Problem Chosen

F

2025
MCM\ICM
Summary Sheet

Choosing a long enough lever to pry over 'cybercrime': analyze determinants, explore legal policies and safeguard cybersecurity

Summary

Recently in Thailand, the incident of actor Wang Xin being tricked into engaging in cyber fraud in Thailand has attracted widespread attention. In recent years, cybercrime cases have been occurring frequently, posing a serious threat to collective and individual property and privacy security. Seeking meaningful identification patterns for robust national cybersecurity policies and improving the effectiveness of laws has become an urgent issue nowadays. This paper proposes a dynamic pattern recognition model for cybercrime based on **Hierarchical Clustering Method**[1], and **Random Forest Regression Model**[2].

In Task 1, we obtained the raw data of the Global Security Index from the Global Cybersecurity Index website, and with the help of Folium and Choropleth, we mapped the cybersecurity index to a map using Python and drew a heat map to obtain a global map of the distribution of the degree of cybersecurity, see Fig. 7. We obtained the raw data of the number of cybercrimes around the globe from github and segmented the data according to the temporal granularity (one year) and extracted the time period in which the cybercrime occurred to get the cybercrime trends in India, Australia, US and UK, see Figures 2-5.In addition, we investigated the data on cybercrime prosecuted or stopped, see Figure 8.Finally, we analysed the optimal decision making by using **Nash equilibrium analysis**[3], the expected utility model, to analyse the circumstances in which a company would choose to pay the ransom instead of reporting to the police.

In Task 2, four typical countries were selected based on the GCI, values of Denmark, Germany, Afghanistan, and Myanmar (petite high cybersecurity index vs. low cybersecurity index.) , analyse the impact of laws and policies on cybercrime. In the government official website to obtain the relevant laws and regulations, as well as the implementation time of the laws and regulations, combined with the number of cybercrime and cybersecurity index of each country, to analyse the legal model of three relevant points, to obtain the characteristics of the effective law and ineffective law between. At the same time, according to the time of promulgation and updating of laws, and the time of intervention in transnational co-operation, we conclude that the time factor has an impact on cyber security.

In Task 3, we searched the data from major authoritative websites for the GDP population size, education level, internet usage rate, etc. of each country, imported the Google Translate library into Python to unify the language of country names, and used Python to fuse the data and filter out the valid data to generate a table. Using **Random Forest Model** to help predict how these influencing factors affect the relevant indicators of cybersecurity, fit the non-linear data to conclude that the factor that contributes the most to the cybersecurity index is GDP. and generate charts through data visualisation.

Keywords: Hierarchical Clustering, Nash equilibrium, Random Forest Model.

Content

I.Introduction

1.1 Background

More and more of our world has become connected through the wonders of modern technology, such as the development of network nechnology. While this online connectedness has increased global productivity and made the world smaller, it has also increased our individual and collective vulnerability via cybercrime. Cybercrime is difficult to counter for a variety of reasons. Many cybersecurity incidents cross national borders, complicating issues of jurisdiction for both the investigation and the prosecution of these crimes.

To address the growing cost and risk of cybercrime, many countries have developed national cybersecurity policies, publicly available on their government websites. The International Telecommunication Union (ITU) is the specialized agency of the United Nations focused on information and communication technology; as such, they play a leading role in setting international standards, facilitating international cooperation, and developing assessments to help measure the status of global and national cybersecurity.

As concerns about cybercrime, the necessity for developing a theory to check the usefulness of strong national cybersecurity policy becomes more obvious. It is therefore urgent to propose a multi-level model to explore the factors that contribute most to the GCI, how to know the geographical distribution of cybercrime and how to judge the legal benefits.

1.2 Restatement of Problem

The question asked us to analyse the factors that affect cyber security and how cybercrime is distributed, as well as how to determine whether legal policies are effective. What we need to do is as follows:

- we investigated the data on primary school completion rates, GDP, population, number of people using the internet, total public spending on education, secondary school completion rates, number of fixed broadband subscriptions.
- A Random Forest Model was used to derive GTP as the most important factor contributing to network security.
- Hierarchical Clustering was used to subdivide the countries classified according to the GCI scale into continental geographies. Finally we visualised the data - the danger index mapped on a map - to derive the geographical distribution of cybercrime.
- We investigated the cybercrime success, frustration, defendant, and prosecution rates in the recent years, which makes the research target clearer and the conclusions more precise.Then we analyse the legal policies of four countries.

1.3 Overview of Our Work

In this paper, We analysed and aggregated a large amount of data and used the Random Forest model to identify the influencing factors that contribute the most to cybersecurity. Based on the fact that the higher the GCI, the lower the cybercrime rate, we used cluster analysis and data visualisation to know the geographical distribution of cybercrime. Finally, we selected regions with extreme GCI values and

analysed whether their laws are effective.Through the above analysis, the flow chart of this paper is shown in Figure 1.

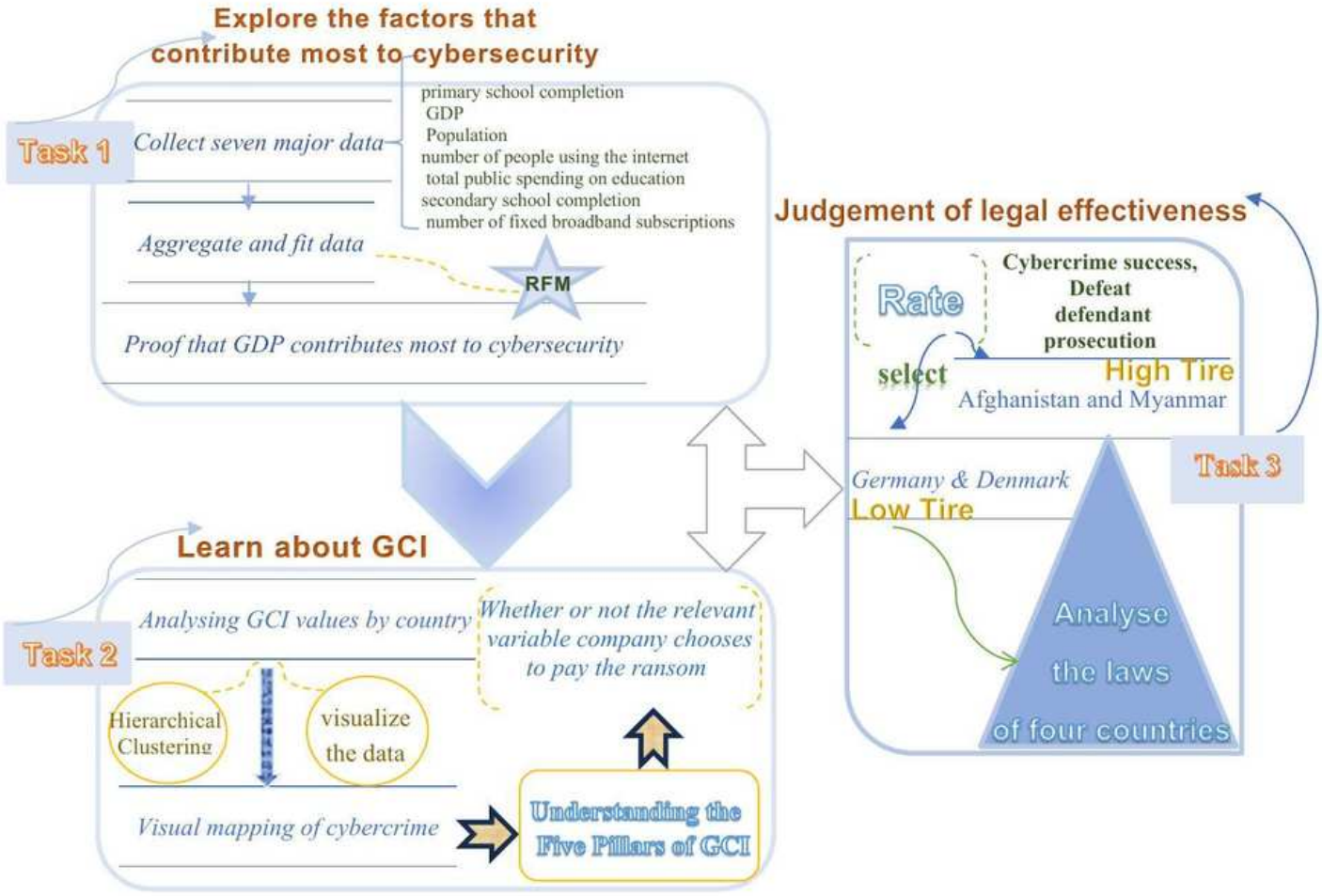


Figure 1.The flow chart of this paper

II. Assumption and Symbol Explanation

2.1 Assumption

- The seven factors of primary school graduation rate, GDP, population, number of people using the Internet, total public expenditure on education, secondary school graduation rate, and number of fixed broadband subscribers are a few of the most important factors affecting cybersecurity, and have changed steadily over time in recent years, and will not be obsolete by the times, so the influence of the other secondary factors is ignored.
- In 5.1, when investigating the issue of GDP and population in each country, there were cases of incomplete data, which we have disregarded because of their small impact.

2.2 Symbol Explanation

For convenience, we use the following symbols in our models, as shown in the table below.

Symbols	Definition
$Merged_{tier}$	The consolidated data contains data on national security gradient rankings and influencing factors for 2020-2023.
R^2	A metric in the model to measure the goodness of fit, the closer to 1 the better the model fit.
MSE	Mean Square Error, the squared average of the difference between the predicted value and the true value of the response, the smaller the value, the better the model
X	Influencing factors such as GDP and population.
Y	Tier values for cybersecurity

III. Task 1

3.1 Crime trends over time

In this chapter, we find a json file of 10,000 crime records by finding them in github's VCDB and transcoding them into an Excel document through Python code. Analysing these data, we can conclude that the countries with high crime frequency, including Myanmar, Cambodia, Afghanistan, etc., while the countries with low crime ratings include Germany Denmark, etc. Find out the trend of cybercrime in each country based on crime frequency. Below are 5 representative countries.

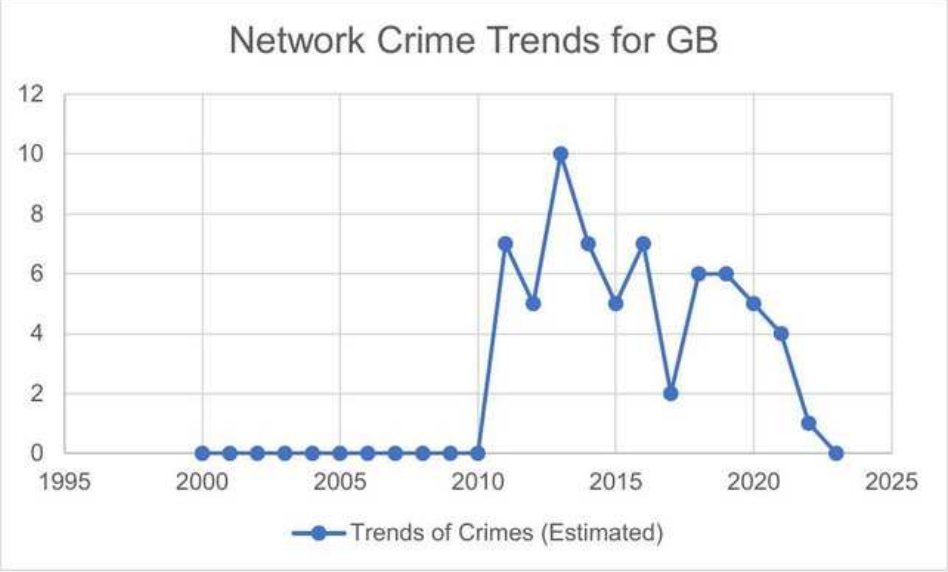
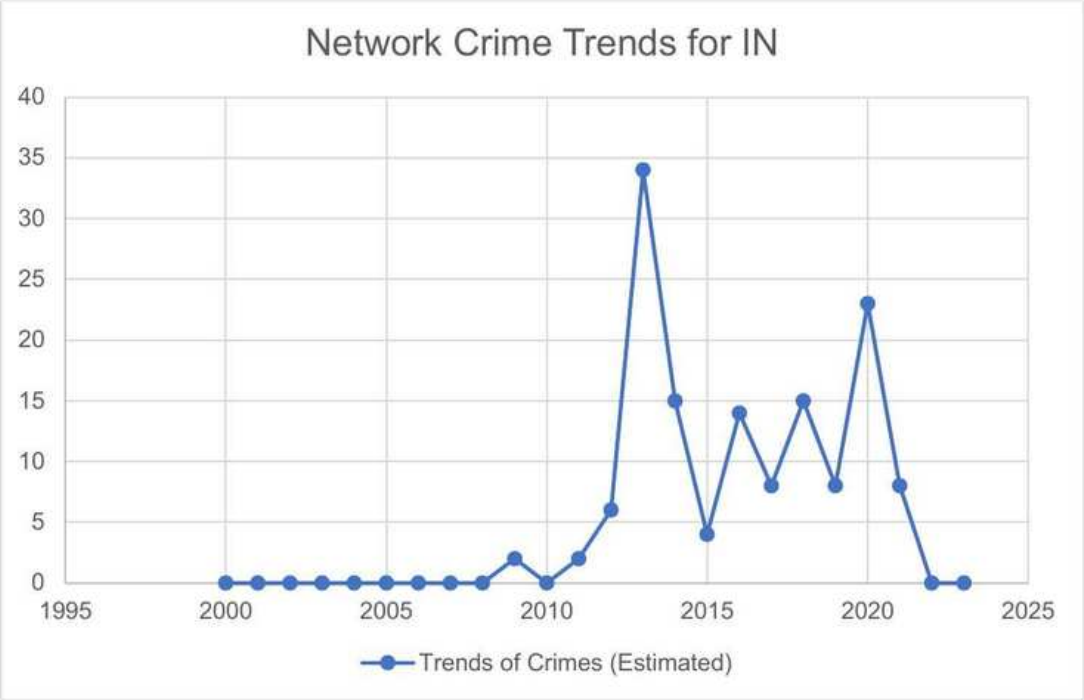


Figure 2. Network Crime Trends for GB

As can be seen from the figure 2, the number of cybercrimes in the UK stabilised in the first ten years of 2010, and plummeted in the six years since 2010. And from 2016 onwards the crime rate plummeted.



Fighre 3. Network Crime Trends for IN

Italy has seen rapid growth since 2012 to 2013. but measured in tens. cybersecurity is less of a problem than in other countries. There are four peaks and three troughs, with a rapid decline starting in 2020.

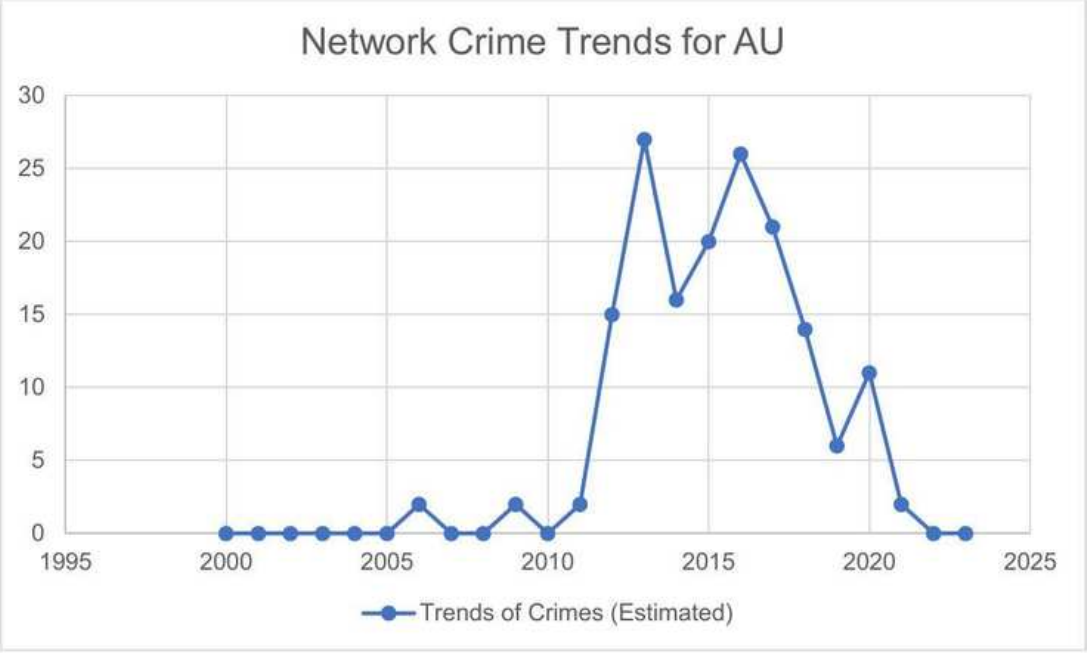


Figure 4. Network Crime Trends for AU

The number of cybercrimes in Australia has shown an M-shape over time, with an upward trend from 2011 to 2013, 2014 to 2016, and 2019 to 2020. The rest of the time shows a downward trend.

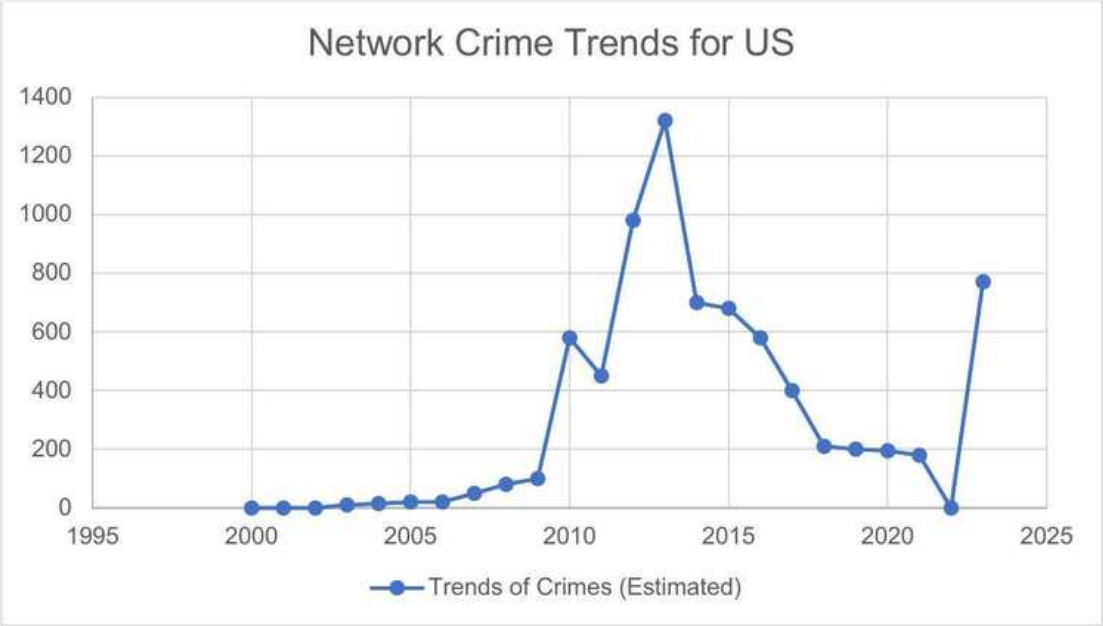


Figure 5. Network Crime Trends for US

In the United States, the number of cybercrimes increased dramatically from 2009 to 2013 and was measured in thousands, 10 to 100 times higher than in other countries, and then declined but remained higher than in other countries. And it starts to pick up from 2022.

In summary, all five countries reached peak levels of cybercrime around 2013 and have since eased.

3.2 Geographical distribution of cybercrime

To consider the global distribution of cybercrime, we refer to the GCI. By reviewing the literature [4], we know that the Global Cybersecurity Index (GCI) is a global cybersecurity ranking index published by the International Telecommunication Union (ITU). It assesses the maturity and efforts of countries around the world in the field of cybersecurity, focusing mainly on the policy,

legal, technological, organisational, capacity building and cooperation aspects of cybersecurity.The purpose of the GCI is to help countries identify their cybersecurity strengths and weaknesses, and to promote the improvement of cybersecurity globally.

The GCI usually classifies countries into different **Tiers**, which reflect a country's performance in various dimensions of cybersecurity. The tiers range from 1 to 5 and are usually:

- Tier 1: leading level, with an efficient cybersecurity system and advanced policies and laws.
- Tier 2: Medium level, with some cybersecurity systems in place but room for improvement in some areas.
- Tier 3:lower level, with a weak cybersecurity system that needs to be strengthened in terms of infrastructure.
- Tier 4
- Tier 5

These tiers help countries and the international community to understand what needs to be strengthened and to take corresponding measures to enhance global cybersecurity protection capabilities.

We examine the global distribution of cybercrime and which countries are high-frequency targets for cybercrime. We start by obtaining the t-value of the Global Cybersecurity Index (which is stratified by scoring and

weighted average of its five pillars) to judge the security level of each country. Then get the json file of nearly 10,000 crime records data from github database and parse out the Excel table through Python. Get the global distribution of cybercrime and the frequency of cybercrime.

We list the countries from Tier 1 to Tier 5 in a three-line table, as shown in Table 1 below.

Table 1.Tier performance :Global

Region	Country	Score
Tier I Role-modelling	Australia/Bahrain/Bangladesh/Belgium/Brazil/Cyprus/Denmark/Egypt/ Estonia/Finland/France/Germany/Ghana/Greece/Iceland/India/Indonesia/ Italy/Japan/Jordan/Kenya/Luxembourg/Malaysia/Mauritius/Morocco/ Netherlands（Kingdom of the）/Norway/Oman/Pakistan/Portugal/Qatar/ Korea（Republic of）/Rwanda/Saudi Arabia/Serbia/Singapore/Slovenia/ Spain/Sweden/Tanzania/Thailand/Turkey/United Arab Emirates/ United Kingdom/United States/Viet Nam;	95-100
Tier II Advancing	Albania/Austria/Azerbaijan/Benin/Canada/China/Croatia/Czech Republic/ Ecuador/Georgia/Hungary/Ireland/Israel/Kazakhstan/Lithuania/Malta Mexico/Philippines/Poland/Romania/Russian Federation/Slovakia/ South Africa/Sri Lanka/Switzerland/Togo/Uruguay/Uzbekistan/Zambia;	85-95
Tier III Establishing	Algeria/Andorra/Belarus/Bhutan/Botswana/Brunei Darussalam/Bulgaria/ Burkina Faso/Cuba/Dem. Rep. of the Congo/Dominican Rep/Eswatini/Ethiopia/Gambia/Guinea/Iran (Islamic Republic of)/Libya/ Malawi/Moldova/Monaco/Mongolia/Montenegro/Mozambique/Myanma/ Papua New Guinea/Paraguay/Peru/Senegal/Sierra Leone/Tunisia/Uganda Trinidad and Tobago/Cameroon/Chile/Colombia/Costa Rica/ Côted'Ivoire/Jamaica/Kiribati/Kuwait/Kyrgyzstan/Latvia/Ukraine/ Vanuatu/New ZealandPanama/North Macedonia/ Nigeria/Nepal （Republic of）;	55-85
Tier IV Evolving	Angola/Argentina/Armenia/Bahamas/Barbados/Belize/Cambodia/Chad/ Bolivia （Plurinational State of）/Bosnia and Herzegovina/Cabo Verde/ Comoros/Congo（Rep. of the）/Djibouti/Dominica/EI Salvador/Fiji/Haiti/EquatorialGuinea/Gabon/Grenada/Guatemala/ Guyana/Honduras/Iraq/Lao P. D, R, /Lebanon/Liberia/Liechtenstein/Madagascar/Mali/Mauritania/ Namibia/Niger/Saint Kitts and Nevis/Saint Vincent and the Grenadines/ Samoa/San Marino/Sao Tome and Principe/Seychelles/Somalia/Sudan/ South Sudden/State of Palestine/Suriname/Syrian Arab Republic/Tonga/ Tajikistan/Turkmenistan/Tuvalu/Venezuela/Zimbabwe;	20-55
Tier VI Building	Afghanistan/Antigua and Barbuda/Burundi/Central African Rep./ Dem. People's Rep. of/Korea/Eritrea/Guinea-Bissau/Maldives/Micronesia/ Marshall Islands/Solomon Islands/Timor-Leste/Vatican/Yemen;	0-20

Then indicators at each level are then disaggregated by region as figure 6.

Figure 6. GCI Tier performance, by region

Places with a higher GCI have a lower cybersecurity index and a higher risk of cybercrime, while places with a lower GCI have a higher cybersecurity index and a lower risk of cybercrime. We map the Tier levels of the GCI on a global map through data visualisation, which solves the problem of cybercrime distribution. We used geo-data visualisation libraries, Geopandas and matplotlib: first to get a geo.json file of the world map and associate the crime values with the corresponding geographic locations (e.g. countries, cities, etc.). The folium library is used to display the map, pandas to process the data, and Geopandas to process the data in geo.json format. Use folium and Choropleth to achieve finer gradient colours (e.g. changing colours according to the specific value of the crime value) through the Choropleth layer or ColorMap class to achieve the legend. Thus achieve the effect of data visualisation.The map in Figure 4 is as follows.

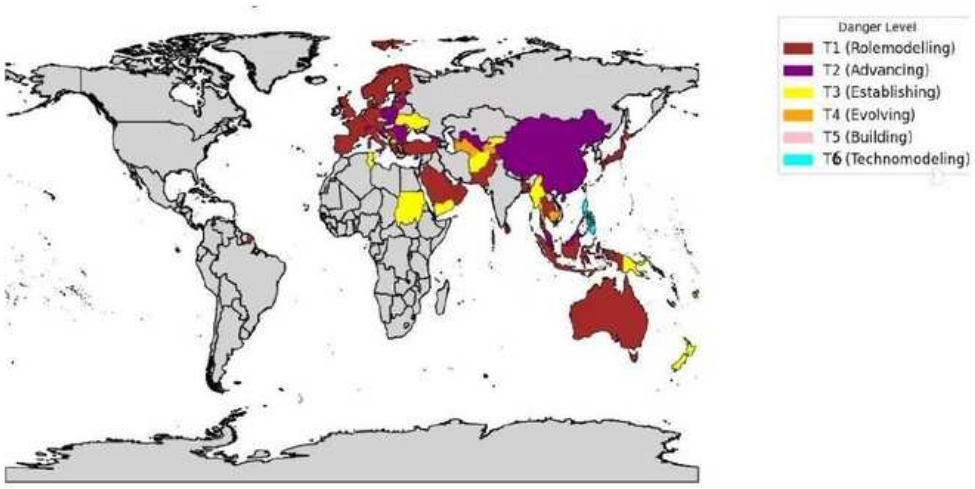


Figure 7. Global cybercrime map

3.3 The five dimensions of the GCI

Based on a search of relevant literature.[4] The ITU Global Cybersecurity Index (GCI) has five core pillars:

- Legal: whether there is a sound legal framework to combat cybercrime.
- Technical: Whether advanced technical means are used to detect and prevent cyber threats.
- Organisation: Whether there is a dedicated institution and strategy to deal with cybersecurity issues.
- Capacity Building: Whether it focuses on personnel training and cybersecurity capacity enhancement.
- Co-operation: whether it co-operates with international or regional agencies to tackle cybercrime.

The GCI can be used as a quantitative indicator to measure the level of cybersecurity, and a higher score means a stronger cybersecurity capability.

We investigated the information in table 2 below.

Table 2. Status of GCI I and II indicators

Tier 1 indicator		Tier 2 indicator
Legal	✓	Substantive law of cybercrime
	✓	Domain-specific cybersecurity legislation
Technical	✓	State or government cybersecurity emergency response agencies
	✓	Industry's cybersecurity emergency response organisation
	✓	National cybersecurity standards implementation framework
	✓	Children's Internet Protection
Capacity Building	✓	Public awareness campaign on cyber security
	✓	Training for Cyber Security Professionals
	✓	Educational Programmes/Academic Courses
	✓	Cybersecurity Research and Development Programme
	✓	National Cybersecurity Industry
	✓	Government Incentive Mechanisms
Co-operation	✓	Bilateral agreements on cybersecurity cooperation
	✓	International mechanisms
	✓	Multilateral agreements on cybersecurity
	✓	Private sector co-operation
	✓	Cross-sectoral co-operation

3.4 Cybercrime success, defeat, defendant and prosecution rates

Determining the object of the study

Based on the chart in 3.1, we clearly identified the extreme countries of Tier 1 and Tier 5, and to further narrow down the scope, we investigated the cybercrime success, frustration, defendant, and prosecution rates in the recent years, which makes the research target clearer and the conclusions more precise. We can then make a targeted study of the legal policies of these regions, as well as judge whether they are effective or not.

Bar charts of cybercrime success, defeat, defendant and prosecution rates for various countries in recent years.

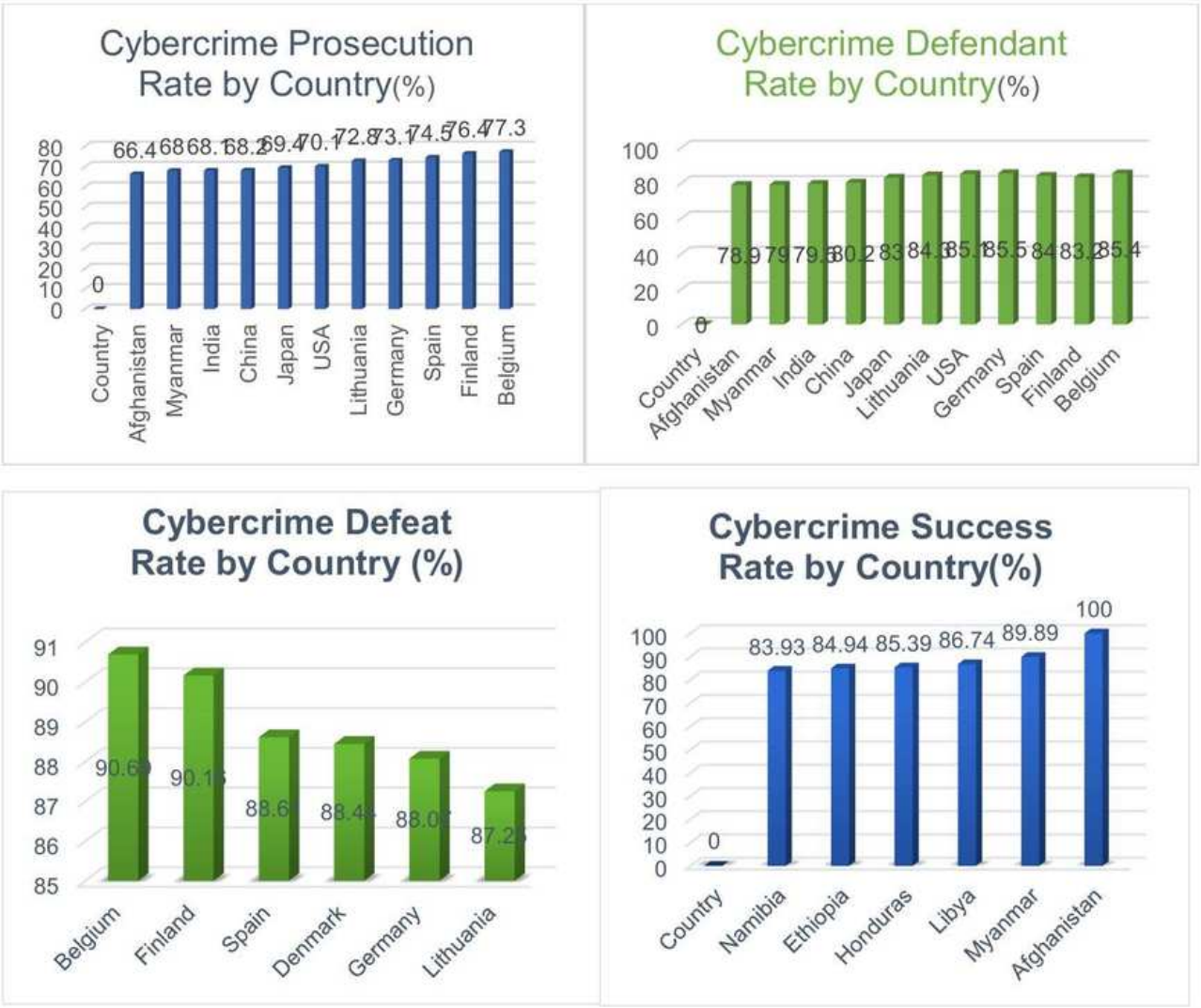


Figure 8. Cybercrime success, defeat, defendant and prosecution rates

It can be observed from these data that countries with higher success rates in cybercrime tend to be areas with weaker legal systems at lower levels of economic development, such as Afghanistan and Zindia, where reporting and prosecution rates are generally lower, indicating that offences are easier to commit and harder to track. In contrast, the countries with higher cybercrime failure rates are mostly developed countries with well-developed legal systems and strong technological defences, such as Belgium and Finland, which also have higher reporting and prosecution rates, indicating a high degree of attention to

cybercrime and effective governance. At the same time, it can be found that there is a certain positive correlation between the reporting rate and the prosecution rate, indicating that strengthening the reporting mechanism may also increase the probability of offenders being prosecuted, a trend that is particularly evident in countries such as Belgium and Finland Overall, the success of cybercrime is closely related to the strength of preventive and governance measures, and the differences in the capacity of countries reflect different levels of technology, law enforcement efforts and public participation.

In 4.1, we will focus on the laws of these countries with extreme GCI ratings, such as regions with a low risk of cybercrime - Germany, Denmark and regions with a high risk of cybercrime - Afghanistan, Myanmar.

3.5 The company in question is willing to pay the ransom

The data we have obtained above are based on successful cybercrime and defendants, so for the sake of the rigour of the paper, we will discuss some special cases below, such as where the company in question did not choose to pay the ransom, etc.

If the company is hacked, does he choose to call the police or pay the ransom?

Assume two parties are involved:

- Companies/Banks: Have the option of paying a ransom or calling the police in the event of a cyber attack.
- Hackers: After a successful attack, they can choose to release the data or continue to increase the attack to get more ransom.

We further analyse：

The company chose to pay the ransom:

- Hacker chooses not to release data: If the company calls the police, the hacker may choose to make further threats or release the data, causing more damage.
- Hacker chooses to release data: If the company pays the ransom or remains silent, the hacker releases the data or stops the attack.

The company chooses to call the police:

- The hacker may be caught, but the data may not be recovered.
- The hacker may have encrypted or intentionally leaked the data. This may also result in a loss of public trust in the company.

We can see that there are two options for each side. The optimal strategy is now analysed using **Nash equilibrium**. Assume that both parties are rational players and choose the strategy that maximises their returns.

The relevant variables are as follows:

Variables	Definition
R	The company chooses to pay the ransom
A	Reporting to the police costs
C	Hackers continue to attack at a cost of C
S	The firm may also have reputational damage

- Conditions of the company's election to pay the ransom:

The company chooses to pay the ransom if and only if:

$$A+S<R \tag{1}$$

i.e., the loss from paying the ransom is less than the total loss from calling the police (A+S)

- Conditions under which the company chooses to call the police:

The company chooses to call the police when and only when:

$$R<A+S \tag{2}$$

i.e., the loss from calling the police is less than the loss from paying the ransom.

- Conditions under which the hacker chooses to release the data:

When the hacker chooses to release the data, he needs to compare the expected gain from continuing the attack with the gain from releasing the data. If the attack continues, more ransom may be gained, but there is also a risk of arrest:

$$R_2 - p_{\text{capture}} \cdot M > R \tag{3}$$

Conditions under which the hacker chooses to continue the attack:

- The hacker chooses to continue the attack if and only if:

$$R_2 - p_{\text{capture}} \cdot M < R \tag{4}$$

That is, he chooses to release the data if the expected gain from continuing the attack is less than paying the ransom.

Now analyse the optimal strategy using the expected utility model

Assuming that the probability of a cyber attack is attack, the hacker will make decisions based on his expected utility. We can further calculate the expected utility considering the probability of each strategy:

The expected utility of the company is:

$$EU_{\text{Company}} = p_{\text{Pay Ransom}} \cdot (-R) + p_{\text{Report}} \cdot (-A - S) \tag{5}$$

The expected utility of the hacker is:

$$EU_{\text{Hacker}} = p_{\text{Pay Ransom}} \cdot R + p_{\text{Report}} \cdot (R_2 - p_{\text{capture}} \cdot M) \tag{6}$$

By analysing these expected utilities and optimising the parameters in the model, we can derive the optimal choice of strategy.

IV. Task 2

4.1 Laws of four regions

4.1.1 German Laws

The law relating to cybercrime in Germany is primarily governed by the German Penal Code and the Cybersecurity Act, which together safeguard the cyber environment in Germany[5].

Table 3. Enforcement of Danish Laws and Cybersecurity Index Rankings

Year	German IT Security Law Enforcement Rate	General Data Protection Protection Regulation Enforcement Rate	Cybercrime Law Enforcement Rate	Overall Network and Digital Security Ranking
2020	88%	89%	87%	4
2021	89%	90%	87%	5
2022	92%	88%	88%	4
2023	93%	90%	90%	3
2024	94%	91%	91%	3

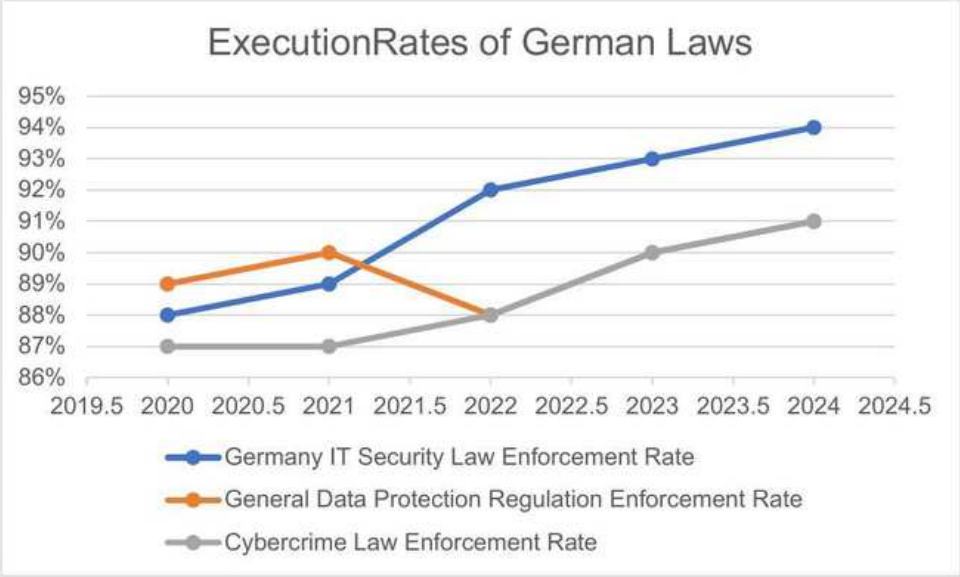


Figure 9. Environment Rates of German Laws

As can be seen in table 3 and figure 9, the average values of the enforcement rate of the IT security law, the enforcement rate of the General Data Protection Regulation and the enforcement rate of the Cybercrime Combating Act in Germany are high and have generally been on an increasing trendover theyears. Germany has the highest enforcement rate of the IT security law,which shows that the IT security law has a great influence and a very strong legal effect in the country.

The German Penal Code has more detailed and strict provisions on illegal access to computer data. The penalties are more severe. And the German law on computer fraud also has more detailed provisions and severe penalties at present, the e-commerce industry as a spring, telecom fraud has become the main form of network fraud, Germany's law effectively protects the people in the online payment or online shopping platform not to be swindled, and cracked down on fraud gangs. These laws effectively increase Germany's resilience to cyber-attacks and allow the government and police to respond quickly. In

summary, German law covers a wide range of areas and effectively strengthens information security in various ways.

4.1.2 Danish Laws

The Danish cybercrime law consists mainly of the Danish Penal Code, the Computer Crimes Act, the Cybersecurity Act and other relevant legislation [6].

Table 4. Enforcement of Danish Laws and Cybersecurity Index Rankings

Year	Danish IT Security Law Enforcement Rate	Danish Data Protection Regulation Enforcement Rate	Cybercrime Law Enforcement Rate	Overall Network and Digital Security Ranking
2020	83%	85%	84%	2
2021	85%	87%	85%	5
2022	88%	88%	86%	5
2023	89%	89%	87%	4
2024	90%	90%	88%	4

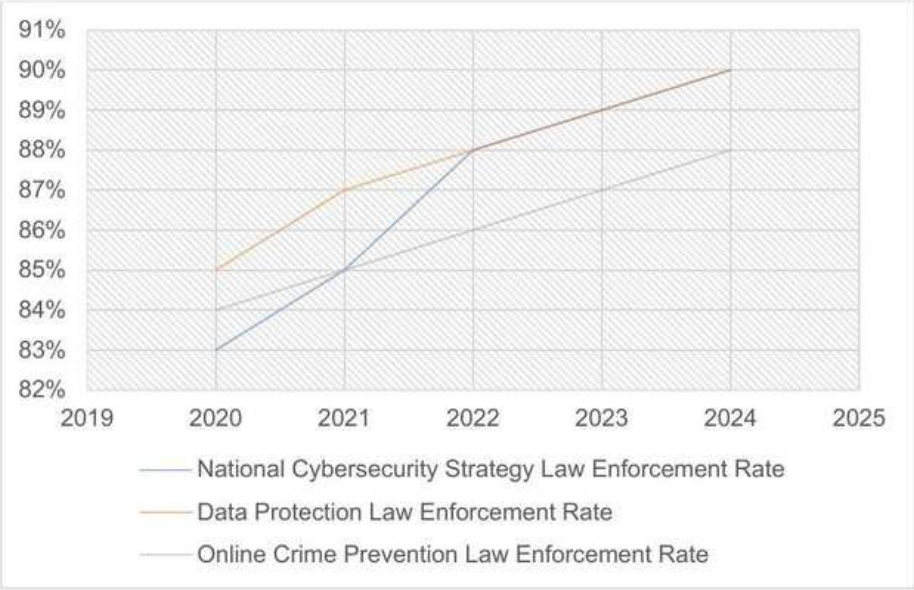


Figure 10. Enforcement of Danish Laws

The Danish legislation is more refined. It contains a serious crackdown on access to computers that I have already granted, strict penalties for illegal surveillance and wiretapping, and a strict crackdown on deliberate tampering with, deleting, falsifying or interfering with computer data. This series can effectively prevent hacker attacks and maintain system security. There are legal provisions on telecommunication fraud as well as cyber fraud that can protect the public from fraud. Clearly define the obligations of network operators and make it clear that network operators must take technical and management measures to prevent network attacks. Enhance the cybersecurity preparedness of the entire country. It can ensure public safety from serious cyberattacks, and it strengthens the prevention and prediction of potential threats, improving the country's ability to respond in the face of large-scale attacks. And Denmark has a set of more severe penalties for cybercrime, which has a high deterrent effect.

4.1.3 Afghan Laws

Afghanistan's cybercrime laws are relatively new, but with the rapid development of the Internet and information technology, the Afghan government has begun to develop regulations to deal with the growing problem of cybercrime. Afghanistan's cybercrime legal system currently consists of legal documents such as the Afghan Penal Code and the Afghan Information Technology Law [7].

Let's look at two specific Afghan laws:

- E-Commerce Regulations.

This law regulates e-commerce transactions and requires that all electronic transactions must comply with relevant laws and regulations to prevent fraud and ensure the legitimacy of transactions.

It states that all online transactions must use encrypted and secure payment systems to prevent any form of fraud.

- Electronic Fraud

Fraud committed through electronic means is also covered by the criminal law of Afghanistan, including false transactions via the Internet, phishing, financial fraud, etc.

Penalties: If fraud is committed via the Internet or other electronic means, suspects may face up to five years in prison and corresponding fines.

The Afghan law also covers regulations related to cross-border fraud, illegal access to computer systems, cyber harassment, and so on. However, we can see that compared to the laws of Germany and Denmark. Afghanistan's law is still not detailed enough, the definition of the specific explanation is not broad enough, and the determination of different situations is not detailed enough, for example, not detailed different levels of hacking. For example, it does not refine the differences between different levels of hacking, such as small-scale attacks and major data breaches. The lack of more detailed sentencing criteria may lead to unfair sentencing. And Afghanistan's law lacks traction on cross-border fraud, many electronic frauds involve cross-border fraud, but the existing law does not deal with this aspect is not perfect, and Afghanistan's lack of international cooperation may lead to difficulties in effectively combating cross-border crime. In addition, the law lacks regulation of online platforms. In contrast to German and Danish laws, the Afghan penal code does not directly regulate platforms, nor does it require them to take precautions. We can note that Afghanistan's law contains

provisions on cyber harassment, but although the law clearly defines cyber harassment, the actual implementation of the law is difficult because it does not provide clear criteria for judgement and is difficult to implement. Although Afghanistan's cyber law system has to a certain extent combated illegal and criminal activities, there is still a gap in implementation and refinement. There are still deficiencies in implementation and refinement that need to be further strengthened. In particular, there is a need for further improvement of online platforms, the international trading environment and cross-border cooperation.

4.1.4 Myanmar Laws

Myanmar's cybercrime legal system is still developing, but in recent years, with the spread of Internet use and the increase in cybercrime activities, the Government of Myanmar has taken a number of measures to enhance cybersecurity and combat cybercrime. Myanmar's cybercrime-related laws mainly include the Electronic Transactions Law, the Information Technology Law and the Penal Code [8].

Similarly, Myanmar has laws on cross-border transactions, electronic information security and data leakage, but there is still a lag, particularly in the Electronic Transactions Act, which was passed in 2004, 20 years after the Act was passed. In these 20 years, technology has changed dramatically, the same form of crime has also produced great changes but the law has not been updated. Many new types of offences have not been dealt with in a timely manner. At the same time, like the Afghan law, the implementing regulations of this law are very unclear. The concepts of the law are vague and the descriptions are extremely broad, which makes it difficult to enforce the law. Moreover, due to the backwardness of Myanmar's science and technology, there are no professional technical means for criminal investigation. It is impossible to respond to new types of cyber attacks in a timely manner. Myanmar's data protection is insufficient, even if the Electronic Transactions Law requires platforms to provide security measures and protect data, but it does not specify how to protect, which leads to data leakage easily. The rights of users are not protected. Moreover, the government of Myanmar's military junta has failed to regulate the various regions of Myanmar in a timely manner, which has led to certain deficiencies in law enforcement and supervision, and many crimes have not been detected and stopped in a timely manner. Moreover, Myanmar is extremely lacking in cross-border cooperation, and it is very difficult to combat many telecommunication frauds, so the country should strengthen international cooperation. The investigation and trial of cross-border crimes are lagging behind. All in all, Myanmar's laws have not been able to adapt to today's ever-changing social environment, which has led to an extremely low national cybersecurity index.

Above all, we can compare the laws of the four countries in the following table 5.

Table 5. Comparative chart of laws in four countries

Country	legal framework	Advantages and Challenges
German	German Criminal Code (2007) Cybersecurity Law (2015/2021)	The German legal system is well - developed, covering a variety of cyber - crimes, including the latest means of cyber - crime. The methods of combating crime are also diverse, applying the latest technologies. The penalties for crimes are relatively comprehensive, with an emphasis on critical infrastructure, cybersecurity, and incident reporting
Denmark	Danish Criminal Code (2021) Computer Crime Law (2014) Cybersecurity Law (2014)	Denmark's legal framework clearly and in detail stipulates specific criminal acts and penalties. It covers various cyber - crimes, emphasizes the security of critical infrastructure, requires the timely reporting of cybersecurity incidents, and has enhanced public awareness of prevention
Afghanistan	Afghanistan Information（2007） Technology Law（2021） Afghan Criminal Law（2021）	The legal system is relatively new and lacks detailed content, which leads to great difficulties in implementation. There is a shortage of sufficient technical support and resources, a lack of certain cross - border international joint actions, and a lack of strong government guarantees. The punishment mechanism is also imperfect
Myanmar	Myanmar's Electronic Transaction Law（2015/2021） Myanmar Information Technology Law（2023）	The legal system is rather outdated and unable to cover the latest forms of crime. There is a lack of strong supervision and a sound legal framework. The enforcement capacity is insufficient, and cross - border cooperation is lacking. The overall public awareness of cybersecurity is low, resulting in an extremely severe situation of cybercrime

4.2 Pattern Judgement.

✧ Dynamic Adaptation and Updating of Laws

Dynamic adaptation of laws is evidenced by the effectiveness of laws that are updated in response to rapidly changing technological environments and crime trends. Such laws maintain the ability to respond to new types of threats. For example, the dynamic updating of Germany's IT security law has significantly improved its ability to respond to emerging cyberthreats. In contrast, Afghanistan's IT law was enacted in 2007 and has not been updated since. Technology and law have not evolved in tandem.

✧ Effective laws where enforcement is positively correlated with effectiveness.

Germany and Denmark, for example, have high enforcement rates as we can see from the chart. Germany's IT security law, which emphasises the dynamic updating of infrastructure protection, contributes directly to the cybersecurity ranking. Denmark's National Cybersecurity Strategy Act excels in preventing cybercrime through cross-sectoral cooperation and preventive measures. The effective law is conceptually clear and has a clear definition of content. Multiple elements should be covered, with a focus on both technical resources and the ability to coordinate law enforcement.

✧ Ineffective laws where enforcement rates are weakly correlated with effectiveness.

For example, Denmark's law on reproduction crime prevention and control has narrow objectives and has had little effect on improving overall cybersecurity rankings. Afghanistan's information technology law has an unclear interpretation of its content and an overly vague scope that makes enforcement difficult and has a limited role in addressing cybercrime. Ineffective legal mechanisms are mainly reflected in the reliance on a single objective and the failure to provide a clear explanation of concepts, which leads to difficult law enforcement, dispersal of resources in secondary areas, and neglect of the overall prevention and control of major cybersecurity risks.

4.3 The temporal importance of the policy

The rationality of the implementation policy. It plays a key role in the effectiveness of the policy. Myanmar, for example, started its policy late and faced the problem of insufficient resources, which led to its extremely serious cybercrime. Germany, on the other hand, has achieved significant results through long-term planning-type policies that have been accumulated over the years.

The timeliness of policy adjustments directly affects the long-term effectiveness of the policy. Germany it security law through regular updates, effective response to emerging threats, covering the current emerging forms of cybercrime, and the use of the latest scientific and technological means to combat cybercrime. Afghanistan's law has not been updated to adapt to the current rapidly changing network environment.

Timely introduction of international co-operation is needed to solve the problem of transnational crime. China, for example, has actively participated in international co-operation to combat transnational cases and achieved effective results. Myanmar, on the other hand, is a late starter and has insufficient resources.V. Task 3

Ⅴ. Task 3

5.1 Random Forest Model

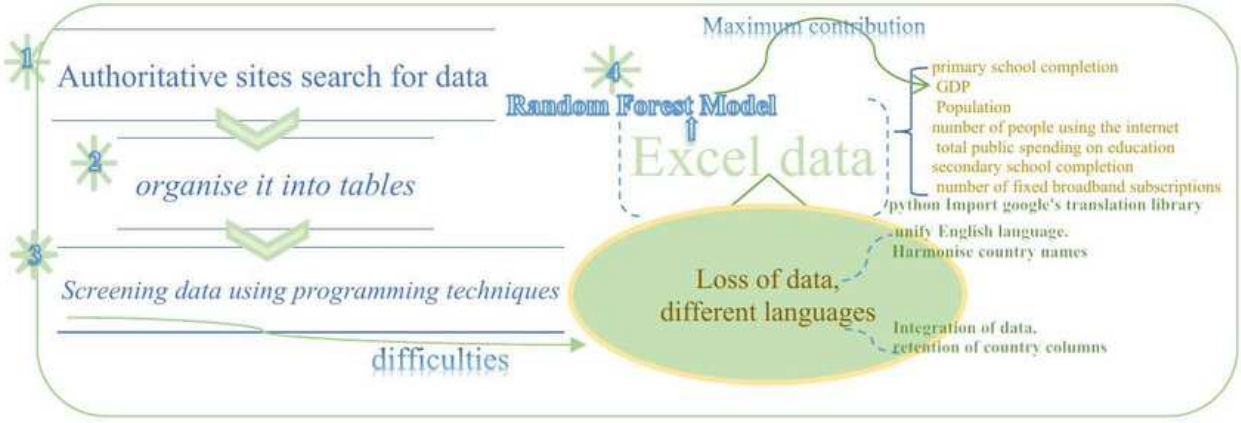


Figure 6. The flow chart of task 1

One of the questions in the competition was which national demographics (e.g. internet access, wealth, education level, etc.) are relevant to your analysis of the distribution of cybercrime? In order to work out which are the most important factors affecting cybersecurity and which contribute the most to cybersecurity, we investigated the last four years of data on primary school completion rates, GDP, population, number of people using the internet, total public spending on education, secondary school completion rates, number of fixed broadband subscriptions, and secure internet servers for each country and consolidated the data on a single Excel.

Below we use the Random Forest model to begin our analysis process.

- Data preparation

Firstly, make sure that all data are clear and error-free, especially when merging. We merged files from different sources into one dataset (merged_data.xlsx).Make sure that there are no missing values or invalid rows in the data, especially columns that are important for the regression analysis.

- Data cleansing

After merging the data, the data needs to be cleaned. Remove rows that contain missing values, especially those with missing values for the target variable (Tier Performance) to avoid affecting the regression model.Keep only those rows that have complete data in each column to ensure the validity of the data.

- Characteristics and target variables

Determine which columns are input features (X) for the model and which are predictive targets (Y).
Input feature (X): remove the Country Name and Tier Performance columns from the dataset as they are not used to train the model.
Target Variable (Y):Select the Tier Performance column as the target variable.

- Training the model

Use a regression model to fit the data:

Use a random forest regression model or another regression algorithm. Random Forest Regression was chosen here, as it automatically handles non-linear relationships between features.Then train the

model by the fit() method.

- Evaluating Model Effectiveness

Once the regression model has been trained, the following metrics are used to assess the performance of the model:

Mean Square Error (MSE): The squared average of the difference between the predicted value and the true value, the smaller the value the better the model.

R^2 Score: Measures the goodness of fit of the model, with values close to 1 indicating a very good fit.

- Analysis of regression coefficients

Look at the regression coefficients of the model to understand the effect of different characteristics on the target variable:

Some coefficients are zero, meaning that these characteristics have no significant effect in the forecast.

Other non-zero coefficients mean that these characteristics have some effect on Tier Performance's predictions, and the magnitude of the regression coefficients reflects their significance.

The code implementation and results are viewed in Appendix at the end of the paper.

- Interpretation of results

Both the Mean Square Error (MSE) and R^2 show the efficiency of the model, with R^2 close to 1, indicating that the model explains the data well. The analysis of the coefficients reveals which features are important for prediction, so that the data can be optimised or the model can be further adjusted.

Note: Random Forest Regression is an integrated learning algorithm that improves the accuracy of predictions by constructing multiple decision trees and combining the predictions from each tree.

Predicting the Tier Performance of countries, identifying the important factors that affect the performance of countries and providing data to support decision making.

Using the class RandomForestRegressor implements the Random Forest Regression model. The main features of this model are:

- Integrating multiple decision trees: reduces overfitting and improves generalisation by constructing multiple different decision trees.
- Handle non-linear relationships: Capable of capturing complex non-linear relationships between features.
- Robust: strong robustness to missing data and noise.

(Robustness is the ability of a system, model, or algorithm to maintain stability and reliability of its performance in the face of input data, environment, or parameter uptake. Simply put, it is the ability of a system or algorithm to resist changes or disturbances.)

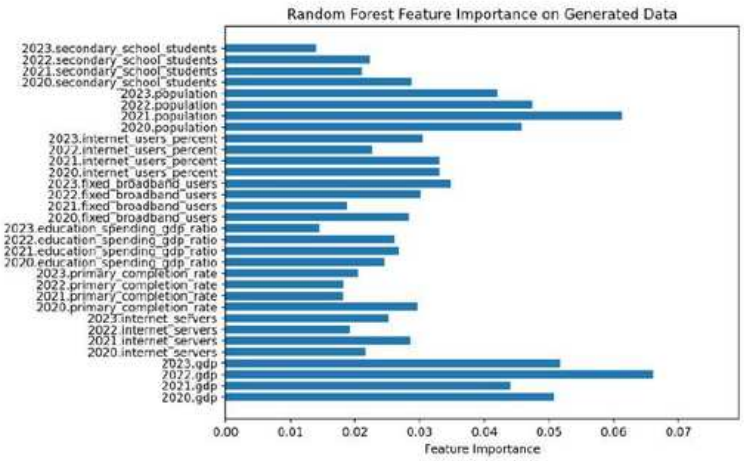


Figure 11. Random Forest Feature Importance on Generated Data

We can clearly see from figure 2 that for the four years from 2020 to 2023, GDP and population contribute the most to cybersecurity, especially GDP. total public spending on education has a smaller impact. So we conclude that GDP is crucial in maintaining cybersecurity.

References

[1] Journal | [J] Food Research International. Volume 202 , Issue . 2025. PP 115728-115728

[2] Journal | [J] Journal of Hydrology: Regional Studies. Volume 57 , Issue . 2025. PP 102194-102194

[3] Journal | [J] Dynamic Games and Applications. Volume , Issue prepublish . 2024. PP 1-34

[4] ournal | [J] Arabian Journal for Science and Engineering. Volume , Issue prepublish . 2025. PP 1-15

[5] Wang, J., & Ni, J. (2009). *Dolmetschen im Rechtsbereich. Teil 2*. https://doi.org/10.17875/gup2009-457

[6] Civilstyrelsen. (n.d.). *Retsinformation*. Retsinformation. https://retsinformation.dk/

[7] *HTTP Server Test Page powered by CentOS-WebPanel.com*. (n.d.). http://moj.gov.af/

[8] *Myanmar National Portal*. (n.d.). http://www.myanmar.gov.mm/

Appendix

```
import pandas as pd
from sklearn.ensemble import RandomForestRegressor
from sklearn.model_selection import train_test_split
from sklearn.metrics import mean_squared_error, r2_score

data = pd.read_excel('merged_data.xlsx')

data_clean = data.dropna(subset=['Tier Performance_Y'])

X = data_clean.drop(columns=['Country Name', 'Tier Performance_Y'])

Y = data_clean['Tier Performance_Y']

X_train, X_test,Y_train, Y_test = train_test_split(X, Y, test_size=0.2, random_state=42)

model = RandomForestRegressor()

model.fit(X_train,Y_train)

Y_pred = model.predict(X_test)

mse = mean_squared_error(Y_test, Y_pred)
r2 = r2_score(Y_test, Y_pred)

print("regression coefficient:", model.feature_importances_)
print("mean square error (MSE):", mse)
print("R^2 fraction:", r2)
```

The results are as follows:

Feature Importances: [0.01878759 0.03361009 0.03081568 0.02885512 0.03575278 0.03431383
 0.01812183 0.02212607 0.10168476 0.10671993 0.1301746 0.10189934
 0.03513317 0.03880588 0.02420054 0.03157658 0.02956702 0.02295208
 0.03212751 0.03286053 0.02528147 0.02441691 0.01599872 0.02421797]
Mean Squared Error (MSE): 0.3459904000000001
R^2 Score: 0.8270048

Report on Use of Al

1. OpenAI ChatGPT (JAN 24, 2025, version, ChatGPT-4o)
   Query1: <Where to find the Criminal Code of Afghanistan>
   Output: <To find the Criminal Code of Afghanistan you can try the following ways:

- Afghan government websites usually publish the country's legal documents, but since Afghanistan's legal information websites may not be as comprehensive as those of other countries, you can try to visit the official websites of the Afghan government or the judiciary to see if there are any publicly available legal documents. The official website of the Afghan Ministry of Justice or the official website of the Afghan Parliament may provide relevant legal documents and regulations. >

2. OpenAI ChatGPT (JAN 24, 2025, version, ChatGPT-4o)

Query1: <Where can I find the German Cybersecurity Act>.

Output: ChatGPT said:< (1) Gesetze im Internet website: this is the official legal database provided by the German government with all German legal texts, including the Cybersecurity Act. You can access it via the following link: Gesetze im Internet - BSI-Gesetz

(2) the website of the German Federal Office for Information Technology Security (BSI): as the implementing agency of the Cybersecurity Act, the German Federal Office for Information Technology Security (BSI) will also have detailed information about the Act and related releases on its website: BSI official website

(3) academic resources and legal databases: if you are accessing legal databases (e.g. Westlaw, LexisNexis), detailed versions of the Cybersecurity Act will usually be available as well, especially for research involving European or international law.

(4) English translation: If you need an English version of the Cybersecurity Law, try searching for some legal translation platforms, or relevant international legal service websites, which may also provide translated versions. If you need more specific provisions or contents, feel free to let me know! >