sensitive data). The additional work and expense of demonstrated exploitation testing may uncover compensating controls that mitigate the risk of the detected vulnerability. It may also provide hard evidence necessary to justify remediation costs of the identified vulnerability.

Production vs. Non-production: Testing against production systems is ideal from a security perspective as it leaves no question as to whether production controls are consistent with an alternate testing environment. As even testing designed to be non-destructive can potentially alter the state of a production environment, it may be necessary to perform testing with the system offline and to provide a facility for capturing the production state prior to the test and restoring after the test.

External vs. Internal: External penetration testing is designed to test a firm's systems as they are exposed to the outside world (typically via the Internet) while internal penetration testing is designed to test a firm's systems' resilience to the insider threat. An advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform penetration testing against both external and internal interfaces and systems [2].

## 4 QUANTITATIVE MEASURES OF CYBER RESILIENCE

### 4.1 Factors of network resilience

The computer network is a system in which several subsystems with independent functions are interconnected through communication links; these connections are managed by a network operating system and a software protocol to perform data communication and sharing of network resources. Multiple subsystems with independent functions can be abstracted as network nodes with different capacities. For example, the intrusion detection system can be considered an observation node and the controller cluster can be considered a monitoring node. In addition, a data centre has strong decision-making power, and huge network terminals are equipped with special action options. By analysing the functional properties of real network entities, inspired by the "OODA" cycle, we define four types of variable capacity of network nodes, including observation, control, decision and action. Also, it allows adjustable bandwidth and delay for network connections, which are also tied to the actual network system. These dynamic properties mentioned above are the basic rationale for evaluating network resilience and also constitute the internal perspective of network resilience. Referring to numerous quantitative studies in the literature, this section considers both the internal and external perspective of the network system. Precisely because of the specific functions of network internals, network resilience performance can be determined from an external perspective, including readiness, resistance, adaptation, recovery, and evolution.

The capabilities of the above four nodes and the capabilities of the two edges will have a significant impact on the network resiliency resulting from the proposed framework. Once the network system is attacked, dynamic and intelligent optimization of these basic capabilities can help achieve network resilience. Our starting point for the proposed framework is a computer network system in the cyber-attack environment. If researchers want to apply the evaluation model to real grids such as smart grids and transport grids, they must first create an appropriate capacity map for the nodes. For example, in an intelligent network, the intruder detection device is a node with observation capability; the safety

release device is a useful button; the IT platform is a decision-making node; The control room is a node with control options. And these capabilities can also be adapted over time to meet the real-time needs of the network system.

Measurement of 5 core capabilities: Basic Networking Attributes: The mathematical model for the network resilience evaluation concerns a basic network  $G(N, E)$ , which comprises a set of nodes  $N$  connected by a set of edges or arcs  $E$ . The relationship between nodes and edges in a network can be visually described by graph. Several graph spectral matrices, such as algebraic connectivity, natural connectivity, and flow robustness, are generally employed to measure the robustness and resilience of network in generally. The graph's topology  $G(N, E)$  can be represented by adjacency matrix and Laplacian matrix. Let  $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$  represent the eigenvalues list of the Laplacian matrix. And all the variables defined for network will be normalized to value in the interval  $[0,1]$  when calculating following equations [6].

Flow robustness, denoted as  $FR(G)$ , is a graph metric that measures the ratio of the number of available flows to the number of total flows in the network. A flow is considered available if at least one of its paths remains reachable after link or node failures. The number of total flows represents the maximum of network flows. For example, a connected network with  $|N|$  nodes have  $|N|(|N|-1)/2$  flows between all node pairs. The range of flow robustness values is between 0 and 1, where 1 means that the graph is a completely connected graph, and 0 indicates that the nodes cannot communicate with each other in the whole network. Let  $\{C_i; 1 < i < k\}$  be the set of connected sub-graph in given network  $G(N, E)$ , and the  $C_i$  of a network can be calculated by union-find set within linear time complexity. The union-find set is a tree- shaped merging and searching data structure, which can solve the problem of a disjointed search with constant-level time and space consumption. It will not consume too much computing resources when calculating the connected subgraph even in large-scale network.

Where the effective graph resistance, denoted as  $R(G)$  and nodes denoted as  $N$ , is a graph metric that measures the network's resistance against nodes or edges destroyed. The

normalized  $R(G)$  is calculated as Equation (4.1), where  $\lambda_i$  is the non-zero eigenvalue of the given graph's Laplacian matrix  $L$ , where the values of  $R(G)^*$  lie in the interval  $[0, 1]$ .

$$R(G)^* = \frac{|N|-1}{|N| \sum_{i=2}^N \frac{1}{\lambda_i}} \quad (4.1)$$

Where the effective graph resistance, denoted as  $R(G)$  and nodes denoted as  $N$ . Besides the measurement of graph spectral matrices, the time-varying attributes of network elements are also crucial factors on modelling core capability of network resilience. With the development of the Software Defined Network (SDN) and Network Function Virtualization (NFV) technologies, the network become more dynamically reconfigurable and programmable. Moreover, network delay and bandwidth can be uniformly scheduled by routers with programmable kernel to achieve the network's modifiability and controllability. As described in section II-C, different network sub-systems and elements equip different networking capacities, which can be more convenient with a wide deployment of SDN and NFV, and the capacities of network elements can be dynamically adjusted over time according to the needs of application scenarios. In order to reflect the dynamic characteristics of network elements in the process of measuring network resilience, we simplify and refine the key time-varying capacities of nodes and edges in this paper. The nodes in the network will be equipped with four kinds of capacities, including observation capacity, control capacity, decision capacity and action capacity, which can be adjusted over time, and the summation is within a certain range, considering that the resource and computing power of nodes are limited in real network. We define the maximum of the total four capacities of each node as MAI. Meanwhile, the edges' capacities in network will be measured by the maximum bandwidth, real-time bandwidth and RTT latency, which are established on the adjacency matrix of network. Define  $\text{MaxBw} = (\text{M Bw}(t)_{ij})_{N \times N}$  as the maximum bandwidth matrix, and  $\text{Bw} = (\text{Bw}(t)_{ij})_{N \times N}$  as the real-time bandwidth matrix, and  $\text{Rtt} = (\text{Rtt}(t)_{ij})_{N \times N}$  as the RTT latency matrix.

Meanwhile, a complete network resilient process should go through the following stages: preparing, resisting, adapting, recovering, and evolving. There are subtle differences between the above two perspectives. The former refers to resilience as a type of overall network capability, similar to CIA principles in information security system. The latter perspective, however, considers resilience as a manifestation or performance of network during operation process. Fundamentally, this is the network's resilient capability that results in resilience performance. Therefore, five core capabilities of resilience will be defined and modelled to describe the resilience capability more specifically as follows.

It should be noted that network resilience is established on time-varying dimensions; therefore, the following five capabilities are transient capabilities, which can vary in values over time.

1. **Rapid Response Capability:** The rapid response capability (RRC) is defined as the system's response speed and emergency capability against disturbance or cyber-attacks. The system can take emergency rescue and recovery measures in earlier times when it has better rapid response capability. This capability is related to the perceptual or observing ability of network components (nodes) and the transmission ability of network links. We combine the abilities of nodes and links with graph theory. In a definite scale network, the node with larger observing ability and more connected edges will have more observation capability, and the link with more bandwidth and less transmission delay will have more rapid response capability. Therefore, the network nodes' observing ability is defined as the product of observation ability and degree distribution of network nodes. The links' transmission ability can be determined by the ratio of edges' betweenness centrality and the RTT delay between node pairs.

2. **Sustained Resistance Capability:** The sustained resistance capability (SRC) is defined as the system's ability to prevent a rapid decline in network performance, which is related to the resources' redundancy, the network topology's robustness, the regional network's autonomous intelligent management, and how to prevent the cascading failures' propagation. The SRC capability can directly affect the resistance duration and the network performance's minimum limit. The numerator considers the average effective graph resistance from a graph theory point of view, and the denominator represents the harm

caused by the destruction of network elements, which is contributed by the criticality and disruption likelihood of nodes and edges together.

$R(G)^*$  is the effective graph resistance of network  $G(N, E)$ , and  $Deg_i$  is the degree of node  $i$ ,  $L_i$  and  $L_{ij}$  are the disruption likelihood of node  $i$  and edge  $(i, j)$ , respectively.  $I_i$  and  $I_{ij}$  are the criticality of node  $i$  and edge  $(i, j)$  to network, respectively. Among them, the  $I_i$  is calculated as the product of node's betweenness and the sum of node's observation and action ability, and the  $I_{ij}$  is calculated as the product of edge's betweenness and the sum of two side node's network criticality

3. Continuous Running Capability: The continuous running capability (CRC) is defined as the system's ability for ensuring the continuous operation of the network service during low efficiency phase. The network can reduce service performance to provide less quality of service while ensuring current network security. If some forwarding nodes on the shortest path fail, the transmission task can still be completed by rerouting, despite increasing the link transmission delay. The CRC is determined by the network's flow robustness, real-time bandwidth, and edges' criticality. It can be clearly analysed that the network can make more rerouting decision with larger  $FR(G)$ , and the critical edge should be equipped with larger real-time bandwidth.

4. Rapid Convergence Capability: The rapid convergence capability (RCC) is defined as the capability to ensure the network's rapid convergence and restoration in the recovery stage, including network status monitoring, recovery strategy deployment, etc., which involve the adjustment of node control ability, decision ability and action ability. The purpose of constructing rapid convergence ability is to speed the recovery rate and reduce the recovery-stage time. The RCC is determined by repair rate of node and edge, the node's control, decision and action ability, the edge's real-time bandwidth and RTT delay. In the recovery stage, the nodes with strong control and decision abilities will have more positive impact on the network through control path, which result in the  $C_i$  and  $D_i$  are weighted by betweenness  $BN_i$ . The node's action ability will directly affect its connected nodes, so the  $A_i$  is weighted by node degree  $Deg_i$ . By contrast, the edge's influence on RCC can be better understood that the edge with larger betweenness  $BE_{ij}$ , larger real-time bandwidth  $Bw_{ij}$  and

less transmission delay  $R_{ttij}$  will make more positive effect on RCC. It should be noted that all variables are normalized to value in the interval  $[0,1]$ , therefore the calculation of equation can make sense.

5. Dynamic Evolution Capability: The dynamic evolution capability (DEC) is defined as the system's capability to continue to evolve and regenerate after recovering for historical destruction and recovery measures. This ability will directly depend on the network's structural entropy and the network components' maximum capability. Network with high dynamic evolution capability will be more resistant against similar destruction in the future. The network with larger structural entropy will have greater structural stability for network's dynamic evolution. Moreover, the adjustment of various abilities of nodes is within the range of the maximum resource of each node  $MAI_i$ . And the maximum of edge's bandwidth  $MB_{wij}$  is also the key factor of dynamic evolution capability. In this paper, the DEC is calculated as the product of the network's structural entropy, the maximum of the node's abilities and the maximum of the edge's bandwidth

#### 4.2 Resilience evaluation model based on DBN

It is necessary to establish an evaluation model appropriate to the network resilience process that varies over time. There are many modelling methods that can visually describe the cause-and-effect relationship in networks, which have been used to assess resilience, as described in related works. In particular, the Bayesian network and the dynamic Bayesian network can capture the conditional independence between random variables, which will be more suitable for assessing the resilience of networks. The Bayesian network (BN), also known as belief networks or causal networks, is a direct acyclic graphical model for describing the conditional probability relationship between data variables based on probabilistic inference theory. The nodes in BN represent random variables, and the links between them represent conditional dependencies between variables with parent nodes, which are determined by conditional probability (CPT) tables. However, static BN cannot be used to model time-varying systems. Therefore, the Dynamic Bayesian Network (DBN) based on the hidden Markov model was proposed to satisfy the time system. In Figure 4.1



we can see why the DBN is also called the two-time interval BN, because in the DBN modelling there are two-time intervals, namely the time interval  $t$  and  $t + \Delta t$ . The discrete time interval  $\Delta t$  is usually set to 1 [10].

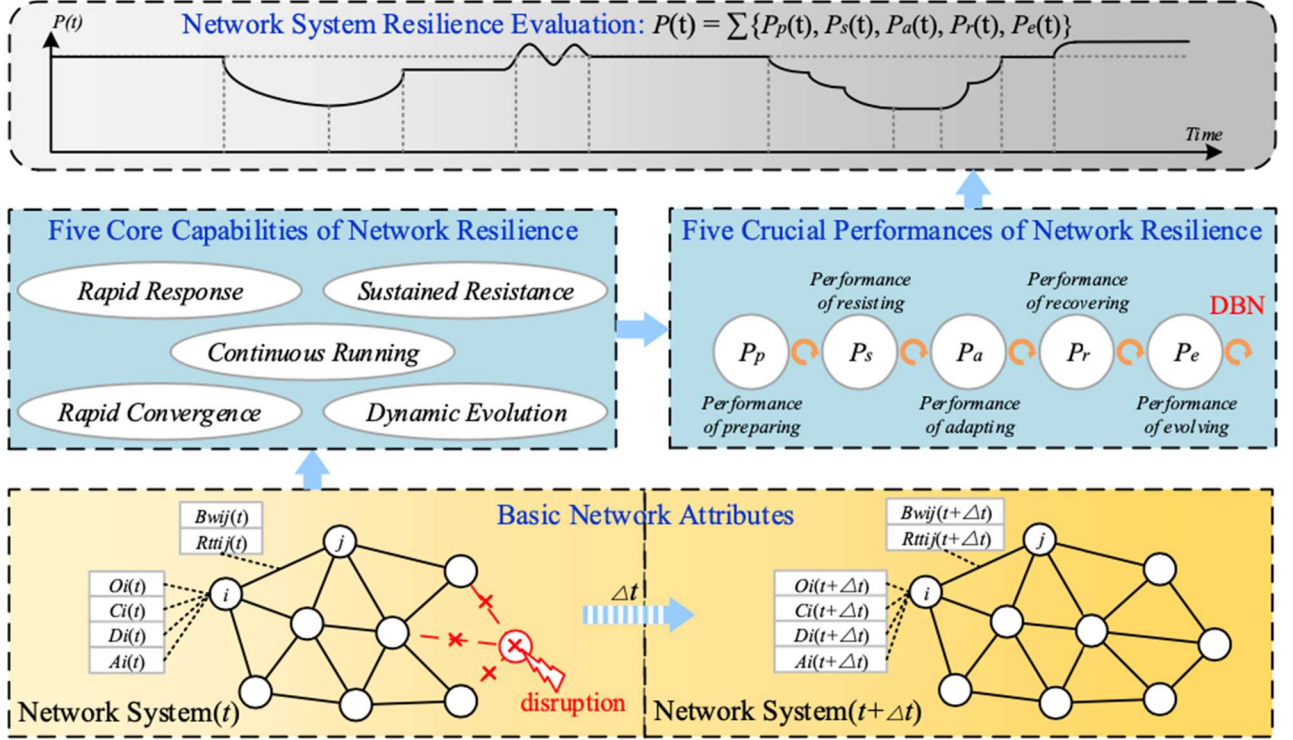


Figure 4.1 – Network resilience evaluation framework

To develop a more detailed resilience assessment model, the characteristics of the resilience network rather than the actual network nodes will be modelled as nodes of the DBN model. There is insufficient literature that describes  $P(t)$  formally, or designates a simple system attribute as a quantitative standard of  $P(t)$ . We establish a detailed quantitative indicator of  $P(t)$ , which is determined by five defined and time-independent network performances:  $P_p(t)$  preparation performance,  $P_s(t)$  resistance performance,  $P_a(t)$  adjustment performance, recovery performance of  $P_r(t)$  and evolution performance of  $P_e(t)$ . These five results are directly influenced by the five fundamental resilience skills described in Section III-B. Meanwhile, there is also a time-dimensional interaction between these five outcomes based on conditional probability. For example, network A and network

B have the same sustained resilience (SRC) at time  $t + \Delta t$  if they experience the same destruction at time  $t$ , but the preparedness power  $P_p(t)$  of the network A is lower than that of network B at time  $t$ . Network A should have better resistive performance  $P_s(t + \Delta t)$  than network B due to the influence of the previous moment.

DBN is adopted in the following details in network resilience modelling and evaluation, and the basic structure of DBN is shown in Fig. 4.2. First, each row of nodes represents the five resilience performances over the same time period, with the five attribute nodes connected by solid arcs. The solid arcs represent the conditional transition probability between the parent node and the self-node. Second, each column of nodes represents the time-varying states of each resilience performance. In Figure 4.2, the dashed arcs between the column nodes represent the temporal conditional transition probability of each resilience performance [10].

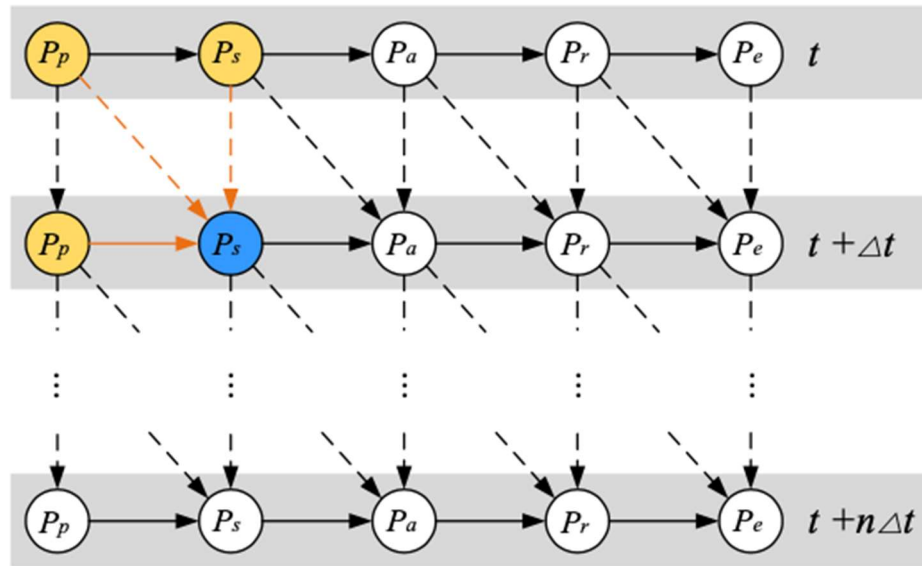


Figure 4.2 – DBN structure of network resilience performances

Conditional transition probability between the parent node at the previous time slice and the self-node at the current time slice [9].

$$P_s^{t+\Delta} = P(P_s^t)P(P_p^t)P(P_p^{t+\Delta}) \times \text{SRC}^{t+\Delta t} \quad (4.2)$$

Where the three conditional transition probability  $P(P_s^t)$ ,  $P(P_p^t)$ , and  $P(P_p^{t+\Delta t})$  are determined by the state of three front nodes, respectively. Based on the evaluation of five resilience performances, the network resilience performance  $P(t)$  can be calculated as a weighted sum of these five performances.

#### 4.3 Numerical discussion and extension of personal experiment

Comparison among other approaches: There has been significant research work performed to evaluate network resilience in recent years. we named these two evaluating methods as compare1 and compare2 respectively. The purpose of this experiment is to demonstrate that our proposed evaluation approach performs better evaluating effects than other methods. The experiment will be performed in certain configurations and assumptions. We make the convention and assumption that the network's destruction mainly focuses on node failure, and once one node fails, the connected edges will fail as well. Then, the failed nodes and edges will be removed from the original network. Moreover, two types of simulated attack behaviours, random- based attack and centrality-based attack, are conducted in the experiment [12].

The random-based attack will randomly delete a given number of nodes and their connected edges from the original network graph. Contrastingly, the centrality-based attack will destroy nodes with larger degree and their connected edges from the network. The relative parameters of experiments are listed in the Table 4.2 below

Table 4.2 – Parameters set in comparison experiment

Symbol	Value	Description
$T_d$	5	The attack occurs at time step 5
$N_d$	$N/3$	The number of deleted nodes during destruction
$N_r$	2	The number of recovered nodes in each time step
$P_A$	1	The probability of effective attack
$P_R$	1	The probability of recovery of nodes and edges

After the attack occurred at time step 5 in the BA and ER networks, the resilience performances declined due to the removal of nodes and edges. The performance of compare1 and compare2 maintain the invariable until the network launches recovery strategies. In contrast, the performance of proposed method continues to decline after destruction. The reason for these differences is that the measurement indicator of compare1 only depends on the network connectivity, or it can be said that it only focuses on the number of nodes in the maximum connected sub-graph, ignoring the network links and capacities.

Similarly, taking the network's flow into consideration, the measurement of compare2 (network flow robustness) shows lower performance reduction due to relatively higher accuracy than compare1. Both of these records only the network's structural properties, which is a relatively constant state value. The evaluation results of compare1 and compare2 neglect many network attributes and functions, which are far from consistent with the real network situation.

Evaluation under different attack and recovery scenarios: The key point of this section is the effective assessment of network resilience in the process of dynamic change rather than specific defence strategies and recovery algorithms. Therefore, network attacks and recovery strategies become input variables to our evaluation framework. To verify the performance of the proposed scoring model in different attack and recovery scenarios, we performed two sets of controlled experiments in scenarios with three levels of attack intensity and three levels of recovery intensity. Each scenario contains three types of networks and two types of modified network models, including random and centralized attack and recovery models. In the modified attack intensity scenarios, the high-level attack is set to  $N_d = (3/4) N$  and  $P_A = 0.8$ , which means that  $3/4$  of the nodes in the original network will be affected by the attack and part of its Nodes whose  $L_i > (1 - P_A)$  are compromised for the attack. Meanwhile, the number of nodes restored is set to 2 at each time step, and the probability of restoring nodes and edges  $P_R$  is set to 1. The purpose of  $P_R = 1$  is to make the controlled experiment more consistent in the recovery phase to demonstrate the differences between the scenarios with modified attack intensity. Similarly, in scenarios with modified recovery intensity, the number of nodes destroyed upon destruction is set to  $(1/2) N$  and  $P_A=1$ , which means a fixed number of nodes will be

destroyed upon destruction. of the attack. These can also eliminate the impact of different attacks on the evaluation of modified network recovery strategies.

#### 4.4 Numerical analysis

In this section, a numerical example is provided to illustrate our methodology in different contexts: a telecommunication network. The telecommunication network case is an abstract example to show how the proposed method can be applied to telecommunication networks and other similar networks. In this case, each node represents a device such as a server or local device, that has its source and destination of data. The resilience of a network depends heavily on the functionality of the servers. We have assumed the equal time interval of  $T$ , in this case, 4-time units, to provide a fair comparison of the resilience of this network.

Telecommunication network: It is assumed that a disruption on a component disconnects it from the network (i.e.,  $\phi_i^n = \phi_i^a; j = \tilde{\phi}_i^a; j_n = 1$ ). The supplies and demands are shown above each node: the first number represents the source node, and the second number represents the destination node per time unit. An arc's flow per time unit at normal operation is displayed above each arc. The proposed telecommunication network is displayed in Figure 4.3 [12].

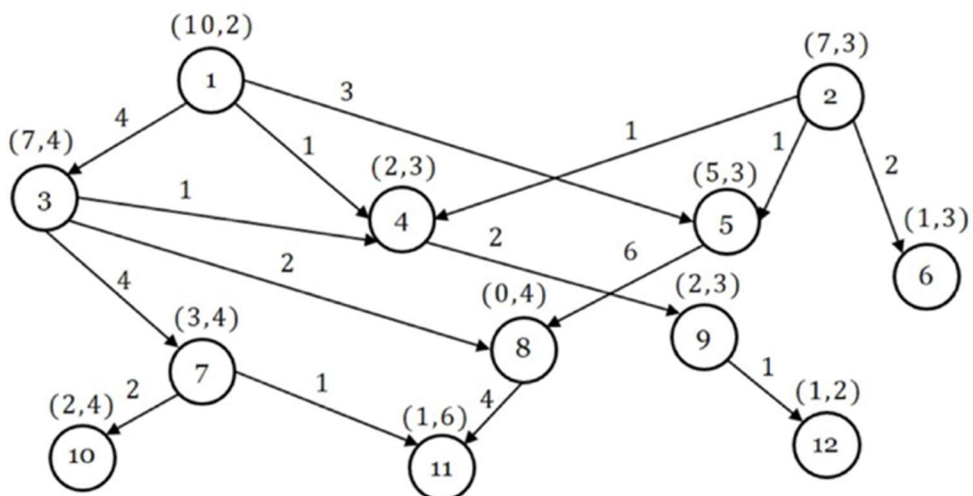


Figure 4.3 – Telecommunication network structure

Node: (source, demand), Arc: flow amount; To calculate the network resilience, the first step is to measure the CRI of each component. To do so, the impact of losing each component on the network (i.e.,  $I^n$  and  $I^a$ ) is calculated.

Component resilience index (CRI): Parameters needed to explain the procedure of measuring CRI

Definition: Impact of a Node Disruption ( $I_i^n$ ) : The impact of a node disruption on the network,  $I_i^n$ , is the total loss when node  $i$  is disconnected from the network. The impact of a node disruption equals the summation of the node source and its incoming flows. It can also be calculated as the summation of node demand and its outgoing flows [7].

$$I_i^n = \sum_j f_{ji} + s_i = \sum_k f_{ik} + d_i, \forall i \in N \quad (4.3)$$

Definition: Impact of an Arc Disruption ( $I_{ij}^a$ )  $ij$  : The impact of an arc disruption on the network is defined as the total loss in the case of disconnecting the arc from the network. Impact of an arc disruption is defined as the flow of that arc [7].

$$I_{ij}^a = f_{ij}, \forall (i, j) \in A \quad (4.4)$$

Definition: Node Criticality: the component criticality is measured as the network loss in a time period that the component is disrupted. The criticality of each component is calculated before a disruption happens by predicting the impact of the component disruption on the network and considering possible alternatives for performing the operation of the disrupted component. In this quantification approach, the disrupted flow is adjusted to the best alternative path where the loss is minimized. An optimization model is proposed to find the best alternative plan in order to minimize the total unmet destinations during the time period that the component is disrupted. A node disruption affects all of the connected arcs as well as the source that the node provides. To calculate the criticality of node  $i$ , the

objective function is defined by Equation (4.6), which is the total unmet destinations the network per unit time:

$$C_i^n = \text{minimize} \sum_{k \in N} IK \quad (4.5)$$

Definition: Arc Criticality (C) : The criticality of an arc is defined in the same way as node criticality. If a disruption happens on an arc, the arc capacity reduces accordingly. To calculate the criticality of arc (i, j), the objective function is defined as:

$$C_{ij}^a = \text{minimize} \sum_{k \in N} IK \quad (4.6)$$

To formulate the CRI for the network components,

$$CRI = 1 - \frac{TDL}{TDN} \quad (4.7)$$

Where TDL -Total destination loss due to the component disruption, TDN - Total destination in the network system during the time interval

Steps for calculation using component resilience index:

1. Step 1: Calculating the impact of each component, Find the impact of a disruption on each node and arc using Equations (4.4) and (4.5),  $I^n$  and  $I^a_{ij}$
2. Step 2: Finding the criticality of each component, Solve optimization model (4.6) to find the criticality of each node,  $C_i^n$ , Solve optimization model (4.7) to find the criticality of each arc
3. Step 3: Calculating the switching time from the alternative plan back to the initial plan, Use the repair rate function of each component to calculate switching times,  $tE^a_{ij}$  and  $tE^n_i$

4. Step 4: Calculating the resilience of each component Use Equations (4.8) and (4.9) to determine the CRI of each node and arc,  $R_i^n$  and  $R_{ij}^a$  [7].

Table 4.1 below shows the indices that are calculated and used for finding the resilience of the nodes

Table 4.1 – Resilience of each node

Node #	$I_i^n$	$L_i^n$	$C_i^n$	$tS_i^n$	$tE_i^n$	$tR_i^n$	$L_1$	$L_2$	$L_3$	$L$	$R_i^n$
1	10	0.2	10	0.2	0	4	0.39	0	3.61	4.00	97.56%
2	7	0.3	7	0.1	0	1	0.20	0	0.85	1.05	99.36%
3	11	0.1	8	0.4	0.55	2	0.40	0.12	0.58	1.09	99.33%
4	5	0.05	5	0.2	0	4	0.05	0	0.45	0.50	99.70%
5	9	0.2	6	0.4	0.67	2	0.65	0.32	0.80	1.77	98.92%
6	3	0.3	3	0.1	0	3	0.09	0	1.26	1.35	99.18%
7	7	0.15	6	0.2	0.29	2	0.20	0.08	0.77	1.05	99.36%
8	8	0.25	6	0.3	0.75	3	0.57	0.68	1.69	2.93	98.21%
9	4	0.2	4	0.5	0	4	0.38	0	1.23	1.60	99.02%
10	4	0.1	4	0.2	0	2	0.08	0	0.32	0.40	99.76%
11	6	0.5	6	0.1	0	3	0.30	0	4.21	4.50	97.26%
12	2	0.35	2	0.3	0	4	0.20	0	1.20	1.40	99.15%

We observe that Node 1 and 11 have a low resilience level in comparison with the others. Node 11 has the lowest CRI among all of the components. The high probability of facing disruption and high criticality associated with this node are the main reasons for its low resilience. Furthermore, Node 1 is responsible for about 25% of the total network source and provides the highest source in the network. This great amount of source from Node 1 results in the large impact index for this node ( $I^1 = 10$ ), meaning that a disruption on Node 1 causes a significant impact on the network. Also, 10 Node 1 has no proper alternative to be used as a substitution of its operation, that makes this node highly critical.



Contrarily, the most resilient node is Node 10, that has a short recovery time, low probability of facing disruption, and low criticality. General resilience of the node is graphically visualised in Figure 4.4

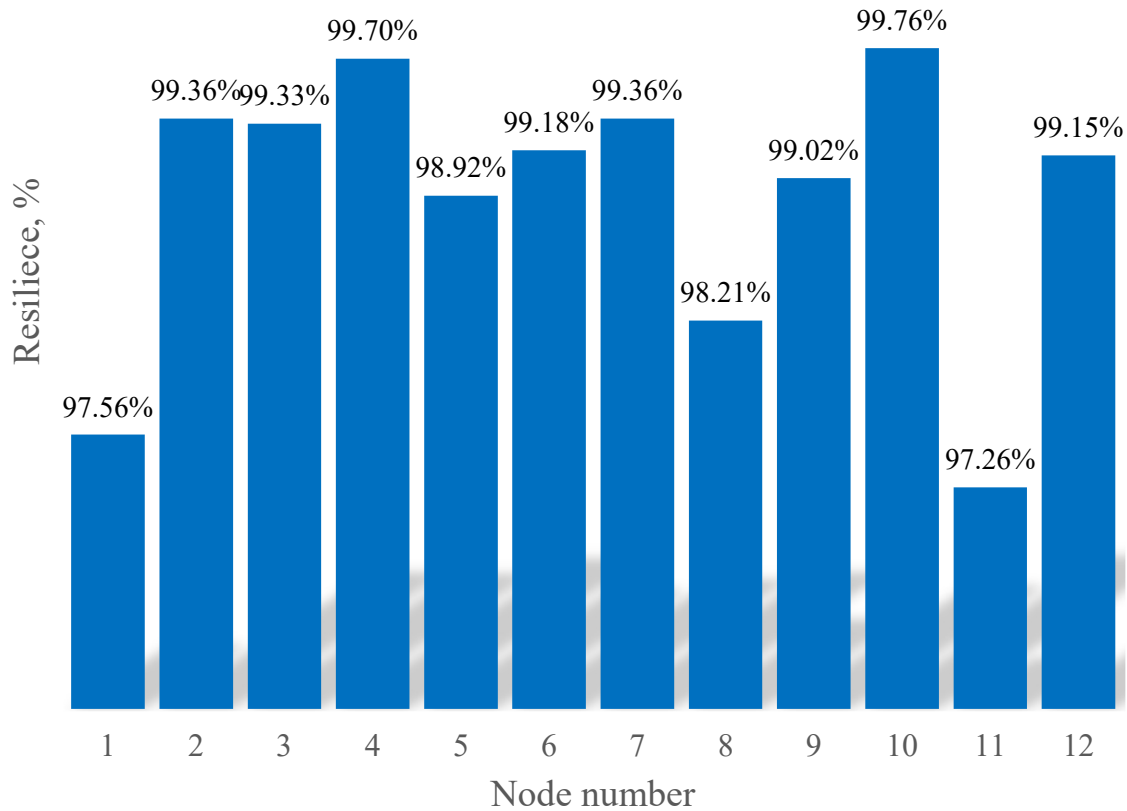


Figure 4.4 – Resilience of nodes

According to the results, Arc (8,11) has the lowest resilience among the arcs ( $R_{8,11}^a = 98.98\%$ ). This arc provides the majority of incoming flow to Node 11, the node with the highest destinations on the network. On the contrary, Arc (7,11) is the most resilient arc ( $R_{7,11}^a = 99.99\%$ ). This large resilience value is justifiable by the fact that Arc (7,11) has the lowest flow and the destinations for its flow can be alternatively satisfied by Arc (8,11).

This study examines the network's ability to use alternative plans. Ignoring this feature and not taking it into account will result in a greater loss of destinations and consequently a lower CRI of the components. Ignoring alternative plans increases the criticality of components to the level of their impact. To prove, consider edges (1,5) and

(3.4) without considering alternative planes. In this case, the expected destination losses associated with their interruption would have increased from 0.34 and 0.10 to 1.35 and 1.00, respectively. Furthermore, the resilience indices of these two arches would have dropped from 99.80% and 99.94% to 99.18% and 99.39% respectively. This highlights that by having alternative plans a significant contribution can be made to improving the resilience of the component.

After calculating the CRI of the components, the network resilience can be enhanced by making an investment in improving the resilience of components with low CRI. Since the resilience of the weakest component in the network is 97.26%, the current network resilience is also 97.26% (i.e.,  $R_{11}^n = 97.26\%$ ). The next two weakest components are Node 1 and Node 8. To improve the network resilience, the resilience of Node 11 can be enhanced to 97.56% (i.e., the resilience level of Node 1).

## CONCLUSION

Knowing the importance of a resilient system, it is adamant that there is a constant need to update and remodel the security of networked systems in order to match and surpass the ever-evolving attempts to penetrate the network.

Evaluating network resilience against random failures and target attacks is an important work in network evaluation and defence. In this research, a comprehensive framework was proposed to qualify the network's time-varying resilience. This framework was developed based on the definition of the dynamic capacities of network components and the measurement of five proposed core network resilience capabilities, which are suitable for the multi-stage processes of network resilience. The DBN approach was employed to quantify the five fundamental and crucial indicators of network resilience performance in temporal network.

The simulation experiments were developed and carried out using a telecommunication network as the base structure for attack and defence of assets, to validate the effectiveness and universality of proposed evaluation framework.

The proposed method for evaluating resiliency according to research carried out is one that identifies the component with the lowest resiliency value as the dictator for the resiliency of the entire system, this component should then undergo a step-by-step process to improve and bolster its individual resilience.

For future work, it is planned to build a resilience evaluation system in physical network environment. Additionally, SDN and networking slice technology deserve attention for providing resilient network capability in future research.

## LIST OF REFERENCES

1. Gritzalis D. Critical Infrastructure Security and Resilience / D. Gritzalis, M. Theocharidou, G. Stergiopoulos. – Springer Nature Switzerland AG, 2019. – 313 p., doi: <https://doi.org/10.1007/978-3-030-00024-0>.
2. Piccolo G. Information Systems for Managers: With Cases / G. Piccolo. – Prospect Press, 2018. – 23 p.
3. Chen K. Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections / K.R Chen, F. S. Wen, and J. H. Zhao // Dianli Zidonghua Shebei/Electric Power Automation Equipment. – 2017. – Vol. 37, No. 12. – pp. 67–72., doi: <https://doi.org/10.16081/j.issn.1006-6047.2017.12.009>.
4. Yeremenko O. Secure Routing in Reliable Networks: Proactive and Reactive Approach / O. Yeremenko, O. Lemeshko, A. Persikov // Advances in Intelligent Systems and Computing II. CSIT 2017. Advances in Intelligent Systems and Computing. – 2018. – Vol. 689. – P. 631–655., doi: [https://doi.org/10.1007/978-3-319-70581-1\\_44](https://doi.org/10.1007/978-3-319-70581-1_44)
5. D'Atri A. Interdisciplinary Aspects of Information Systems Studies / A. D'Atri, M. Marco, N. Casalino. – Physica-Verlag Heidelberg, 2008. – 416 p., doi: <https://doi.org/10.1007/978-3-7908-2010-2>.
6. Henry D. Generic metrics and quantitative approaches for system resilience as a function of time / Henry. D, Ramirez Marquez J.E. // Reliability Engineering & System Safety. – 2012. – Vol. 99. – P. 114–122.
7. Cai Y. Reliability analysis of cyber–physical systems: case of the substation based on the IEC 61850 standard in China / Y. Cai, Y. Chen, Y. Li, Y. J. Cao. – 2018. – P. 25–89.
8. Mackenzie C.A. Measuring changes in international production from a disruption: Case study of the Japanese Earthquake and Tsunami / C.A. Mackenzie, J.R. Santos, A. Barker // International Journal of Production Economics. – 2012. – Vol. 138. –P. 293–302.

9. Cai Y. Reliability Analysis of Cyber–Physical Systems: Case of the Substation Based on the IEC 61850 Standard in China / Cai Y, Chen Y, Li Y, Cao Y, Zeng X. // Energies. – 2018. – No. 10(11). – P. 2589., doi: <https://doi.org/10.3390/en11102589>.
10. A Quantitative framework for network resilience evaluation using dynamic Bayesian network [Electronic resource] – 2021. – Resource access mode: www/URL: <https://deepai.org/publication/a-quantitative-framework-for-network-resilience-evaluation-using-dynamic-bayesian-network>.
11. What are the types of cyber security assessment [Electronic resource] – Resource access mode: www/URL: <https://iosentrix.com/blog/What-is-cybersecurity-assessment-types-of-cybersecurity-assessments/>.
12. Navid Ahmadian N. A. A Quantitative Approach for Assessment and Improvement of Network Resilience / N. A. Navid Ahmadian, J. C. Jaeyoung Cho // Reliability Engineering & System Safety. – 2020. – Vol. 200. – P. 106977., doi: <https://doi.org/10.1016/j.ress.2020.106977>.
13. Haihua Y. Critical nodes identification in complex networks / Y. Haihua, Shi An // School of transportation science and technology. – 2019. – 8 p., doi: <https://doi.org/10.3390/sym12010123>.
14. Yuchen Z. Optimal decision-making approach for cyber security defence using game theory and intelligent learning / Zhang Yuchen, Jing Liu // Security and Communication Networks. – 2019. – P. 1-16., doi: <https://doi.org/10.1155/2019/3038586>