Computers & Security 120 (2022) 102820

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Attributes impacting cybersecurity policy development: An evidence from seven nations

Alok Mishra[a,b,*], Yehia Ibrahim Alzoubi[c], Memoona Javeria Anwar[d], Asif Qumer Gill[d]

[a] *Informatics and Digitalization, Molde University College—Specialized University in Logistics, 6410 Molde, Norway*
[b] *Department of Software Engineering, Atilim University, Ankara 06830, Turkey*
[c] *Management Information Systems Department, College of Business, American University of the Middle East, Egaila 15453, Kuwait*
[d] *School of Computer Science, The University of Technology Sydney, 15 Broadway, Ultimo, NSW 2007, Australia*

ARTICLE INFO

Article history:
Received 28 April 2022
Revised 24 June 2022
Accepted 28 June 2022
Available online 30 June 2022

Keywords:
Cybersecurity
Policy
Cyberspace
Infrastructure
Protection
Security
Threats

ABSTRACT

Cyber threats have risen as a result of the growing usage of the Internet. Organizations must have effective cybersecurity policies in place to respond to escalating cyber threats. Individual users and corporations are not the only ones who are affected by cyber-attacks; national security is also a serious concern. Different nations' cybersecurity rules make it simpler for cybercriminals to carry out damaging actions while making it tougher for governments to track them down. Hence, a comprehensive cybersecurity policy is needed to enable governments to take a proactive approach to all types of cyber threats. This study investigates cybersecurity regulations and attributes used in seven nations in an attempt to fill this research gap. This paper identified fourteen common cybersecurity attributes such as telecommunication, network, Cloud computing, online banking, E-commerce, identity theft, privacy, and smart grid. Some nations seemed to focus, based on the study of key available policies, on certain cybersecurity attributes more than others. For example, the USA has scored the highest in terms of online banking policy, but Canada has scored the highest in terms of E-commerce and spam policies. Identifying the common policies across several nations may assist academics and policymakers in developing cybersecurity policies. A survey of other nations' cybersecurity policies might be included in the future research.

1. Introduction

Almost every nation now relies heavily on the digital sector. In cyberspace, which refers to the virtual world of computers, the free-flowing information around the network in computers is a topic of fascination (Libicki, 2021). The growing usage of the Internet and cyber-based technologies for nearly everything has resulted from the fast growth of information and communications technology (ICT) and the worldwide digital transformation (Eriksson and Giacomello, 2022). Citizens, organizations, and governments are the primary users or actors in cyberspace. The growing popularity of Cloud computing, ICT, internet of things (IoT), and smartphones has led to a new ecosystem of human-technology interaction (J. Lippert and Cloutier, 2021).

Cyber threats have risen as a result of the growing trend of digitization and excessive reliance on the digital world (Mohan et al., 2020). The risk posed by cybercriminals who use cyberspace for their gain by exploiting people's information, property, operations, and other digital assets is known as a cyber threat (Paananen et al., 2020). Governments' increasing reliance on the Internet for essential state services (e.g., E-government services, etc.) has made it an appealing target for cybercriminals (Mishra et al., 2022). Cyber threats are motivated by a variety of factors, including the collection of sensitive information, harm to a country's sovereignty, ideological grounds, or other state-level crimes (Roshanaei, 2021). Because of the exponential rise of online activities, more hackers, cybercriminals, and terrorists can target valuable assets and critical social and governmental infrastructures, posing a threat to cyberspace security and stability (Gandhi et al., 2011). Critical infrastructure is the target of the most prevalent and disruptive cyber-attacks (Anwar and Mahmood, 2018). Regardless of the form of cyber threats, prompt and adequate response policies are essential (Ibrahim et al., 2020). As a result, Cybersecurity (CS) may be of national or worldwide concern (Hatcher et al., 2020). CS is defined as a set of security concepts, policies, tools, guidelines, risk management techniques, best practices, and training that may be utilized to secure an organization's cyber

[*] Corresponding author.
E-mail addresses: alok.mishra@himolde.no (A. Mishra), yehia.alzoubi@aum.edu.kw (Y.I. Alzoubi).

https://doi.org/10.1016/j.cose.2022.102820

Table 1
List of abbreviations used in the article.

Abbreviation	Definition	Abbreviation	Definition
ACSC	Australian Cyber Security center	FISS	Fraud Intelligence Sharing Systems
APRA	Australian Prudential Regulatory Authority	GDPR	General Data Protection Regulations
BIC	Bank Identifier Code	HIPAA	Health Insurance Portability and Accountability Act
CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography and Marketing Act	IASP	Internet Access Service Provider
CASL	Canada's Anti- Spam Legislation	ICT	Information and Communications Technology
CCA	Controller of Certifying Authorities	IEEE-SA	IEEE Standards Association
CISP	Cyber Information Sharing Partnership	IoT	Internet of Thing
CMA	Communications and Multimedia Act	ISAC	Information Sharing and Analysis Centers
CNCI	Comprehensive National Cybersecurity Initiative	ISM	Information Security Manual
CNII	Critical National Information Infrastructure	ISMF	Information Security Management Framework
CPA	Consumer Protection Act	IT Act	Information Technology Act
CRPL	Consumer Rights Protection Law	NCSS	National Cyber Security Strategy
CSIRT	Cybersecurity Incident Response Teams	NEP	National Encryption Policy
CS	Cybersecurity	NIS	Network and Information Security
CPR	Cyberspace Policy Review	NCSP	National Cyber Security Policy
DoS	Denial of Service	PIPEDA	Personal Information Protection & Electronic Documents Act
EC3	European Cyber Crime center	PPP	Public–Private Partnership
EISA	Energy Independence and Security Act	SAFE	Security and Freedom through Encryption
ENISA	European Network and Information Security Agency	SERC	State Electricity Regulatory Commission
ESIGN	Electronic Signature in Global and National Commerce Act	SGA	Smart Grid Australia
ETA	Electronic Transactions Act	SWIFT	Society for Worldwide Interbank Financial Telecommunications
EU	European Union	TA	Telecommunication Act
Fire	Firefox for Incident Reporting	UECA	Uniform Electronic Commerce Act
FISMA	Federal Information Security Management Act	UETA	Uniform Electronic Transactions Act

environment and assets (ITU 2022). To mitigate risks and vulnerabilities, CS employs a variety of policies. Due to rising rates of espionage, loss of key information, and hostile cyber-activity, practically all governments want safe cyberspace (Buja, 2021). However, traditional methods of practicing CS are insufficient (Graham et al., 2016). Holistic policies for the CS system across the nation, across ecosystems, and in its infrastructure are required (Libicki, 2021).

The lack of a credible CS policy has caused many companies in many nations to fail to counter cyber-attacks (K.J. Lippert and Cloutier, 2021). This study was inspired by this reality. Cyber-attacks have been more common in recent years, forcing several governments to implement legislation and regulations to enhance their CS (Khan et al., 2022). For example, one of the most essential steps to enhance CS is the implementation of the general data protection regulations (GDPR) in Europe (The-European-Parliament-Council 2016). Despite these attempts, identity theft, data breaches, account takeover, and other cyber-attacks are on the rise every year (Dalal et al., 2022). The main reason for this is that each country has its own set of policies. Given this heterogeneity, it is very costly and difficult for organizations to comply with all policies (Mishra et al., 2022). The lack of a generally acknowledged and clear definition of cyber hazards is the biggest impediment to forging a worldwide consensus on CS (Wu and Irwin, 2016). To better comprehend the arc of CS policies and to overcome the variety of CS policies, this paper focuses on identifying and exploring the use of the fundamental attributes that influence the development of CS policies in various nations. There is a scarcity of research examining CS policy, and hence, this paper addresses this gap by answering the following research question.

RQ: How do different nations implement CS policies to address critical CS attributes?

In this paper, previous studies, research publications, and publicly available policy documents are evaluated and assessed comprehensively across seven nations: Malaysia, Australia, the USA, China, Canada, India, and the European Union (EU). This was essential to investigate how these governments handle key CS aspects such as policy process, policy information, cyber threats identification, and policy instruments. The following are the major contributions of the paper: To begin, this paper explores the different laws and regulations and their purposes developed in these nations. This was essential to identify the common attributes of CS deployed in different nations. This will not only assist nations in improving their CS policies in the future, but it will also serve as a useful benchmark for comparing CS policies in various nations. Moreover, this paper identified a set of essential CS attributes that meet the current requirements to protect cyber-activities. These attributes include telecommunication, network, Cloud computing, E-commerce, online banking, smart grid, consumer rights, cybercrime, national encryption, privacy, identity theft, digital signature, data security, and spam. These findings will assist academics and policymakers in paying close attention to the attributes that are crucial for the formulation of CS policy frameworks. Also, the findings will assist new scholars and policymakers in ICT-growing nations in broadening their perspectives to improve CS.

Table 1 summarizes the abbreviations that appeared in this article. The rest of this article is organized as follows. Section 2 provides the background of the study and highlights the related work. Section 3 details the methodology used to conduct this research followed by Section 4 where results are presented, and the research question is addressed. Section 5 discusses the findings, limitations, and future directions, and Section 6 concludes this article.

2. Background and related work

This section provides background information and literature on the research problem. First, the reasons for investigating the selected nations are discussed. Then, we'll highlight the rising cybercrimes, factors impacting the rate of cybercrimes, and the role of governments in improving CS.

2.1. Selection of nations

The nations selected in this study have suitable cyberspace security legislations. Furthermore, these countries have sufficient data for cyber-security concerns and policies. Therefore, their policies can serve as a model for developing a complete strategy. The selection process was due to the following reasons.

- The USA has a large number of Internet users. The majority (more than 300 million) of the population has access to the Internet, and this number is steadily rising (Statista 2022). Because this country's internet economy is worth a trillion dollars, it has a well-developed cybersecurity strategy (Chukwu and Idoko, 2021).
- The EU is comprised of some of the world's wealthiest and most industrialized nations, where the majority of the people use the Internet. The Internet is utilized for a wide range of purposes, and as a result, they confront a variety of security risks. Accordingly, cybersecurity policy is also highly comprehensive (Laurer and Seidl, 2021).
- Australia has more than 20 million internet users, a huge student population, and millions of visitors each year. It indicates that Australia's cybersecurity regulations influence a large number of individuals, and the country is working to develop a faultless strategy for all types of Internet users (Miralis et al., 2022).
- With over 30 million (88 percent) Internet users, Canada is yet another developed country that has been subjected to several significant cyber-attacks, and as a result, it is one of the most cybersecurity-aware nations (Shaykevich, 2019).
- China has the most Internet users (more than 1 billion) of any country on the planet (Statista 2022). The largest E-commerce corporation in the world, without an adequate policy, a large number of individuals will be unable to utilize a variety of internet services (Wei, 2020).
- India is the world's second-largest Internet user (more than 600 million) nation (Statista 2022). Even though the internet penetration rate is modest when compared to other nations, it is among the fastest-growing IT industries in the world. It also has multiple laws addressing various cybersecurity concerns; hence it was chosen (Kethineni, 2020).
- Malaysia is among Asia's quickest growing economies. In comparison to other Asian nations, it has a fairly high rate of Internet subscribers. In Malaysia, more than 30 million of the population use the Internet (Statista 2022). Many experts have engaged in producing Malaysia's cybersecurity regulations; as a result, Malaysia has been chosen for examination (El-Muhammady, 2021).

There are a few additional nations with a substantial number of Internet users and well-developed infrastructure that were not chosen for a variety of reasons. South Korea and Japan, as examples of these countries, have a huge number of Internet users, however, the available cybersecurity materials are written in Korean and Japanese, respectively, hence it was not included in our study. Because the policies of the United Kingdom are encompassed by the policies of the EU, there is no need to describe them individually. Moreover, there was no need to include EU members individually; as a result, countries like Denmark were left off the list. New Zealand was also excluded due to its small Internet users' number, due to its tiny population. Singapore is not featured in the list since there is relatively little information regarding its cybersecurity policies available online.

2.2. The rise of the cybersecurity crimes

Cybercrime has become the most significant and severe concern, especially during the COVID-19 pandemic, according to (Lallie et al., 2021). When it comes to cybercrime, the issue isn't whether it can target national infrastructures, private businesses, or people. Hadi-Janev and Bogdanoski (Hadji-Janev and Bogdanoski, 2015) define it as how equipped the public and government institutions are to rapidly notice and control the harm. The Internet has evolved into a parallel type of existence and living today (Lloyd, 2020). The growing use of the Internet and online exchange of information is seen to be the primary cause of the rise in cybercrime. Traditionally, antimalware, and antivirus solutions are the principal choice to prevent cybercrimes (Libicki, 2021). However, the intricacy and variety of today's cybercrimes have outgrown the capabilities of traditional malware programs. As a result, the CS community considers the development of more novel and effective malware defensive systems to be a pressing issue (Mishra et al., 2022).

Cross-border cyber threats are being addressed in a variety of ways. Depending on the nature and scope of the crime, many nations have implemented different ways to combat it. In Jang-Jaccard and Nepal (J. Jang-Jaccard and Nepal, 2014), new attack approaches resulting from rising technology such as cellphones, Cloud computing, social media, and critical infrastructure were examined. Hackers pose a threat to an organization's information resources' security. The key situational elements that induce information security policy breaches were found by Johnston et al. (Johnston et al., 2016). Anwar and Mahmood (Anwar and Mahmood, 2018) highlighted several current cyber-attack-related transgressions. Limiting cyber-attacks on companies and governments requires effective information sharing and coordination during incident resolution. Because the limited known methods for preventing cyber-attacks were insufficient, the information sharing and analysis centers (ISAC) and cybersecurity incident response teams (CSIRT) developed innovative techniques for reporting and coordinating incidents. Also, Firefox for Incident Reporting (Fire) was established to organize incident information exchange with CSIRTs consistently throughout the incident resolution process (Libicki, 2021). In addition, the fire included capabilities for secure communication, sensitive information labeling, real-time interaction with handlers and analysts, and a database of stakeholder points of contact (Bahuguna, 2015). Maghu et al. (Maghu et al., 2014) reviewed many studies and identified strategies for dealing with escalating cyber risks. All of the research cited above concentrates on individual aspects of cybercrime and does not sufficiently address the complexities of building a holistic CS strategy. This study builds on prior research on the theoretical foundations of this multifaceted subject, demonstrating that the need for a complete approach to CS policy creation may be realized through a series of phases, each focusing on a distinct aspect.

2.3. Factors impacting the rate of cybercrimes

With the increasing frequency of cyber-attacks in recent years, policymakers and governments all across the world continue to raise concerns (Muhammad and Kandil, 2021). Cyber threats are a worldwide and national concern that transcends borders (Paananen et al., 2020). One cause for the rise in cyber threats is that CS policies are not established with a global view in mind. Understanding other nations' tactics is critical to put the ever-changing CS landscape into context. Furthermore, most nations' CS policies place a strong emphasis on the larger picture, such as national security, health care, and national defense (Rajaretnam, 2020). The issue emerges when smaller units are overlooked, such as when the human aspect of CS is neglected. Because of this lack of interest in individuals, state actors can easily handle the various security requirements of people in this context. The use of cyberspace for national security has a detrimental influence on global CS. To tackle this difficulty, CS policy should be strong enough and concentrate on personal information protection (Cavelty, 2014). Recognizing the human dynamics of CS is critical for analysts to expand their knowledge.

There is a severe lack of qualified experts as well as academic programs in the context of CS (Dalal et al., 2022). Various nations, like New Zealand and the USA, see this as a human capital issue (ICLG 2022). Fourie et al. (Fourie et al., 2014) examined the severity of the problem and its many aspects. They provided an examination of cyber-attack data collected by a CS research center, as well as instances and actual solutions from New Zealand. Oltramari et al. (Oltramari et al., 2014) concentrated on the prerequisites for developing a model of CS analyst decision-making. They focused on the knowledge representation and cognitive components of such a model by merging ontological and cognitive architectures in a crossbred-modeling framework while presenting the primary features of such a model. In this sense, the cognitive world, as well as the physical or digital domain, characterize cyberspace (Maung and Thwin, 2017). As a result, CS has evolved into a complex subject that needs scientific knowledge in terms of experimentally tested as well as theoretically based models (Roshanaei, 2021). Interferences with behavior change are ubiquitous in areas of human-computer interaction, but they are uncommon in the discipline of computer science. Coventry et al. (Coventry et al., 2014) offered strategies for collaborating with organizations to create social interferences. This strategy combines designing features with a set of behavior modification goals to help the researchers to collaborate to find a collection of nudges that may encourage optimal behavioral practice. They explained how a structured method was successfully used in the creation of a nudge to alleviate uneasy behaviors related to wireless network selection (Coventry et al., 2014).

Muhaya and Bakry (Muhaya and Bakry, 2010) investigated the variables that are necessary for different nations' national security strategies. The nations surveyed were the USA, Malaysia, Australia, Canada, and China (Muhaya and Bakry, 2010). Graves et al. (Graves et al., 2016) looked at how the empirical difficulties of incorrect perception were overcome, imprecise data, and missing data might impact and occasionally hurt politicians', corporations', and people's security decision-making procedures. They also investigated how these instances may be used in the context of national security. Between 2009 and 2011, Luiijf et al. (Luiijf et al., 2013) examined and contrasted 19 The national cyber security strategy (NCSS). USA, UK, Australia, Canada, France, Spain, New Zealand, Japan, Estonia, Germany, Czech Republic, Lithuania, India, Romania, Luxembourg, South Africa, Uganda, and the Netherlands were among the nations involved (Luiijf et al., 2013). This study provided insight into the shared methods and flaws as well as recommendations to aid nations in the development of their NCSS. The entire technique for security-informed safety and hazard assessments was the emphasis in (Bloomfield et al., 2016). All of the studies mentioned above illustrated the factors that contribute to an increase in cybercrime, but none of them offer guidance on how to create effective CS policies to combat these crimes.

2.4. The role of governments in preventing cybercrimes

Governments are now attempting to enhance their preparations to combat these cyber-attacks. Governments must create dynamic means to counter these threats due to the pace and nature of technology (Lloyd, 2020). The appropriate role of nation-states in Internet administration and strengthening global CS was examined by Shackelford et al. (Shackelford et al., 2015). Governments are attempting to protect their vital infrastructure. Various nations have varying cyberspace legislation, underlining the need for citizens to find comprehensive solutions (Shackelford et al., 2015). As a consequence, the worldwide goal is to achieve a general agreement about the future of Internet administration and promote CS. A collection of nations collaborated to create the NCSS. Although each of these NCSS plans to define the same set of CS risks, the national emphasis points and techniques differ significantly (Shackelford et al., 2015). This does not imply that governments are solely responsible for CS policies due to their detrimental impact on critical infrastructure protection. Carr (Carr, 2016) reviewed several works on the private-public interaction in dealing with problems in national CS plans. The researchers discovered a significant disparity between the private and public estimates. The private sector has a reluctance to take responsibility or bear obligation for national CS (Carr, 2016). Governments' efforts to manage national CS raise challenges about how states may promote their security in the digital age (Manwaring and Hanrahan, 2019). Communities cannot grow unless a government can guarantee safe and dependable digital connectivity. As a result, more than a hundred nations have devised national CS defense policies to address CS threats (Libicki, 2021).

3. Research methodology

The research design is a combination of literature review and comparative analysis (Tranfield et al., 2003). The method for acquiring research data is divided into two phases. The first phase is doing an information search using academic resources and the Internet. The second phase is doing a focused search of security and government websites. The data is acquired using the literature review process. It draws on all accessible literature (such as journals, conferences, and white papers) to find answers to the research question. Exploratory, descriptive, and explanatory techniques are the three types of literature study methodologies. To find answers to questions involving "what" and "who," an exploratory research approach is utilized (Alzoubi and Gill, 2021). The explanatory approach, on the other hand, provides the "how" and "why" answers. The descriptive approach is used to investigate and describe a phenomenon or a series of occurrences. The literature study approach was chosen because it aids in the collection and investigation of data in the context of research. It also aids in the integration of qualitative and quantitative data, which is necessary when dealing with complex phenomena and doing in-depth studies (Alzoubi and Gill, 2020; Zainal, 2007). This study compares CS policies using a mix of these techniques. This was essential to determine how each nation's CS policy prioritizes cyber risks, as well as the responsibilities of agencies, departments, and governments in each nation in addressing CS challenges. Because this is a fast comparison study, it gives a picture of the current era and is entirely dependent on data from open-source materials. All of the information and data may be traced back to their sources.

4. Results

4.1. Cybersecurity policies in selected nations

This section covers how distinct attributes in CS policies in different nations were chosen, as well as why these nations were chosen. The common attributes of CS in seven nations are compared to see how these nations are dealing with CS concerns. The threats of CS are always changing, and the stakes are enormous (Calderaro and Craig, 2020). Governments that concentrate their efforts on the most important attributes of CS may be better able to prevent cyber-attacks, reduce their damage, and better safeguard their enterprises, residents, and key infrastructure (Rajaretnam, 2020). Table 2 summarizes the differences and similarities in the development of the CS policies among selected nations. The elaboration on them is discussed in the following sections.

4.1.1. Cybersecurity policies in USA

The current CS strategy is an upgrade of president Bush's comprehensive national cybersecurity initiative (CNCI) in 2008. Obama's administration placed CS policy among the nation's priorities, implementing the cyberspace policy review (CPR) in 2009

Table 2
Differences and similarities in the cybersecurity policies among selected nations.

Comparators	USA	EU	Australia	Canada	China	India	Malaysia
Reasons for development	Infrastructure protection	Cyber threats	E-commerce	Infrastructure protection	Infrastructure protection	Infrastructure protection	Infrastructure protection
Priority ingovernment	Major infrastructure	Top ten	Top ten	Top seven	Highest priority	Top three	Top ten
Cyber force	Proposed	No	No	No	Yes	Proposed	No
Implementation	No	Yes	Yes	Yes	Yes	Yes	Yes
Open, secure cyberspace	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Agencies involvement	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 3
Cybersecurity regulations and purposes in USA.

Law/Act	Purpose
Cybersecurity Act of 2015, Cybersecurity Enhancement Act of 2014, National Cybersecurity Protection Act of 2014, Cybersecurity Workforce Assessment Act, CNCI	Cybercrime (Le and Zamora, 2018)
Cyber Privacy Fortification Act of 2015	Privacy (Baadsgaard, 2022)
Identity Theft and Assumption Deterrence Act	Identity theft (Sabol, 1999)
USA Anti-Terrorist Laws and International Business & Trade Creation of CSI ports	E-Commerce (Odoyo, 2010)
Electronic Signature in Global and National Commerce Act (ESIGN), Uniform Electronic Transactions Act (UETA)- adopted by 48 states	Digital signature (WhiteHouse 2022)
Payment Card Industry Data Security Standard (PCI DSS), HIPAA, the Sarbanes-Oxley Act, FISMA, and Children's Online Privacy Protection Act of 1998	Cloud computing data security (Baadsgaard, 2022)
Protecting Cyber Networks Act	Network security (Harrop and Matteson, 2014)
Telecommunications Act of 1996	Telecommunication (WhiteHouse 2022)
Data Security Act and Breach Notification Act	Data security (Le and Zamora, 2018)
SAFE ACT, Secure Public Networks Act	Encryption (Spitzer, 2014)
Federal Trade Commission Act, Federal Food, Drug, and Cosmetic Act, Fair Debt Collection Practices Act, Fair Credit Reporting Act, Truth in Lending Act, Fair Credit Billing Act, and the Gramm–Leach–Bliley Act	Consumer rights protection (FTC 2022)
EISA of 2007	Energy (Westhoff, 2008)
CAN-SPAM Act 2003	Assault of non-solicited pornography (Kigerl, 2009)

(WhiteHouse 2022). In CPR, 10 short-term and fourteen mid-term activities are specified. The USA administration used September 11th as a springboard to enhance the cyber threat by encompassing significant infrastructure and handling it as if it were a public safety issue. The essential CS infrastructure was then established in February, focusing on developing a framework for reducing cyber threats (WhiteHouse 2022). Government intervention in CS policy and public-private partnership (PPP) in the USA is a self-regulation optional responsibility. Because certain elements of CS legislation overlap with other laws, it is not yet fully stated. The USA government is attempting to shift from optional to compulsory regulations (Baadsgaard, 2022). Table 3 summarizes the cybersecurity laws and acts and their purposes in the USA.

4.1.2. *Cybersecurity policies in EU*

Europe is well ahead of the rest of the world in terms of CS innovation. The EU's organizational structure is a cooperative actor attempting to establish itself as a strategic player in a linked world. Other actors around the globe, on the other hand, are attempting to shift global concerns to address several security-related challenges that necessitate sophisticated and progressive steps to secure their existence (Gijrath et al., 2018). The necessity for CS has grown as the number of online assaults has increased. The kind and frequency of hostile intrusions into cyberspace nowadays vary. It becomes imperative to investigate the EU's plans or measures for preventing cyber-attacks (Van der Meulen et al., 2022). In 2013, the EU issued a CS policy as well as a proposal for a network and information security (NIS) Directive, recognizing the threat of cybercrime. The European Cyber Crime center (EC3) assists in the protection of European citizens and businesses by assisting criminal surveys and raising awareness of emerging trends in cyber-attack operations (Sarma, 2022). In the EU's legislation, information security was highlighted as a critical concern, highlighting the possible hazards connected with the extensive use of ICT. Information security may be used to safeguard and avoid threats, as well as to make it easier for users to comply with certain legal obligations (Fuster and Jasmontaite, 2020). Table 4 summarizes the cybersecurity laws and acts and their purposes in the EU.

4.1.3. *Cybersecurity policies in australia*

For two reasons, the Australian government views the CS as a critical policy topic. The first is concerned with the human impact and financial cost of cybercrime on Australian persons and enterprises (Manwaring, 2009). The second reason is that the cyber threat has a significant impact on ICT because of the high levels of reliance that Australians have, both communally and personally on ICT[80]. Accordingly, the australian cyber security center (ACSC) developed the information security manual (ISM). Borgman et al. (Borgman et al., 2015) interviewed people with officials of several government departments to determine whether current methods are enough for implementing ISM and sorting data for the relevant South Australian government organizations. They identified the major topics that the South Australian state should look into in the stages of the information security management framework (ISMF) that have been done by other Australian states (Rajaretnam, 2020). In 2009, the Australian government released its CS strategy. In addition, the Australian federal government has suggested and put forward several regulations for recognizing, investigating, regulating, and punishing crimes and illegal behaviors in cyberspace. Furthermore, Australia's public institutions, governmental, and non-governmental organizations have played an important role in protecting CS while also lowering the prevalence of cybercrime (Miralis et al., 2022). Table 5 summarizes the cybersecurity laws and acts and their purposes in Australia.

4.1.4. *Cybersecurity policies in canada*

Bailetti et al. (Bailetti et al., 2013) stated that they created an engine consisting of five structures: a project society, an

Table 4
Cybersecurity regulations and purposes in EU.

Law/Act	Purpose
CISP, ENISA	Cyber protection (Murdoch, 2021)
EU's Data Protection Directive	Privacy (Birnhack, 2008)
Criminal Code	Identity theft (Faure, 2017)
Use of FISS and SWIFT Laws, and Safe Harbour	Online banking (Fuster and Jasmontaite, 2020)
Electronic Commerce Directive 2000	E-commerce (Lodder and Murray, 2017)
EU Directive for Electronic Signatures (1999/93/EC), EU VAT Directive	Digital signature (Pappas, 2002)
Data Privacy Directive and the future of EU Cloud computing	Cloud computing data privacy (Kontargyris, 2018)
NIS Directive	Network Security (Katulić, 2018)
Telecommunications Act	Telecommunication (Vogelsang, 2015)
EU Data Protection Regulation 2018	Data security (Goddard, 2017)
EU Data Protection Regulation	National encryption (Goddard, 2017)
Data Protection Directive, European General Data Protection Regulation 2014	Consumer rights (Weatherill, 2013)
Directive (2002/58/EC) on Privacy and Electronic Communications	Electronic communication (Gijrath et al., 2018)
Directive 2001/77/EC, Directive 2003/54/EC, Green Paper 2005, Directive 2006/32/EC, COM (2007) 723 final. Directive 2009/72/EC, Conclusions of the European Council 2011. Commission Recommendation on Preparations for the Roll-out of smart metering systems (C/2012/1342), EC standardization mandate for smart meters (M/441) EC standardization mandate for electric vehicles, (M/468) EC standardization mandate for smart grids (M/490)	Smart grid (Iqtiyanillham et al., 2017)

Table 5
Cybersecurity regulations and purposes in Australia.

Law/Act	Purpose
TA 1997, Cybercrime Act 2001, Broadcasting Services Amendment (Online Services) Act 1999, Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022	Cybercrime (AustralianHomeaffairs 2022)
Australian National Privacy Act of 1988 (amended 2014, Enhancing Privacy Protection Act 2012 (Privacy Amendment), Australian Prudential Regulatory Authority (APRA), Australian Government Agencies Privacy Code 2017	Privacy (Bennett Moses et al., 2019)
Criminal Code Amendment (Theft, Fraud, Bribery, and related offenses) Act 1999, Financial Transaction	Identity theft (Kyriakakis, 2007)
ETA 1999, Capital Territory - ETA 2001, New South Wales- ETA 2000, Northern Territory- ETA 2000, Queensland- ETA 2001	Electronic transaction (Webb, 2007),
E-Payments Code	E-payment (White, 2007)
2015 Cloud Computing in Australia market report	Cloud computing data security (Manwaring and Hanrahan, 2019)
Cybercrime Act	Network security (Chan et al., 2003)
Telecommunications Act 1979 (Interception and Access)	Telecommunication (Nicholls, 2012)
Privacy and Data Protection Act 2014	Data security (Watts and Casanovas, 2019)
Cybercrime Act 2001	National encryption (Brookes, 2022)
Spam Act 2003	Spam (Manwaring, 2009)
Australian Consumer Law	Consumer rights (Malbon and Nottage, 2013)
Green Energy Act	Green energy (Haidar et al., 2015)

Table 6
Cybersecurity regulations and purposes in Canada.

Law/Act	Purpose
PIPEDA 2000, PIPEDA 2005, Protecting Canadians from Online Crime Act 2014	Online security (Jaar and Zeller, 2008; Lukings and Lashkari, 2022)
PIPEDA	Privacy (Jaar and Zeller, 2008), Cloud computing data security (Phillips, 2018),
PIPEDA 2005 (S-4), An Act to amend the Criminal Code	Identity theft (Jaar and Zeller, 2008)
E-Payments Code, SSL, Chip and Pin policy	E-payment (King, 2012)
Uniform Electronic Commerce Act (UECA), PIPEDA 2000	Digital signature (Weiland, 2001)
National Defense Act	Network security [(Bell, 2006), 2006]
Telecommunications Act	Telecommunication (Frieden, 2005)
Canadian State Council Directive No. 273	Data security (Phillips, 2018)
Criminal Code's Lawful Access Powers	National encryption (Perrin, 2009)
Spam Act, CASL 2014	Spam (Shaykevich, 2019)
CPA 2002, S.O. 2002	Consumer rights (Piché and Saumier, 2018)
Green Energy Act	Green enrgy (Streich, 2010)

ecosystem, an exterior community, an organization, and a stage, in order to boost the performance and ability of Canadians. Resource flows, strategic aim, organizational consensus, and governance bind these structures together. This engine is expected to boost the number of Canadian enterprises expanding abroad into CS markets, which may be called a new vision for the national cyber security policy (NCSP) [(Bell, 2006), 2006]. Canada is now regarded as one of the most digitally advanced nations in the world, with nearly all official and commercial entities relying on the Internet. It is reasonable to conclude that the CS's issues are mostly tied to the state of the ICT sector (Phillips, 2018). Table 6 summarizes the cybersecurity laws and acts and their purposes in Canada.

4.1.5. *Cybersecurity policies in china*

China is in a similar situation as Canada. China has made significant development in ICT, but as a new consumer of these technologies, it is still a long way behind established nations (Feng, 2019). China is not in a high position in terms of CS policies, but it will overcome this difficulty soon. This is quite likely to happen if China's interest in CS policy grows

Table 7
Cybersecurity regulations and purposes in China.

Law/Act	Purpose
Draft Cybersecurity Law (July 2015), draft Network Data Security Management Regulation 2021	Online security (Huld, 2022)
Antiterrorism Law (effective January 2016), National Security Law (July 2015)	Terrorism (Chen and Sun, 2021)
CRPL	Privacy (Swartz, 2007)
Criminal Code Network Security Law	Identity theft (Feng, 2019)
BIC	Online banking (Austin, 2018)
Chinese E-Commerce Law	E-commerce (Huang and Li, 2019)
Electronic Signature Law of the People's Republic of China	Digital signature (Wang and Wang, 2005)
China's Cloud Computing Regulations	Cloud computing data security (Parasol, 2018)
Network Security Law	Network security (Parasol, 2018)
Telecommunications Regulations of the People's Republic of China	Telecommunication (Subsorn and Limwiriyakul, 2012)
Regulations on the Administration of Commercial Encryption, State Council Directive No. 273	National encryption (Fujikawa, 2013)
China Consumer Protection Law (Amendments 2014)	Consumer rights protection (Wei, 2020)
Amendment of the Renewable Energy Law (2009), State Electricity Regulatory Commission (SERC)	Renewable energy (Brown et al., 2018)

Table 8
Cybersecurity regulations and purposes in India.

Law/Act	Purpose
IT Act 2000 (amended 2006 and 2008)	Online security (Sumanjeet, 2010)
Privacy Protection Bill	Privacy (Rajvanshi and Singhal, 2016)
Act 2000 (Section 66C - Punishment for identity theft)	Identity theft (Kethineni, 2020)
CPA 1986 S.43A of the Indian Technology Act 2000, IT Act	E-commerce (Prasad et al., 2016)
IT Act 2000	Digital signature (Sumanjeet, 2010)
CCA	Cloud computing data security (Srikanth and Dhanapal, 2011)
IT Act 2000	Network security (Dalei and Brahme, 2014)
Telecom Regulatory Authority Indian Act-1997	Telecommunication (Kumar et al., 2018)
PPB	Data security (Patel and Conners, 2008)
IT Act 2000, NEP 2015	National encryption (Mohanty, 2019)
CPA 1986 and National Consumer Disputes Redressal Commission	Consumer rights (Patidar, 2013)
IEEE Standards Association (IEEE-SA)	Smart grid (DSCI 2022)

(Subsorn and Limwiriyakul, 2012). China is committed to Internet development and has achieved significant progress. China also works to create cyberspace that is secure, accessible, friendly, and helpful (Feng, 2019). Kshetri (Kshetri, 2013) proposed a categorization, classification, and typology of cybercrime in China, which may be useful in deciphering cybercrime organizations and possible offenders' structures, personal traits, manners, and outlines. They could provide a comprehensive overview of the key features of cybercrime in China. Table 7 summarizes the cybersecurity laws and acts and their purposes in China.

4.1.6. Cybersecurity policies in india

In the area of CS policies, India is an example of a nation that lacks comprehensive plans. Cyber-attacks cause significant harm and put vital infrastructure at risk (Prasad et al., 2016). The poor distribution of fundamental skills required in a knowledge-based society is certainly due to a shortage of development in the ICT industry, which inhibits tapping the yet-untapped inventive potential of huge young Indian people resources (Bilbao-Osorio et al., 2014). In July 2013, India's government released the NCSP, which outlined 14 objectives, including improving critical infrastructure security and training 500,000 skilled CS professionals in five years. The NCSP is a key component of the nation's PPP efforts to improve the CS scenery (Kshetri, 2013). Table 8 summarizes the cybersecurity laws and acts and their purposes in India.

4.1.7. Cybersecurity policies in malaysia

Malaysia adopted ICT as a tool for growth, increasing the usage of digital information systems in the industry, government, and the private sector (Wahid et al., 2021). However, cybercrime has put digital information systems in danger, particularly in the critical national information infrastructure (CNII). As a result, Malaysia's NCSP was established to safeguard the CNII from the threats it faces (El-Muhammady, 2021). The government and businesses' role in responding to cybercrime, the function of cyber laws, and their collaboration with traditional law to combat cybercrime, which is on the rise in Malaysia, are debated in Binti's study (Binti Mohamed, 2013). The fact that crimes increase every year prompted a lot of concern among the public and the administration (Binti Mohamed, 2013). It is difficult to prevent these crimes in Malaysia due to a lack of staff and technology (El-Muhammady, 2021). To be able to combat attacks like DoS, actual mechanisms for preventing and detecting cybercrime activity on all networks are required (Wahid et al., 2021). Table 9 summarizes the cybersecurity laws and acts and their purposes in Malaysia. Fig. 1

4.2. Attributes of cybersecurity policy in selected nations

It is not just the responsibility of IT to create efficient firewalls and security solutions; it is also the responsibility of relevant officials to enact specific regulations to make cyberspace safer (Carr, 2016). There is a scarcity of knowledge about common attributes that are crucial for the creation of CS policy (Mishra et al., 2022). This section discusses the identified attributes of CS policies across selected nations. It's worth noting that the attributes that influence CS policies aren't fixed and need to evolve to address the changing CS landscape. Further, some of the attributes could be common across different situations compared to more situation-specific specialized attributes. For instance, privacy is a generic attribute whereas spam could be related to an email or messaging capability. With the advancement of business and technology needs, these attributes may change and new attributes may emerge (Murdoch, 2021). For example, because Cloud computing services were not generally accessible a few years ago, there was no unified policy in place, but it has since grown out to be the most in-demand innovation in cyberspace (AlAhmad et al., 2021). Similarly, as technology advances, cyberspace becomes more complicated, thus a well-organized and comprehensive security policy is critical (Mishra et al., 2022). The current analysis has the ben-

Table 9
Cybersecurity regulations and purposes in Malaysia.

Law/Act	Purpose
National Cybersecurity Policy	Online security (Pătraşcu, 2018)
PDP Act 2010	Privacy, identity theft (Shahwahid and Miskam, 2015)
Digital signature Act 1997	Digital signature (Saripan and Hamin, 2011)
Cloud Computing Laws	Cloud computing data security (Pătraşcu, 2018)
CMA 1998	Network Security Laws (Hussein, 2000)
NCSP, TA 1950	Telecommunication (Abdullah et al., 2018)
PDP Act 2010	Data security (El-Muhammady, 2021)
Telecommunications Law, Internet Access Service Provider (IASP)	Spam (Wahid et al., 2021)
National Consumer Disputes Redressal Commission, CPA 1999	Consumer rights (Yusoff et al., 2012)
ASEAN Smart Grid Congress	Smart grid (Brown et al., 2018)

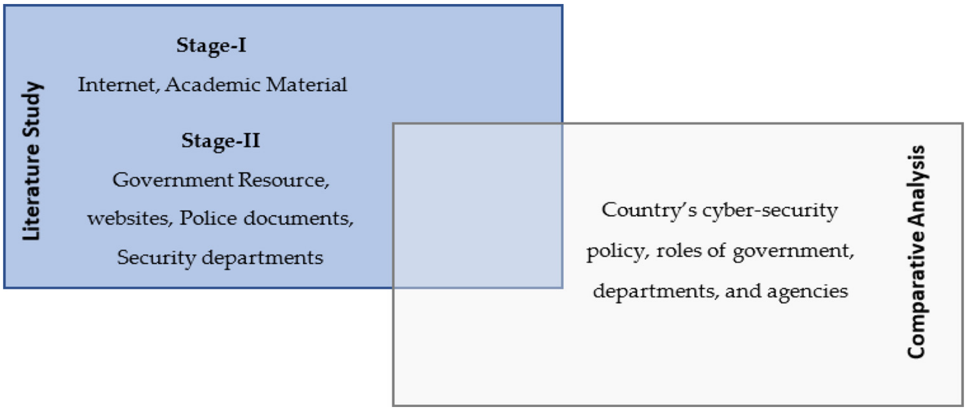

Fig. 1. Research methodology.

efit of compiling a list of attributes that have a major influence on CS policy and are common across many nations. Telecommunication, network, Cloud computing, E-commerce, online banking, smart grid, consumer rights, cybercrime, national encryption, privacy, identity theft, digital signature, data security, and spam, are among the fourteen common attributes identified in the literature, as shown in Fig. 2.

These attributes may help and guide policy improvement because a policy does not have to work for all stakeholders in all scenarios (Rosenzweig and Lieberman, 2012). All or some of these attributes can aid nations in developing a global or region-level multi-nation CS strategy, which is critical in reducing cyber-attacks and establishing safe global cyberspace or ecosystem (Knapp, 2009). These policy attributes may not only make cyberspace safer, but they may also impact a nation's economy, as marketers actively monitor various aspects of each nation's CS policy (Goddard, 2017). The relevance of these attributes among the selected nations is discussed in the next section. The common attributes of CS in seven nations are compared to see how these nations are dealing with CS concerns.

4.2.1. Telecommunication policy

Telecommunication is among the earliest actions in cyberspace, and it has undergone several adjustments as ICT advances and telecommunication infrastructure changes (Sampigethaya et al., 2011). Acts like the National CS Policy and Telecommunication Act (TA) (Crandall, 2005) are examples of regulation on this subject. These statutes ensure that every network operator follows adequate security procedures, does not harm the state in any manner, and offers greater service to all customers (Laurent, 2021). In the USA, the telecommunications legislation protects customer data under computer protection and provides it mandatory for businesses to deal with data theft concerns as a result of greater competition. The NCSP, as well as Malaysia's TA of 1950 and the EU's Telecommunications Act, establish policy efforts by changing infrastructure and enacting stronger national control laws. They've devised an integrated information system strategy in which the corporations will exchange transaction details with government enforcement authorities and will conduct frequent monitoring.

By dividing the duties of government and organizations in telecommunications data protection, the Chinese TA, the Australian Telecommunications (Interception and Access) Act, and the Indian Telecom Regulatory Authority Indian Act-1997 operate on a similar framework. The Australian Telecommunications Interception and Access Act prohibits unauthorised access to protected information. To address analogous challenges, Canada has enacted a similar telecommunications legislation. Because telecommunications are among the earliest cyber services, its rules are well-developed and standardized in comparison to other cyber services' regulations. Almost every nation has a telecommunication statute that is nearly identical to the others. New inventions such as 5 G are increasing the consumer experience, but they are also requiring revisions to the communications legislation. Because sophisticated technologies have expanded the number of clients and the sensitivity of their actions, telecommunication services security has become more important than ever (Chen and Sun, 2021).

4.2.2. Network policy

A hacked network can pose a major threat not just to the people of a nation but also to the state, according to network security regulations (Buchanan, 2011). Telecom firms must secure their systems against all types of cyber threats, including phishing, Worms, Viruses, and other similar threats (Wilson, 2014). Even terrorist acts can be carried out via a network that has been agreed upon (Li et al., 2018). Acts like the Protecting Cyber Networks Act, Cybercrime Act, and National Defense Act are the consequence of regulation in the field network in nations like the USA and Canada (Lloyd, 2020). The security of equipment in any network is determined by the network operators' standards. The EU has issued directives to give regulatory policy guidelines for network security,

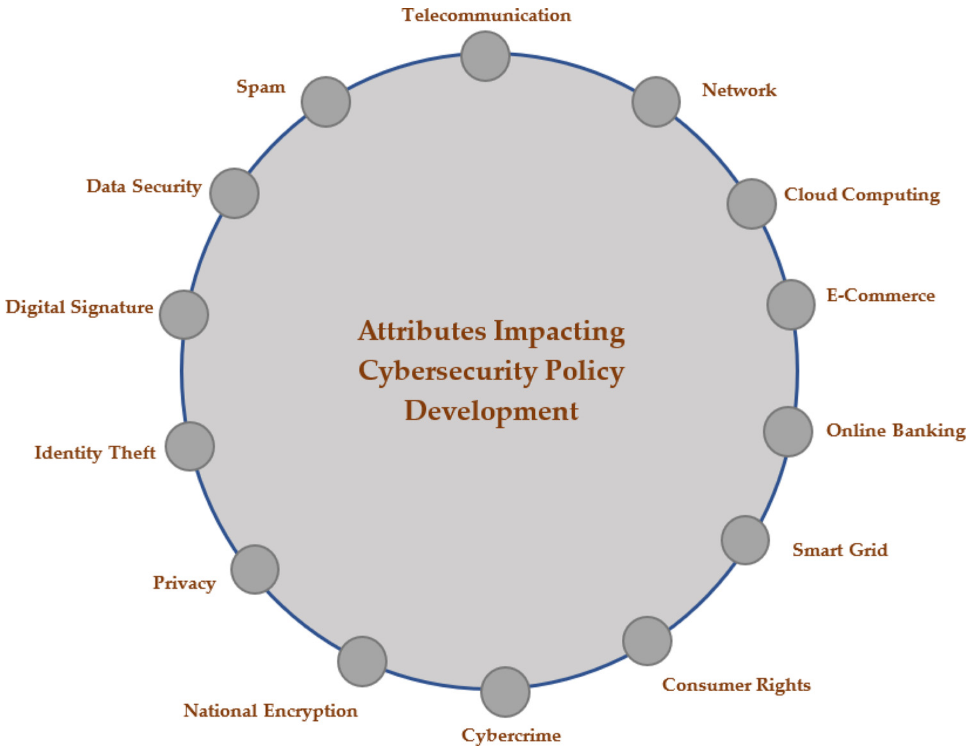

Fig. 2. Attributes impacting CS policy development.

and other nations are functioning under their own rules. The Australian Cybercrime Act identifies scams by establishing personally identifiable alarm and credit file verifying systems, which are comparable to Malaysia's Communications and Multimedia Act (CMA) 1998, which identifies scam actions by clarifying network identities and notifying regulatory authorities of fraudsters' identities (Srinivas et al., 2019).

India's IT Act of 2000, Protecting Cyber Networks Act of the USA, Canada's National Defense Laws, and China's Network Security Law all operate under network security protection by identifying various points of safeguard such as children's online privacy, phishing, access to data and DoS, concealing and demolishing data secured on networks (Parasol, 2018). These nations' legislations enable data protection networks; however, most nations, including Australia, the USA, Canada, and the EU, fall behind in providing IoT security, such as collecting personal data in a safe network location.

4.2.3. *Cloud computing policy*

The security of data in Cloud computing is especially important since many individuals and organizations depend on the Cloud (AlAhmad et al., 2021). Although Cloud computing has many advantages, its security is difficult to provide owing to its dynamic nature and relatively limited architecture (Casagran, 2016). To make Cloud computing safe, digital instruments are necessary, and the Data Signature Act is employed to accomplish this purpose (Lloyd, 2020). This act requires every service provider to provide a sophisticated digital signature mechanism to secure each customer's data in any Cloud. Users of Cloud computing services are likewise protected under the Data Privacy Act (Kumar et al., 2018). In the same way that computer security events necessitate extensive legislation to safeguard user data, Cloud-based data security necessitates comprehensive and complex laws. The Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, and the Federal Information Security Management Act of 2002 (FISMA) are all used to keep Cloud computing safe in the USA. In the EU's Data Privacy Directive and Chinese Cloud computing regulations, data protection Cloud computing legislation is linked to global perceptions, and strict rules (including not transmitting a user's private data from one country to another without that user's permission) are imposed.

The Australian National Privacy Act of 1988, as well as Malaysia's Cloud Computing Laws, ensure data protection by prohibiting organizations from disclosing private data for direct marketing purposes. The Controller of Certifying Authorities (CCA) in India, on the other hand, has built a specialized infrastructure-based tool to encrypt data. The Indian authorities are merging digital signature codes with Cloud computing to reduce fraud risk. The Personal Information Protection & Electronic Documents Act (PIPEDA) of Canada gives users additional power and allows them to manage their Cloud-based data and report fraud to the appropriate regulatory authorities. Companies in Canada, like those in the USA, Australia, and Malaysia, must protect user data by obtaining agreement from consumers before moving data from one platform to another. The entire system is responsible for Cloud security. Any flaw in any aspect of the system might expose the entire system (Alshammari et al., 2021).

4.2.4. *E-Commerce policy*

The increase in online purchasing provided by the E-Commerce Law has elevated E-commerce to a whole new level. People like the convenience of online buying platforms, but they are also a source of sensitive information theft (Badotra and Sundas, 2021). According to local rules, any firm with E-commerce capabilities must utilize an allowed payment option (Gijrath et al., 2018). E-Payment Codes give guidance to e-commerce businesses, although they are not as widely used as they are in the banking industry (Hartono et al., 2014). Privacy rules, on the other hand, provide a certain amount of protection in this area of cyberspace (Villa et al., 2018). To safeguard E-commerce related business transactions, International Business and Trade Creation of CSI ports and Anti-Terrorist Law have been adopted in the USA. Also, Australia, the EU, China, Canada, and India support E-commerce transactions through legislation such as Australia's Electronic Transaction Act 1999, the EU's E-Commerce Directive 2000, China's E-Commerce Law, and Canada's Secure Sockets Layer (SSL).

There are no laws in Malaysia that enable E-commerce; instead, businesses are supplied with a secure digital portal via which they may receive and send free payments online (Tan and Lee, 2021). This network in Malaysia is a powerful and secure system for securing transactions and lowering fraud risk to a greater level. The protection provided by EU law is strict since it establishes unified requirements for customers and businesses while also establishing a secure connection (Badotra and Sundas, 2021). Similarly, the secure connection gateways technique is used by the USA to combat fraud, although it has a different EU structure. In India, the S.43A of the Indian Technology Act, 2000 and Consumer Protection Act (CPA) 1986 give compensation to organizations that fail to secure data, which is a legal gap that allows for fraud (Basu and Jones, 2003). E-commerce regulations in India and China, both of which have large populations of Internet users, are similar in that their rules emphasize user protection by adopting anti-terrorism legislation to protect the E-commerce sector (Min et al., 2015). User protection is critical under E-commerce regulations, and it is the responsibility of both users and service providers to achieve this protection (Huang and Li, 2019). This is a long shot because customers can utilize services according to their preferences, but if they're held accountable, fraudsters will have a tougher time succeeding, and users will demonstrate responsibility while using any E-commerce service (Persadha et al., 2015).

4.2.5. Online banking policy

Online banking is the way of the future in the banking industry. Every transaction on any platform should be secured (Chaimaa et al., 2021). Laws requiring the usage of line encryption push every bank to do so efficiently. Every bank and financial institution is required under the E-Payment Code to take adequate precautions to safeguard transactions on their digital platforms (Chukwu and Idoko, 2021). These regulations and laws make it mandatory for every financial firm to utilize branch link cryptography, firewalls, and digital certificates for customers to have a secure online banking service (Kiljan et al., 2016). In the USA, India, and Malaysia, online banking is accompanied by a government regulation requiring firms to use IT security measures such as antivirus and firewalls to secure data. The policy also encourages businesses to develop data-protection software. In contrast to the EU, where Safe Harbor, society for worldwide interbank financial telecommunications (SWIFT) Laws, and fraud intelligence sharing systems (FISS) have been designed to safeguard retail banks from fraud, the USA has no dedicated forensic investigation strategy (Srinivas et al., 2019).

In addition, E-Payment Codes are being produced in Australia, which identify the methods by which contract terms between clients and banks should be defined. To limit the threat of false transactions between local and foreign nations, China has devised a similar code-related regulation, to move money, known as bank identifier code (BIC) (Binding and Purnhagen, 2011). In Canada, there are no clear regulations regarding online banking; instead, Chip and Pin policy (i.e., a cryptic chip card) is used to enable digital verification and payment, and everyone should follow this technique to avoid being a fraudster (Albrecht, 2018).

The strategy for a safe online banking procedure is heavily influenced by a nation's internal dynamics (Kiljan et al., 2016). As a result, the laws in each of the seven nations are highly varied. Certain nations, such as Malaysia and India, are focusing on encryption, while software and tools are used in the USA to protect communication (Chukwu and Idoko, 2021). The existence of well-established legislation for online banking suggests that it is a critical aspect of Internet security policy. Since hacking and invading tactics are also evolving, present software and tools may not establish a safe setting for online banking in the future; thus, it is suggested to continuously enhance policies following the growing number of cyber technologies (van de Weijer et al., 2019).

4.2.6. Smart grid policy

Smart grids are among the uses of computer systems, and they fall under the cyberspace umbrella since they employ a digital communication mechanism to monitor and regulate energy supply (Wang et al., 2015). The safety of these grids is guaranteed by the nation's security laws. Several nations employ the Grid Energy Act to safeguard grids and people from harm caused by these grids (Anwar and Mahmood, 2018). The Energy Independence Act encourages the development of smart grids, while the IEEE standard organization works to maintain the high reliability and safety of smart grids (Gunduz and Das, 2020). Smart grids enable governments to track and regulate their electricity production, transmission, and delivery. These grids have become increasingly popular across the world. Apart from Malaysia, each of the six nations involved in this initiative has legislation in place to protect the digital data utilized in the electricity supply system. The energy independence and security act (EISA) of 2007 in the USA contain more information regarding the use of renewable resources than it does about the security of digital data. This law lacks specificity when it comes to user data security.

The ASEAN Smart Grid Congress in Malaysia had a similar problem in that it offered thorough security, like technical studies and site inspections, but it did not provide specifics on how to use digital security in smart grids. While, Canada's Green Energy Act, Australia's Smart Grid Australia (SGA) policies, China's Amendment of the Renewable Energy Law (2009), and the EU's Directive 2001/77/EC, Directive 2006/32/EC, COM (2007) 723 final and Directive 2009/72/EC, provide detailed mechanisms for enacting legislation and protecting data to reduce fraud claims. These nations are implementing changes in energy structure and information systems that will safeguard information. Furthermore, the EU's EC standards requirement for electric cars (M/468) is very successful in preventing fraud through the usage of vehicles that employ encryption techniques to protect customer data. India's smart grids are likewise protected by IEEE standards.

4.2.7. Consumer rights policy

Consumer rights protection law (CRPL) is a law that protects consumers' rights as technological improvements and the nature of products and services change (Miedema, 2018). Cyber service users have several rights. These clients have a right to privacy, and service providers must make reasonable efforts to preserve that right (Chin and Yusoff, 2016). In any event, the personal information of clients must not be disclosed to any unauthorised party (Kerber, 2016). It is the duty of the governments to enact appropriate anti-spam legislation and take serious steps to ensure secure cyberspace as well as the responsibility of the service providers to safeguard their systems (McIntosh, 2015). Consumer rights are protected by legislation in China, the EU, the USA, Australia, Canada, Malaysia, and India. Consumer rights rules in the EU and China are quite similar to the privacy laws outlined above, in that companies are prohibited from misusing personal information without the agreement of consumers. The CPA 1986 in India and the National Consumer Disputes Redressal Commission in Malaysia use the Prima facie approach for identifying and preventing fraud and preserving consumer rights via accusations, while the Malaysian CPA 1999 has applied a service charge on goods and services that are involved in developing technical innovations for consumer safety in an attempt to lessen the unfair trade of private information and the liabilities will be carried by the consumers.

The USA, on the other hand, has thorough legislation to protect consumer rights, such as the Fair Debt Collection Practices Act, the Federal Food, Drug and Cosmetic Act, and the Fair Credit Reporting Act, which distinguish between data threats of each customer to offer a safe infrastructure. The CPA of 2002 was enacted in Canada and is still in effect today to safeguard customers' rights.

Most nations employ these two laws to safeguard consumer privacy and data security; as a result, most nations utilize these two laws to defend consumer rights; however, Australia and the USA have more successful customer laws. They have a statute in place to safeguard customers from any type of fraudulent conduct by any individual or organization that might negatively impact the customer experience. Food, medicines, bills, and loans are all included. It is suggested that conventional consumer rights legislation be combined with regulations protecting consumer rights in cyberspace (Miedema, 2018). Sharing and spreading deceptive material is also a breach of consumer rights, but enforcing the law to prevent content sharing, particularly in this social media age, is difficult. Customers' rights should be protected without compromising their right to free speech, according to a policy that should be created (Idowu, 2019).

4.2.8. Cybercrime policy

The Computer Security Act prohibits any individual or organization from hacking into the computers of another company or individual. Previously, the Draft Computer Security Act (Draft CS Act) was employed to keep computers safe (Walton et al., 2021). There are additional provisions in the IT Act to decrease computer security events (Lloyd, 2020). As a result, researchers have arrived at a solution to keep attackers away from computer clients (Wu and Irwin, 2016). Without tackling computer security breaches, CS is insufficient. Computer security breaches are protected by legislation in the USA, Australia, Canada, China, and India. The Cybersecurity Act of 2015, Cybersecurity Enhancement Act of 2014, National Cybersecurity Protection Act of 2014, and Cybersecurity Workforce Assessment Act have all been passed in the USA to combat computer security risks. China is tougher because it has an anti-terrorism statute that applies to computer security breaches. To combat computer security incidents, Australia is relying on outdated legislation, the TA 1079. Australia, like Canada, has enacted privacy legislation for this reason.

In contrast, the European Network and Information Security Agency (ENISA) was established in the EU to monitor computer security vulnerabilities and give scenario measures to resolve them. The Malaysian National Cybersecurity Policy, for example, focuses on resolving computer security concerns such as fraud, harmful code, hacking, and DoS attacks. In this sense, fraud investigation is a significant component in whole states, and rules are developed by particularly addressing hackers, with vulnerabilities decreased via the use of preemptive instruments for national consumer security (Pătraşcu, 2018). Draft China's Cybersecurity Law (effective July 2015) and Antiterrorism Law (effective January 2016) are now being drafted in order to provide precise security rules and reduce the risk of cyber-attacks in the country. IT laws are utilized in India to deal with computer security issues. Because it incorporates multiple other qualities such as data security, network security, and privacy, computer breach of security is among the most problematic traits (Bennett Moses et al., 2019).

The Cyber Protection Act, which includes the Information Technology Act (IT Act), the Privacy Protection Act, and the Electronic Document Act (Buja, 2021), guarantees fundamental protection to all users in cyberspace. Calderaro and Craig (Calderaro and Craig, 2020) stated that the primary goal of law in this sector is to ensure that no organization or individual harms other societies, individuals, states, or organizations in any way. The objective is to provide a safe atmosphere for everyone while maintaining a good quality of service (Haddad and Binder, 2019). The findings show that each of the seven nations supports CS legislation drafted by national governments. The Chinese safeguard management and the EU's safeguard management are functioning at roughly the same process for protecting against CS at federal levels, such as developing applications and network paralysis for Trojan attacks and hackers. The Australian Telecommunications Act of 1977 places restrictions on telecommunication that applies punishment against hackers for wrongdoing. The act process in China is particularly powerful since it includes all types of phishing strategies and data hacking before anybody thinks of doing fraudulently. As a result, the CS policy process is successful across all nations since each government governs telecommunication channels through a controlled infrastructure, lowering the dangers and hazards connected with data hacking. Compared to the USA, Australia, India, and China, the security within the Canadian Electronic Documents Act (PIPEDA) 2000 and Personal Information Protection and ETA 2006 of Malaysia can be considered as limited as it opposes any extraordinary measures that may be taken in the event of a problem.

The regulations of all these nations demonstrate the disparity in their cyber-protection legislation. Australia's stance has not altered in a long time. It continues to rely on late-nineteenth-century broadcasting and telecommunications legislation. India's telecommunications laws were revised in 2008, although it is still outdated. The EU's Cyber Information Sharing Partnership (CISP) is, on the other hand, more current. For CS, these rules take advantage of real-time data exchange. Other nations should take note of improved legislation, regulations, and mechanisms to improve the security of their cyberspace. To strengthen the data exchange system, it is suggested that communication between different private industries and government departments be improved (NCSC 2022). Several regulations can aid in improving communication by requiring relevant businesses and authorities to provide information that can aid in improving CS (NCSC 2022).

4.2.9. Encryption policy

Any nation's encryption policy defines regulations for protecting virtual data and securing public and private networks (Dizon and Upson, 2021). Wang et al. (Wang et al., 2016), define this policy as a government's desire to preserve all communications networks. For this reason, nations adopt several legislations and acts, such as the IT Act, the Data Protection Regulation, and the Secure Public Networks Act (Laurent, 2021). These acts apply to all service suppliers in the telecommunications and Internet sectors (Dizon and Upson, 2021). In the USA, strict encrypting data laws have been implemented under the Security and Freedom through Encryption (SAFE) Act, which mandates that every 15 days, the governmental regulatory body conducts an assessment of encryption technology and determines the degree of anonymity. The Chinese Regulations on the Administration of Commercial Encryption, on the other hand, have accomplished an industrial-based policy under which a cryptographic chip will be connected to smartphones and computers, reducing the risk of fraud by encrypting data at the point of generation rather than waiting 15 days (Segal, 2016). The IT Act of 2000 and the NEP of 2015 in India are deemed inadequate since they demand encrypted data to be stored for 90 days, increasing the risk of hacking and criminal activity (Prasad, 2022). Canada's State Council Directive No. 273, Australia's Cybercrime Act 2001, and the EU Data Protection Regulation have established a worldwide method to encrypt the data, with the ministry having the right to alter it. However, there is a need for encrypting data legislation in Malaysia, as no rules have been formed yet.

A worldwide encryption standard can assist to enhance encryption efficiency in all nations; however, since a big quantity of data has already been encrypted, it is exceedingly hard, making it impossible for any company to modify its encryption policy unexpectedly. The national encryption regulation is essential for understanding how a nation safeguards its cyberspace (Devi, 2019). It is advised that service providers establish a policy that allows them to readily encrypt data while still providing acceptable security to consumers, and identity-based encryption is one approach to do so (Chatterjee and Sarkar, 2011).

4.2.10. Privacy policy

People have the right to privacy in cyberspace, and the Privacy Protection Act and Civil Law Act are sufficient to preserve everyone's basic privacy (Relyea, 1986). However, several technological challenges are related to cyberspace, necessitating particular legislation to define and offer individuals the best possible privacy (Laurer and Seidl, 2021). Data Protection Reform is the consequence of efforts to ensure that all users have enough privacy (Neama et al., 2016). These revisions also make it illegal for any entity to breach people's privacy in the name of security without their consent or a compelling justification (Yee, 2006). Each of the seven nations has its privacy protection statute, but these laws are aimed at various types of protection. For example, the USA's Cyber Privacy Fortification Act of 2015 and India's Privacy Protection Bill impose fines on companies that fail to provide the necessary security level to clients, such as prison or a fine, whereas China's CRPL creates a backdoor for the purchase and sale of counterfeit goods. Public and private regulations include Canada's PIPEDA, Malaysia's PDP Act 2010, Australia's Privacy Act 1988, and the EU's Data Protection Directive. The EU's privacy law is seen as acceptable, and it functions under a user-as-owner mechanism, making it a particularly designed statute for personal information.

Australia is still employing the 1988 Privacy Act. Malaysia's PDP Act is also being used to safeguard privacy. In Malaysia, the same rule is used to combat identity theft. Similarly, Canada has the same PIPEDA law that deals with privacy and identity theft. Because of the disparity in people's awareness, privacy regulations in all of these nations varies significantly. In comparison to Malaysia, China, and India, EU and USA privacy rules are relatively rigorous. It is difficult for all nations to safeguard privacy while allowing law enforcement agents sufficient access to data for the investigation of various CS (Cole et al., 2017). The current cyber applications and innovations also allow the service provider to monitor the user's location, making enacting a proper privacy regulation more difficult (Yang et al., 2020). It is suggested that society experts, police agencies, and cyber providers meet to address privacy issues in order to develop more thorough and effective privacy legislation (Tsesis, 2019).

4.2.11. Identity theft policy

Identity theft is one of the most serious cybercrimes, since it may generate a slew of societal problems as well as national security concerns (van de Weijer et al., 2019). Because identity theft on social networks is fairly easy, it is hard to protect against identity theft in certain circumstances and apply appropriate punishment (Hoffman and McGinley, 2010). A lot of legislation work has been done in the sector. The Theft and Assumption Deterrence Act prohibits anybody from impersonating another person for any reason (Steel, 2019). Identity theft is also prohibited by the Personal Information Protection Act, the Electronic Document Act, and the Privacy Act. Due to the nature of some cases of identity theft, the Criminal Code may be used (Hoffman and McGinley, 2010). Identity theft is safeguarded in the EU by a criminal code formed via coordination between national and territorial authorities, but liberalization is still needed to prevent identity theft at both the personal and institutional levels. The Australian Criminal Code Amendment Act 1999, Malaysia's PDP Act 2010, Canada's PIPEDA 2005 (S-4), the USA's Identity Theft and Assumption Deterrence Act laws, and the Chinese Criminal Code Network Security Law all provide regulations to lessen the probability of forgery to a larger extent (van de Weijer et al., 2019). Each nation supports legislation to safeguard against identity fraud, and the provisions of the USA and Indian laws appear to be successful since they provide support via precise bans and punishments (Steel, 2019).

The EU, Australia, Canada, and China all have regulations that are fairly similar when it comes to identity theft. India does not have a complete regulation regarding this trait; however, its IT Act of 2000 contains a provision that defines any entity that imitates another entity's identity in cyberspace to be a criminal. *PDP* data protection regulations can also include this characteristic; as a result, Malaysia only has a *PDP* statute in place to address identity theft (Shahwahid and Miskam, 2015). Although many nations have comparable laws against identity theft, a complete code is still needed since many Internet users create profiles on various social networking platforms using the names of different individuals. Until somebody submits a report, the law does not take effect (Kethineni, 2020). Furthermore, social media companies do not go into great depth to confirm the identities of their members since doing so would limit their user base, and there is no regulation requiring them to do so. Clients are often hesitant to reveal personal information for fear of identity theft. It is necessary to work to resolve this problem through law and advanced technologies (Hoffman and McGinley, 2010).

4.2.12. Digital signature policy

The existence of a digital signature alone is insufficient to protect digital data. Somani et al. (Somani et al., 2010) suggested that digital signatures be complex enough to keep data safe. In some nations, the Electronic Signature Act requires all relevant authorities to build an electronic signature system that not only protects data but also identifies persons (Somani et al., 2010). Financial transactions are also protected by these signatures. The Digital Signature Act and the IT Act are two pieces of legislation on this subject (Lloyd, 2020). The digital signature policy was established to assist minimize the danger of identity fraud, and each of the nations mentioned supports the legislation to help reduce the risk of fraud. The ETA 2001 and the ETA 2000 are two effective Australian statutes in this area (Webb, 2007). The Electronic Signature Law of the People's Republic of China creates a private network among two parties in communication, allowing people residing far apart to validate each other's identities and reducing the risk of fraud. The data protection is secured under EU legislation by issuing user certificates and generating e-signatures that identify the signatory before performing the transactions, according to the EU Directive for Electronic Signatures (1999/93/EC). This technique is less dangerous, and the IT Act 2000 in India encourages the same type of technique in which P2P communication is assured, resulting in the development of a secure link.

All of these nations' policies on digital signatures are quite similar, although Malaysia lags since it still follows the 1997 digital signature statute. The USA, the EU, Australia, Canada, and India all have legislation in place to ensure that the digital signature level is high enough. Because no infrastructure or regulation allows the creation of digital signatures of individuals, digital signatures are largely employed by large businesses. The fundamental problem here is that digital signatures may be replicated with extreme accuracy, making them subject to security threats (Hatcher et al., 2020). Every nation's CS strategy should promote the deployment of innovative, user-friendly technologies to make this cyberspace more valuable and secure.

4.2.13. Data security policy

Another important shared trait in CS is the Data Security Act, which covers both public and private data (Idowu, 2019). All users can access and utilize public data, but only legitimate users can obtain and use personal information (Kumar et al., 2018). A vast amount of people's sensitive information may be stored in business enterprises. This information must not be misused in any way (Laurent, 2021). In many nations, the personal data protection (PDP) Act protects users' data, while the Data Security and Breach Notification Act prevents any organization or individual from acquiring and using data belonging to another organization or individual without proper authorization (Crandall, 2005). Data protection requirements are included in data security legislation (Lallie et al., 2021). All nation's data protection regulations vary depending on their population, GDP, and public awareness (Kumar et al., 2018). The USA Data Security Act and Breach Notification Act have made recommendations for educating small and big businesses about data protection and developing nonbinding best practice tools for online transactions. Deceptions will be recognized in this situation by keeping watch on the operations of the firms, and data use will intervene in the event of any illegal activity. The Australian Privacy and Data Protection Act 2014 requires businesses to offer customers data security measures and obtain their agreement before releasing personal data; else, businesses would violate confidence (Watts and Casanovas, 2019). Comparable permission regulations have been enforced on firms under India's PDP Bill and Canada's Criminal Code's Lawful Access Powers, in addition to disk imaging in India and compliance agreement in Canada. China, although being a developed country, has no explicit data protection legislation. To address data protection challenges, the EU has well-developed provisions under its data protection legislation (Laurer and Seidl, 2021).

Various regulations, such as the crimes act, can be utilized to tackle data breaches in China, but a suitable policy to safeguard the data of businesses and individuals is required. Data protection is one of the aspects of CS policy that has received significant attention recently; as a result, all major nations, including the USA, Australia, and the EU, have updated data security rules and regulations. Because data security is linked to privacy in certain ways, privacy laws can be used to address data security issues in some instances. This, maybe, is one of the reasons why China does not have data security legislation (Feng, 2019). Authorities may not have grasped the distinction between data privacy and security. Data privacy and data security must be defined and classified independently so that a unique regulation may be designed to make digital data safer (Idowu, 2019).

4.2.14. Spam policy

Spam is defined as electronic messages that include unsolicited material and are sent to a large number of recipients (Alzoubi et al., 2021). Dunham and Bradshaw (Dunham and Bradshaw, 2004) state that spamming is mostly used to promote low-quality or unlawful items. Spam degrades the experience for users and disseminates offensive material to the public. Furthermore, spamming is also utilized for hacking; consequently, spamming requires particular laws (Laurent, 2021). To do this, the Spam Act is applied (Beardwood and Stern, 2014). The IT Act also includes anti-spam provisions. In several nations, the Directive on Privacy and Electronic Communication is also used to combat spam in cyberspace (Kigerl, 2015). Except for India, where no law has been formed to decrease spam operations, nations such as China, the EU, the USA, Australia, Canada, and Malaysia have established policy provisions for spam acts. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) of 2003 in the USA decreases the risk of fraud by prohibiting the use of false topic lines in product marketing to clients. Every marketing communication is scrutinized against a set of guidelines to ensure that customer information is not misused. Businesses in the EU, on the other hand, are subject to the Directive (2002/58/EC) on Privacy and Electronic Communications, which imposes a flat price for electronic communication. Likewise, China's Anti-Spam law and Canada's anti-spam legislation (CASL) 2014 provide a safe marketplace by notifying enterprises in detail of regulatory requirements and infractions. For this CS issue, Australia has comparable spam legislation.

Spamming goes undiscovered because of several CS difficulties as well as because customers have come to view spamming as one of the unavoidable consequences of using the Internet and have become unconcerned about it. In a nation like India, the lack of a well-established anti-spam law demonstrates the authorities' stupidity. Although improved knowledge of spamming and filtering software has lessened the impact of spam, thousands of Internet users throughout the world are still affected by this security problem. Telling the difference between spam and mass marketing is a hard task. The legislation prohibiting intensive distribution may elicit a response from businesses. It is suggested that a standard be developed to identify spamming, as well as a regulation that protects customers from spam while enabling businesses to market themselves freely (Shaykevich, 2019).

5. Discussion

This study intends to address the research questions: How do different nations implement CS policies to address critical CS attributes? RQ was answered in Section 4.1 and Section 4.2. Fourteen common CS attributes that influence CS policy framework formation were identified and analyzed on how the seven nations (the USA, the EU, Canada, Australia, China, India, and Malaysia) approached these traits. These attributes are telecommunication, network, Cloud computing, E-commerce, online banking, smart grid, consumer rights, cybercrime, national encryption, privacy, identity theft, digital signature, data security, and spam. While these attributes are self-contained, interdependencies between these attributes can be further specified for a specific context. In this section, the implications of the findings, the limitations of this study, and future directions are also discussed.

5.1. Overall evaluation

The CS threat has escalated to such a degree worldwide that removing it has become quite challenging. On the other hand, Nation's measures have helped to regulate this issue to some level. Every nation is not subjected to the same amount of danger. While there is no standard for evaluating cybersecurity policies, most recent research and professionals in the industry (e.g., (GCSCC 2022; Dutton et al., 2019; Naseir, 2021; Collett, 2021; Nakhli, 2022; ENISA 2022; GFCE 2022; UNODA 2022)) have identified common factors that should be examined for successful policy implementation. The description for each of the eight factors used to evaluate the cybersecurity policy is summarized in Table 10.

For rating cybersecurity policy factors, the simple additive weighting (Fishburn, 1967) technique is utilized, which is probably the most popular and well-known approach (Pipyros et al., 2018). The overall score of a policy is calculated using this technique as the weighted total of the factors utilities or scores. Each factor is assigned a normalized weight, and the total weight should be equal 1. For the sake of this study and owing to a lack of research that gave such an evaluation, we have assigned the same weight to each of the eight factors (i.e., 0.125), even though various factors may be valued differently in different nations. For example, certain countries, such as China, impose some cybersecurity attributes while others, such as Canada and the USA, do not, for some policies like network and e-commerce policies. The evaluation values for each cybersecurity attribute revealed in this study are summarized in Table A1 - Appendix A. The scores of each policy among the seventh nations are depicted in Fig. 2. It is important to note

Table 10
Cybersecurity evaluation factors description.

Factor	Description
Infrastructure	The capability of the country to design and implement a cybersecurity policy, as well as to improve its cybersecurity endurance by bolstering its cyber defense, incident management, equipment, skills, and ICT protection assets.
Knowledge and awareness	Knowledge and abilities examine policy quality, affordability, and adoption by individuals, government, and businesses. It also has to do with cybersecurity awareness campaigns, expert training, and formal cybersecurity educational materials, among other things.
Frameworks and models	Create and maintain procedures, tools, and operations for collecting, analyzing, and using state, data, and summary from other disciplines in order to set up tactical operating cybersecurity situations.
Standards and regulations	Adopt and create national laws and standards relating to cybersecurity, both direct and indirect, with a focus on regulatory standards for cybercrime-related statutes and applicable regulations.
Management	Manage a cybersecurity program that includes a planning process, administration, and cybersecurity operations that are aligned with the country's strategic priorities and the threat to national infrastructure.
Evolution policy	Cybersecurity policy should be adaptive, evolving, and tailored to meet new problems and requirements.
Specialization	Professional team that is tasked with maintaining a certain cybersecurity act or law.
Enforcement	Applying punishment or penalties for firms or individuals not following anti-cybercrime laws and regulations.

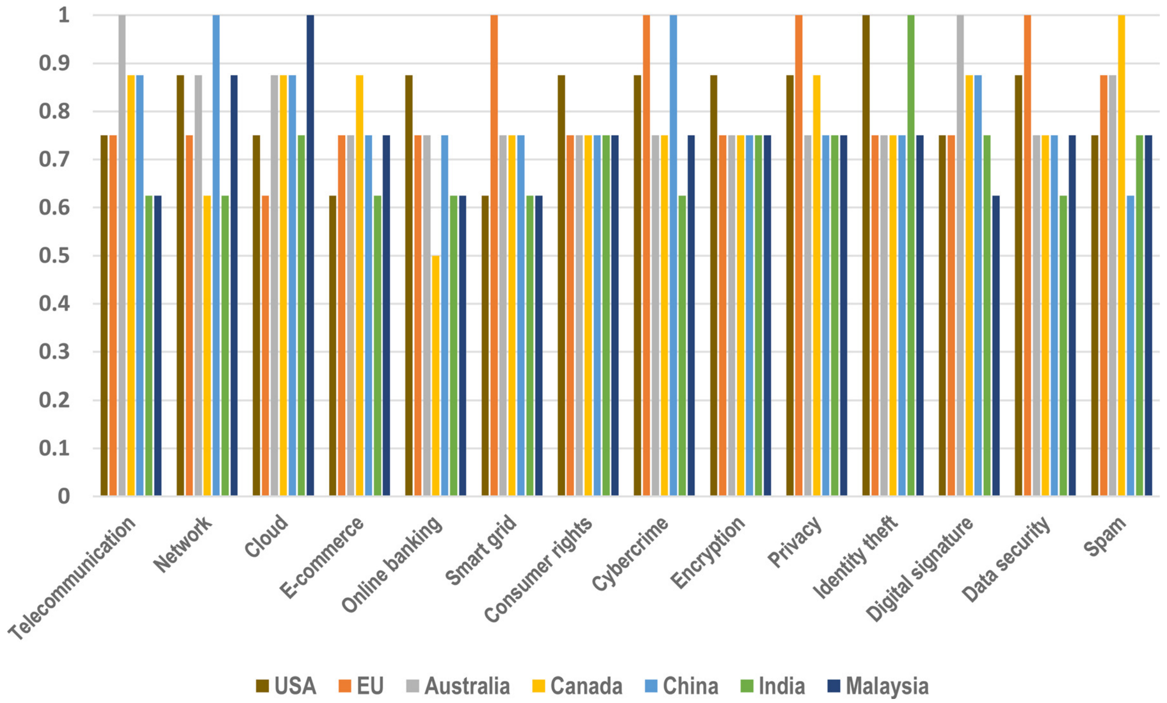

Fig. 3. Cybersecurity factors simple additive weighting.

here that the purpose of such an evaluation is not to suggest that one country is better than others. Rather, it is about demonstrating an approach to analyzing and scoring the various attributes. These should not be taken as an official ranking of countries.

According to Fig. 3, in terms of adopting the most effective regulations for online banking (0.875), identity theft (1.0), national encryption (0.875), and consumer rights (0.875), the USA leads the way (van de Weijer et al., 2019). In terms of identity theft (1.0) policy, India, on the other hand, is tied with the USA. In terms of E-commerce (0.875) and spam regulations (1.0), Canada came out on top (Shafqat and Masood, 2016). Because the EU and China have different legislation and security measures in place to combat cybercrime, they received the highest scores (1.0). In addition, the EU has the highest scored policies in terms of data security (1.0), privacy (1.0), and smart grid (1.0) (Shackelford et al., 2015). Furthermore, China has the highest network policy score (1.0). Telecommunications (1.0) and digital signatures (1.0) policies may all be modeled after Australia's regulation. Malaysia received the highest ranking in terms of Cloud computing policy (1.0).

Table 11 compares and contrasts the merits and disadvantages of various CS strategies in the nations examined. Because the USA has so many large companies with many customer records, the country's financial markets are the most vulnerable to data breaches. Despite its leadership in online banking, identity theft, national encryption, and consumer rights policies, telecommunications (0.75) policy required updating to its regulations, network (0.875) has no special laws, and Cloud (0.75), privacy (0.875), and e-commerce (0.625) policies are not properly managed even after policy creation due to the availability of large datasets (Kurt, 2015). The smart grid (0.625) in the USA has not been upgraded in the previous few years, it is vulnerable to cyber-attacks. Also, the cybercrime (0.875) policy, despite its comprehensive measure, follows a self-governance approach. Moreover, digital signature (0.75) and spam policies (0.75) do not have special laws, and data security (0.875), despite using modern techniques, lax enforcement.

In four policies, however, the EU came out on top: smart grid, privacy, data security, and cybercrime. Due to outdated laws, weak regulations, or a lack of specific legislation, it received a 0.75 in all telecommunication, network, E-commerce, online banking, encryption, and identity theft policies. Telecommunications (1.0) and digital signature (1.0) policies scored highest in Australia. To safeguard Cloud computing (0.875), E-commerce (0.75), online banking

Table 11
Evaluation of cybersecurity policies among selected nations.

Attribute	USA	EU	Australia	Canada	China	India	Malaysia
Telecommunication	Laws require modification	Old act	Highest score@@(1.0) – special law	Special act	Special laws	Old laws	Old laws
Network	Special laws	Special directives, its policy is still lagging	cyber-crime laws are used	National defense act is used, no special law	Highest score (1.0) – special law	IT act is used	Using old acts
Cloud	Several laws used	Under-developed policy	Several laws used	Personal protection policies	Global perspective policy	Providing infrastructure through CCA	Highest score (1.0) – special law
E-Commerce	Anti-terrorist law	Electronic Commerce Directive 2000	Electronic Transaction Act 1999	Highest score (0.875) – special law	Specific law	No specific law	No comprehensive law
Online Banking	Highest score (0.875) – special law	Only FISS is used	Developed e-payment codes	No comprehensive laws	Bank identified codes	Focus only on encryption	Focus only on encryption
Smart Grid	No special laws, EISA provides some guidance	Highest score (1.0) – special law	No special law	No special law, green energy act is used	Renewable energy laws are used	Follows some IEEE standards	ASEAN is used to get directions
Consumer Rights	Highest score (0.875) – special law	Developed law in 2014	General consumer law	Special law but it requires amendment	amended its laws in 2014 to improve them	Old laws	Old law of1999 is in practice
Cybercrime	Most comprehensive laws - CNCI	EU (ENISA) and China have highest score (1.0) with multiple laws	Telecommunication law (old)	PIPEDA, no policy for emergency situation	EU and China (anti-terrorism law) have highest score	IT act is used, no special law	Different regulations, no support for emergency situation
Encryption	Highest score (0.875) – SAFE policy	Data protection act	No special laws	Global mechanism in its policy	Industrial based policy	Special laws but ineffective	Basic criminal codes are used
Privacy	Punishment but policy need improvement	Highest score (1.0) – special law	Privacy act of 1988 - not good enough currently	Personal data protection	Consumer protection law has loopholes	punishment but ineffective	Personal data protection used
Identity Theft	USA and India have highest score (1.0)	Only criminal code is used, no special law	Personal protection laws, no special law	Only criminal code is used, no special law	Only criminal code is used, no special law	USA and India have highest score (1.0)	Personal protection laws, no special law
Digital Signature	Multiple laws used	Electronic signature directive, needs upgrading	Highest score (1.0) – special law	Multiple laws, no special law	Private infrastructure is used	Same IT Act of 2000 is also used here	Its lagging with old laws of 1997
Data Security	Modern policy and very effective	Highest score (1.0) - most advanced	Privacy laws are used	Personal information protection policy	No special laws	Personal data protection, needs modification	Personal information policy
Spam	Several laws used	Well-developed infrastructure used	Special spam act	Highest score (1.0) – special law	Old regulations which were used for email protection	No special law	No special laws. TA is used

(0.75), and CPAs, Australia, like the EU, has developed a closed connection between corporations, governments, individuals, and suppliers by imposing rules that match national demands (Turner and Stough, 2020). Since it relies on self-governed procedures for online banking (0.5), data security (0.75), and network security rather than top-down authority, Canada faces a similar degree of hazard as the USA [46]. In contrast to the USA, Canada's E-commerce CS policies (0.875) are effective because they are continually upgrading CS standards at the national level and providing institutions with enough infrastructure for securely sharing data.

According to the Law 360 research, China is pursuing effective policy steps to reduce CS dangers to a greater level. China scored highest in terms of network and cybercrime policies. China established new national security legislation in 2016 that includes Cloud computing (0.875), network, online banking (0.75), E-commerce (0.75), and telecommunications (0.875) under data localization processes, whereby data will not be transmitted for retention to international jurisdiction. In this regard, before proceeding with the cross-border data transfer, the companies must first obtain approval from government officials and satisfy the data transfer regulation. Other attributes, such as identity theft (0.75), spam actions (0.625), and smart grid (0.75), are not included in this policy, therefore it is recommended that the government issue a new notice to cover these areas (Stratford and Luo, 2016). Furthermore, according to Binding and Purnhagen (Binding and Purnhagen, 2011), CPAs in China and the EU are similar due to the implementation of national plans.

In Malaysia, extensive ICT infrastructure investment and resulted in leading in terms of Cloud computing. The government has boosted its investment in this area to ensure the efficient use of online banking (0.625) (Goi, 2005). Malaysia is recognized as the first nation in Southeast Asia to pass CS legislation, and it has prioritized network infrastructure (0.875), E-commerce (0.75), and Cloud computing (1.0) in its policy objectives. Malaysia's CS policies are mostly related to national defense and public health, which are beyond the scope of this paper, and Malaysia is still seen as less competitive than Canada and India, for instance, when it comes to dealing with CS concerns (Carroll and Kellow, 2021). The

Indian identity theft policy scored the highest along with the USA identity theft policy, due to the strict regulations applied. However, other policies such as telecommunication, network, online banking, smart grid, cybercrime, and data security indices scored 0.625 for each, since they rely solely on minimal high levels and no special laws have been developed, and major organizations have failed to apply these standard established rules, resulting in a loss of competence in policy regulations (Devi, 2019). In China, India, and Malaysia, which have many Internet users who are unaware of the hazards, identity theft (scored 0.75) and spam scams (scored 0.625, 0.75, 0.75, respectively) are highly frequent. The countries' financial situations also motivate the people in these nations to engage in criminal activities. Within the CS threat scenario for the EU, Australia, and Canada, ransomware is among the most common risks.

As a result, it can be concluded from recent the above assessment and discussion that CS policy implementation in the USA and EU are highly effective in stopping threats since they cover a wide range of features under a particular law and are backed up by a robust development infrastructure (Shackelford et al., 2015). China may come second but need further consolidations in the cybersecurity policies. Even though India, Australia, and Canada are becoming more powerful nations on the global stage, they still need to concentrate on effective policy execution (Manwaring, 2009). Furthermore, specific policies of countries such as Malaysia and Canada perform better, but on comparison criteria, the countries must work harder to get a comparative benefit (Shafqat and Masood, 2016).

5.2. Implications

The identified attributes are crucial for CS policy since they encompass the majority of CS challenges (Mishra et al., 2022). The results of this study suggests that it is critical to solve these concerns since hi-tech attacks cost billions of dollars every year (Paananen et al., 2020). Security and data privacy are the trendiest problems in CS, particularly in industrialized countries with a large number of international corporations (Tsesis, 2019). For over a decade, CS policies have had legislation governing data privacy, security, telecommunications, spamming, and network security, which are critical because they boost user confidence, which leads to a growth in the number of users and economic prospects (Al-Garadi et al., 2016). It is critical to have a telecommunication attribute to maintain communication services safe (Kiljan et al., 2016). These attributes are still important for CS policies, but modern features like Cloud computing security, smart grid, and e-commerce have also become important. The smart grid's ability to monitor and regulate electricity generation, protection, and distribution is critical (Gunduz and Das, 2020). The Cloud computing attribute is important for CS policy because it shows that the policy is evolved enough to maintain CS in the present-day (Tissir et al., 2021). Encryption, digital signatures, and online banking are all crucial features for safe transactions.

Some nations' policies scored more than others in managing some attributes. This means that while a nation's policy cannot be called the best, it may be argued that a nation has the most effective (according to this study evaluation) policy for a specific application. The findings demonstrate that when it comes to CS, each nation has its unique set of strengths and shortcomings. Every nation's cyberspace is vast, and there are several security challenges linked with it. Accordingly, only a large firm with vast resources can maintain CS. Furthermore, CS mandates that the authority monitors cyber services so that any data breach may be investigated and security vulnerabilities assessed. Accordingly, the federal government and cyber service providers play a critical role in policy creation. Cyber service providers state what level of legal protection their services require. Every government also establishes a dedicated federal agency or initiative to assess the present situation and do research on different causes of CS across the world to make policy suggestions. The Networking and Information Technology Research and Development Program, for instance, in the USA, presents a CS road map.

CS is about more than just solid policies and firewalls; CS is also about apprehending criminals. Law enforcement agencies are responsible for ensuring the dominance of the law and enforcing it in reality. Because one institution cannot monitor all rules, the nature of cyber risks fluctuates. As a result, the structure of regulations also varies significantly. Some risks are the responsibility of local governments, while others are the responsibility of the federal government. In the USA, the Federal Bureau of Investigation maintains a CS division that investigates cyber threats on a local level for each state police department. Other nations, such as Australia, Canada, India, Malaysia, China, and the EU, have police departments that enforce the law.

Risks to each nation vary due to a variety of variables such as geographic constraints, foreign policy, and political conditions. Ranking of cyber risks is done by looking at past cyber risk incidents. Cyber risks are also prioritized by different governments based on their frequency. If a nation faces higher dangers of spamming and privacy violations than other risks, these risks will be prioritized (Shaykevich, 2019). The estimated financial damage in the event of cyber risks may also be used to prioritize risks. If a cyber threat has the potential to inflict significant societal disruption or financial damage, nations will devote greater resources to combating it (Manwaring and Hanrahan, 2019). Based on the findings of this study, we can argue the following recommendations in order to enhance CS architecture.

- The CS policy should be adaptable, allowing the state to enhance it as technology improves. It is advised that all nations examine the policies of other nations to get inspiration and incorporate topics relevant to their setting. This method can aid in the creation of a complete and successful policy. Also, the growing information-sharing mechanism under the cyber protection act should promote communication between all governmental and private sectors.
- In terms of digital signatures, any government must embrace this technology in order to protect digital material. Improved technology and legislation that encourages consumers to provide their identities, increasing meetings between decision-makers and service providers; society leaders lead to more worldwide appropriate privacy rules are all needed to combat identity theft.
- Network security laws have to be improved in several nations, such as the EU, India, and Canada, where IoT security rules fail to collect private data securely. With the growing number of international data protection rules, including a policy that allows service providers to offer sufficient security for users and simply data encryption can be effective solutions.
- Currently, differences in telecommunication infrastructure across different nations make telecom service security a key concern. As a result, nations must assist each other in improving the efficacy of the communication infrastructure to find a solution.
- The publication of data privacy and consumer rights is a major concern, particularly in the social media space; as a result, a new strategy that protects consumer rights and privacy is an effective solution.

5.3. Limitations

Even though this study accomplished its aims and notwithstanding all of the time and effort put into its preparation, it has certain inescapable limitations. Due to time and fund support restrictions, no questionnaire was employed and no interviews with specialists from other nations were undertaken. Interviews with certain specialists in a few nations may aid in the development of a more comprehensive list of common CS attributes. Incorporating more prevalent attributes might lengthen and complicate the study process. Furthermore, to obtain information on various policies of chosen nations, only publicly available papers of selected nations were used. Some nations' most recent papers were not accessible on their official websites. In India, for example, there was no paperwork accessible for the spam act statute. Similarly, the policy of national encryption in Malaysia was not accessible, which may hide various laws and procedures to safeguard cyberspace. In addition, although this study utilized a rigorous method to analyze each policy, all factors were given equal weight. Different policies, on the other hand, maybe prioritized or weighted differently in each country.

Only seven nations were analyzed. There are several additional nations with well-developed IT infrastructure and big populations of Internet users. South Korea and Japan, for example, have around 115 million web users. More than 90% of the people in these two nations utilize the Internet. Because official documents and policies, in these nations, were only available in South Korean and Japanese languages, it was not feasible to investigate their CS policies without the help of an experienced translator, which might result in time and financial issues. Finally, the research's analysis and findings are qualitative, which makes it prone to bias, another drawback of this study.

5.4. Future directions

Based on the analysis of CS policies in the seven nations. With the aid of this study, a nation can establish a suitable CS policy, but the research may be expanded in numerous areas to achieve extra insights. Here are some possible future research directions in this domain.

- In order to study other related attributes of CS policy, it is essential to analyze the CS policies of other nations with a high number of IT users and well-developed IT infrastructure. Other nations' research may reveal new cybercrime strategies and procedures, which can aid law enforcement authorities in combating comparable cybercrime in their nations. Since analyzing the policies of a wide number of nations would take a significant amount of time and money, a suitable sponsor will be necessary for such a study to yield more insightful results. The findings of this paper can make a significant contribution to future research projects of this kind.
- Because cyberspace is always expanding and the technologies linked with it are developing, the problems for CS are also growing. Simple measures can aid in the current fight against cybercrime and CS concerns, but they may not be suitable in the future. It is necessary to design a more dynamic policy that can be implemented over time and allows authorities to make swift modifications. An advanced study should be performed to identify a mechanism to build a dynamic policy (Graham et al., 2016). The TA of the USA is an example of such a policy. It was created in 1996 and is still functioning with all contemporary telecommunications systems and technology.
- Differences in national policies also contribute to certain cybercrime. For example, a hacker residing in a nation with lax or no policies against breaches or hacking might attempt to infiltrate a network or hack a system. A universal CS policy might help all Internet users throughout the world have a better experience. To determine how a worldwide policy may be formed, substantial research is required. It is feasible for a nation to adopt policies that safeguard not just its cyberspace but also prohibit persons within its borders from hurting the cyberspace of other countries in any way. It may even help to strengthen international relations (Carroll and Kellow, 2021). This work can serve as a foundation for developing such policies or doing advanced research for this goal.

6. Conclusions

Since cybercrime has the potential to jeopardize national security, it is critical to combat these crimes decisively. To combat cybercrime, there should be well-established policies, as well as the identification of critical CS traits so that a comprehensive policy can be devised. A variety of stakeholders contribute to the development of a CS policy, but the government is the driving force behind the policy's creation and modification. This study examined current literature, research papers, websites, blogs, and other publicly available materials in order to compile a list of common attributes that are significant in the establishment of CS policy. The study investigated and contrasted the CS policies of seven nations (the USA, the EU, Australia, Canada, Malaysia, China, and India), as well as how each attribute is addressed.

Fourteen common features were identified as critical for decent CS policies as a result of our literature review. While establishing a CS policy, every government may consider these attributes. Every nation, it has been reported, has its method of securing its cyberspace. Their priorities change depending on the economy, political climate, and user awareness. The general public and corporate groups exert significant pressure in this area. This paper demonstrates how difficult it is to create a policy that addresses all of the issues. The policies of other nations may be used to help national CS policy. The first step toward establishing safe cyberspace is to design a comprehensive CS policy. This study serves as the foundation for a country's attempts to eradicate all CS hazards; as a result, every government should have a department dedicated to developing and accessing its policies. Without a comprehensive policy for all CS attributes, any nation's cyberspace cannot be protected. Cyberspace can become safer if all nations agree on common attributes and adopt a worldwide strategy for the CS.

Declaration of Competing Interest

None

Appendix A

All factors were given an equal weight of 0.125. The eight factors used in this evaluation are extracted from (Shackelford et al., 2015; Binding and Purnhagen, 2011; van de Weijer et al., 2019; Devi, 2019; Shafqat and Masood, 2016; Kurt, 2015; Turner and Stough, 2020; Stratford and Luo, 2016; Goi, 2005; Carroll and Kellow, 2021).

Table A1
Cybersecurity attributes factor evaluation.

	Telecommunication						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	
Frameworks and models	✔	✔	✔	✔	–	✔	✔
Standards and regulations	✔	✔	✔	✔	✔	–	–
Management	✔	✔	✔	✔	✔	–	–
Sustainable process	–	–	✔	–	✔	–	–
Specialized department	✔	✔	✔	✔	✔	✔	✔
Enforcement	–	–	✔	✔	✔	✔	✔
Total	0.75	0.75	1	0.875	0.875	0.625	0.625

	Network						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	✔	✔	–	✔	–	✔
Management	✔	–	✔	✔	✔	✔	✔
Sustainable process	✔	✔	✔	✔	✔	–	–
Specialized department	✔	–	–	–	✔	–	✔
Enforcement	–	✔	✔	–	✔	✔	✔
Total	0.875	0.75	0.875	0.625	1	0.625	0.875

	Cloud						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	✔	✔	✔	–	✔
Management	✔	✔	✔	✔	–	✔	✔
Sustainable process	✔	✔	✔	✔	✔	✔	✔
Specialized department	–	–	–	–	✔	–	✔
Enforcement	–	–	✔	✔	✔	✔	✔
Total	0.75	0.625	0.875	0.875	0.875	0.75	1

	E-Commerce						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	✔	–	✔	✔	–	–
Management	–	–	✔	✔	–	✔	✔
Sustainable process	–	✔	–	✔	✔	–	–
Specialized department	✔	–	✔	✔	–	–	✔
Enforcement	–	✔	✔	–	✔	✔	✔
Total	0.625	0.75	0.75	0.875	0.75	0.625	0.75

	Online banking						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	✔	–	✔	–	–
Management	–	✔	–	✔	–	✔	✔
Sustainable process	✔	✔	–	–	✔	–	–
Specialized department	✔	–	✔	–	–	–	–
Enforcement	✔	✔	✔	–	✔	✔	✔
Total	0.875	0.75	0.75	0.5	0.75	0.625	0.625

	Smart grid						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	–	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	–	✔	–	–	✔	–	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	–	✔	✔	✔	✔	–	–
Specialized department	✔	✔	–	–	–	–	–
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.625	1	0.75	0.75	0.75	0.625	0.625

(*continued on next page*)

Table A1 (*continued*)

	Telecommunication						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
	Consumer rights						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	–	–	–	–	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	✔	–	✔	–	–	–	–
Specialized department	✔	✔	–	✔	✔	✔	✔
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.875	0.75	0.75	0.75	0.75	0.75	0.75
	Cybercrime						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	✔	–	–	✔	–	–
Management	✔	✔	✔	✔	✔	–	✔
Sustainable process	✔	✔	–	–	✔	✔	✔
Specialized department	✔	✔	✔	✔	✔	–	–
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.875	1	0.75	0.75	1	0.625	0.75
	Encryption						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	–	–	–	–	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	✔	✔	✔	✔	✔	✔	✔
Specialized department	✔	–	–	–	–	–	–
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.875	0.75	0.75	0.75	0.75	0.75	0.75
	Privacy						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	–	✔	–	✔	–	–	✔
Management	✔	✔	✔	✔	✔	–	–
Sustainable process	✔	✔	–	–	–	✔	✔
Specialized department	✔	✔	✔	✔	✔	✔	–
Enforcement	✔	✔	✔	✔	✔	✔	✔
Total	0.875	1	0.75	0.875	0.75	0.75	0.75
	Identity theft						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	–	–	–	✔	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	✔	✔	✔	✔	✔	✔	✔
Specialized department	✔	–	–	–	–	✔	–
Enforcement	✔	✔	✔	✔	✔	✔	✔
Total	1	0.75	0.75	0.75	0.75	1	0.75
	Digital signature						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	–	✔	✔	✔	✔	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	✔	–	✔	✔	✔	–	–
Specialized department	–	✔	✔	–	–	–	–
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.75	0.75	1	0.875	0.875	0.75	0.625

(*continued on next page*)

Table A1 (*continued*)

	Telecommunication						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
	Data security						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	✔	–	✔	–	–	–
Management	✔	✔	✔	✔	✔	✔	✔
Sustainable process	✔	✔	✔	✔	✔	–	✔
Specialized department	✔	✔	–	–	–	–	–
Enforcement	–	✔	✔	–	✔	✔	✔
Total	0.875	1	0.75	0.75	0.75	0.625	0.75
	Spam						
Factor	USA	EU	Australia	Canada	China	India	Malaysia
Infrastructure	✔	✔	✔	✔	✔	✔	✔
Knowledge and awareness	✔	✔	✔	✔	✔	✔	✔
Frameworks and models	✔	✔	✔	✔	✔	✔	✔
Standards and regulations	✔	✔	✔	✔	–	–	–
Management	✔	✔	–	✔	✔	✔	✔
Sustainable process	✔	✔	✔	✔	–	✔	✔
Specialized department	–	–	✔	✔	–	–	–
Enforcement	–	✔	✔	✔	✔	✔	✔
Total	0.75	0.875	0.875	1	0.625	0.75	0.75

References

Libicki, M.C., 2021. Cyberspace in Peace and War. Naval Institute Press.

Eriksson, J., Giacomello, G., 2022. Cyberspace in space: fragmentation, vulnerability, and uncertainty. In: Cyber Security Politics. Routledge, pp. 95–108 M. D. Cavelty and A. Wenger, Eds., ed.

Lippert, K.J., Cloutier, R., 2021. Cyberspace: a digital ecosystem. Systems 9, 48–67.

Mohan, A.M., Meskin, N., Mehrjerdi, H., 2020. A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. Energies 13, 3860.

Paananen, H., Lapke, M., Siponen, M., 2020. State of the art in information security policy development. Comput. Secur. 88, 101608.

Mishra, A., Alzoubi, Y.I., Gill, A.Q., Anwar, M.J., 2022. Cybersecurity Enterprises Policies: a Comparative Study. Sensors 22, 538.

Roshanaei, M., 2021. Resilience at the Core: critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. J. Comput. Commun. 9, 80–102.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P., 2011. Dimensions of cyber-attacks: cultural, social, economic, and political. IEEE Technol. Soc. Mag. 30, 28–38.

Anwar, A., Mahmood, A.N., 2018. Cyber security of smart grid infrastructure. In: 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), pp. 303–308.

Ibrahim, H., Karabatak, S., Abdullahi, A.A., 2020. A study on cybersecurity challenges in E-learning and database management system. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5.

Hatcher, W., Meares, W.L., Heslen, J., 2020. The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. J. Cyber Policy 5, 302–325.

ITU, 2022. Definition of Cybersecurity [Online] Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx .

Buja, A.G., 2021. Cyber Security Featuresfor National E-Learning Policy. Turkish J. Comput. Mathematics Educat. (TURCOMAT) 12, 1729–1735.

Graham, J., Olson, R., Howard, R., 2016. Cyber Security Essentials. CRC Press.

Khan, S.K., Shiwakoti, N., Stasinopoulos, P., 2022. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accident Analysis Prevent. 165, 106515.

The-European-Parliament-Council, 2016. General data protection regulation-GDPR. J. Europ. Union 4, 1–88. https://gdpr-info.eu/.

Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J., Brummel, B.J., 2022. Organizational science and cybersecurity: abundant opportunities for research at the interface. J. Bus. Psychol. 37, 1–29.

Wu, C.-H.J., Irwin, J.D., 2016. Introduction to Computer Networks and Cybersecurity. CRC Press.

Statista. Countries with the highest number of internet users as of February 2022 [Online]. Available: https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/

Chukwu, M.A., Idoko, E.C., 2021. Inhibitors of electronic banking platforms' usage intention in deposit money banks: perspectives of elderly customers in developing economy. Sch. Bull 7, 134–145.

Laurer, M., Seidl, T., 2021. Regulating the european data-driven economy: a case study on the general data protection regulation. Policy Intern 13, 257–277.

D. Miralis, P. Gibson, and J. Ceic. Australia: cybersecurity laws and regulations, viewed 24 January 2022, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia [Online].

Shaykevich, A., 2019. The king of the CASL: canada's anti-spam law invades the United States. Brooklyn Law Rev. 84, 1321–1353.

Wei, D., 2020. From fragmentation to harmonization of consumer law: the perspective of China. J. Consumer Pol. 43, 35–56.

Kethineni, S., 2020. Cybercrime in India: laws, Regulations, and Enforcement Mechanisms. In: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer, Macmillan, Cham, pp. 305–326 T. Holt and A. Bossler.

A. El-Muhammady, "Malaysia: balancing national development, national security, and cybersecurity policy," in *Routledge Companion to Global Cyber-Security Strategy*, S. N. Romaniuk and M. Manjikian, Eds., ed: Routledge, 2021, pp. 325–336.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., 2021. Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. 105, 102248.

Hadji-Janev, M., Bogdanoski, M., 2015. Handbook of Research On Civil Society and National Security in the Era of Cyber Warfare. IGI Global.

Lloyd, I., 2020. Information Technology Law. Oxford University Press.

Jang-Jaccard, J., Nepal, S., 2014. A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 80, 973–993.

Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. Europ. J. Informat. Syst. 25, 231–251.

Bahuguna, A., 2015. FIRe: firefox for Computer Security Incident Reporting and Coordination. IITM J. Manage. IT 6, 3–11.

Maghu, S., Sehra, S., Bhardawaj, A., 2014. Inside of Cyber Crimes and Information Security: threats and Solutions. Int. J. Inform. Comput. Technol. 4, 835–840.

Muhammad, N.B., Kandil, A., 2021. Information protection of end users on the web: privacy issues and measures. Int. J. Inf. Comput. Secur. 15, 357–372.

Rajaretnam, T., 2020. A review of data governance regulation, practices and cyber security strategies for businesses: an Australian perspective. Int. J. Technol. Manage. Informat. Syst. 2, 1–17.

Cavelty, M.D., 2014. Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. Sci. Eng. Ethics 20, 701–715.

ICLG. 2022 Cybersecurity-laws-and-regulations [Online]. Available: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., Sarrafzadeh, H., 2014. The global cyber security workforce: an ongoing human capital crisis. In: 14th Global Business and Technology Association Conference, Baku, Azerbaijan, pp. 173–184.

Oltramari, A., Ben-Asher, N., Cranor, L., Bauer, L., Christin, N., 2014. General requirements of a hybrid-modeling framework for cyber security. In: 2014 IEEE Military Communications Conference, Baltimore, MD, USA, pp. 129–135.

Maung, T.M., Thwin, M.M.S., 2017. Proposed effective solution for cybercrime investigation in Myanmar. Int. J. Engin. Sci. 6, 1–7.

Coventry, L., Briggs, P., Jeske, D., van Moorsel, A., 2014. SCENE: a structured means for creating and evaluating behavioral nudges in a cyber security environment.

In: International conference of design, user experience, and usability, Cham, pp. 229–239.

Muhaya, F.T.B., Bakry, S.H., 2010. An approach for the development of national information security policies. Int. J. Adv. Sci. Technol. 21, 1–10.

Graves, J.T., Acquisti, A., Christin, N., 2016. In: Big Data and Bad data: On the Sensitivity of Security Policy to Imperfect Information, 83. University of Chicago Law Review, pp. 117–137.

Luiijf, E., Besseling, K., De Graaf, P., 2013. Nineteen national cyber security strategies. Intern. J. Critical Infrastruc. 6 9, 3–31.

Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., Tonks, S., 2016. The risk assessment of ERTMS-based railway systems from a cyber security perspective: methodology and lessons learned. In: International Conference on Reliability, Safety, and Security of Railway Systems, Cham, pp. 3–19.

Shackelford, S.J., Russell, S., Haut, J., 2015. Bottoms up: a comparison of voluntary cybersecurity frameworks. UC Davis Business Law J. 16, 217.

Carr, M., 2016. Public–private partnerships in national cyber-security strategies. Int Aff 92, 43–62.

Manwaring, K., Hanrahan, P.F., 2019. BEARing responsibility for cyber security in Australian financial institutions: the rising tide of directors' personal liability. J. Bank. Finan. Law Practice 30, 20–42.

Tranfield, D., Denyer, D., Smart, P., 2003. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British J. Manage. 14, 207–222.

Alzoubi, Y., Gill, A., 2021. The Critical Communication Challenges Between Geographically Distributed Agile Development Teams: empirical Findings. IEEE Trans. Prof. Commun. 64, 322–337.

Alzoubi, Y.I., Gill, A.Q., 2020. An Empirical Investigation of Geographically Distributed Agile Development: the Agile Enterprise Architecture is a Communication Enabler. IEEE Access 8, 80269–80289.

Zainal, Z., 2007. Case study as a research method. J. kemanusiaan 5.

Calderaro, A., Craig, A.J., 2020. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. Third World Q 41, 917–938.

WhiteHouse. The Comprehensive National Cybersecurity Initiative. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative, viewed 2 February 2022 [Online].

J. Baadsgaard. 2022 Cybersecurity Laws & Regulations [Online]. Available: https://www.ipohub.org/cybersecurity-laws-regulations/

Le, V.H., Zamora, B., 2018. The Price of a Data Breach. ISACA J. 4, 1–11.

Sabol, M.A., 1999. Identity Theft and Assumption Deterrence Act of 1998-Do Individual Victims Finally Get Their Day in Court. Loyola Consum. Law Rev. 11, 165–173.

Odoyo, S.G., 2010. The effects of US anti-terrorist laws on international business and trade. Syracuse J. Int. Law Commerce 38, 257.

Harrop, W., Matteson, A., 2014. Cyber resilience: a review of critical national infrastructure and cyber security protection measures applied in the UK and USA. J. Bus. Contin. Emer. Plan 7, 149–162.

Spitzer, R.J., 2014. New York state and the New York safe act: a case study in strict gun laws. Albany Law Rev 78, 749–787.

FTC. Federal trade commission act. federal trade commision. https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act, viewed 30 January 2022 [Online].

Westhoff, P.C., 2008. The Energy Independence and Security Act of 2007: Preliminary Evaluation of Selected Provisions (FAPRI-MU #01-08). Food and Agricultural Policy Research Institute, University of Missouri Columbia.

Kigerl, A.C., 2009. CAN SPAM Act: an Empirical analysis. Int. J. Cyber Criminol. 3, 566–589.

Gijrath, S., van der Hof, S., Lodder, A.R., Zwenne, G.-J., 2018. Concise european data protection, e-commerce and IT law. Kluwer Law Int. BV.

N. Van der Meulen, E. Jo, and S. Soesanto. Cybersecurity in the European Union and beyond: exploring the threats and policy responses, viewed 19 January 2022, http://resp.llas.ac.cn/C666/handle/2XK7JSWQ/4077 [Online].

S. Sarma. Cyber Security Mechanism in European Union, viewed 19 January 2022, https://icwa.in/show_content.php?lang=1&level=3&ls_id=618&lid=561 [Online].

Fuster, G.G., Jasmontaite, L., 2020. Cybersecurity regulation in the European union: the digital, the critical and fundamental rights. In: The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. Springer, Cham, pp. 97–115 M. Christen, B. Gordijn, and M. Loi, Eds..

Murdoch, S., 2021. Cybersecurity Information Sharing. The Oxford Handbook of Cyber Security. Oxford Handbooks Online - Scholary Research Review, London P. Cornish, Ed., ed.

Birnhack, M.D., 2008. The EU data protection directive: an engine of a global regime. Comput. Law Secur. Rev. 24, 508–520.

Faure, M., 2017. The development of environmental criminal law in the EU and its member states. Rev. Europ., Comparat. Int. Environ. Law 26, 139–146.

Lodder, A.R., Murray, A.D., 2017. EU Regulation of e-commerce: a Commentary. Edward Elgar Publishing.

Pappas, C.W., 2002. Comparative US & (and) EU Approaches to E-Commerce Regulation: jurisdiction, Electronic Contracts, Electronic Signatures and Taxation. Denver J. Int. Law Policy 31, 325–347.

Kontargyris, X., 2018. IT Laws in the Era of Cloud-Computing: A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy. Nomos Verlagsgesellschaft, Baden-Baden, Germany.

Katulić, T., 2018. Transposition of EU network and information security directive into national law. In: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1143–1148.

Vogelsang, I., 2015. Will the US and EU telecommunications policies converge? A survey. Economia e Politica Industriale 42, 117–155.

Goddard, M., 2017. The EU General Data Protection Regulation (GDPR): european regulation that has a global impact. Int. J. Market Res. 59, 703–705.

Weatherill, S., 2013. EU Consumer Law and Policy. Edward Elgar Publishing.

IqtiyaniIlham, N., Hasanuzzaman, M., Hosenuzzaman, M., 2017. European smart grid prospects, policies, and challenges. Renewable Sustainable Energy Rev. 67, 776–790.

Manwaring, K., 2009. Canning the spam five years on: a comparison of spam regulation in Australia and the US. Comput. Law 76, 5–11.

C. Brookes. Cyber Security: time for an integrated whole-of-nation approach in Australia, viewed 20 January 2022, https://defence.gov.au /[O*nline*].

Borgman, B., Mubarak, S., Choo, K.-K.R., 2015. Cyber security readiness in the South Australian government. Comp. Standards Interfaces 37, 1–8.

AustralianHomeaffairs. Submissions and discussion papers [Online]. 2022 Available: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers

Bennett Moses, L., Churches, G., Parker, N., 2019. Submission to the review of telecommunications and other legislation amendment (assistance and access) act 2018. UNSW Law Res. Paper 20, 1–6.

Kyriakakis, J., 2007. Australian prosecution of corporations for international crimes: the potential of the Commonwealth Criminal Code. J. Int. Crimin. Just. 5, 809–826.

Webb, T., 2007. Electronic case management in New South Wales, Australia. Inform. Commun. Technol. Law 16, 73–86.

White, P., 2007. The Regulation of Electronic Funds Transfer in Australia: an Integrated Multidisciplinary Approach. Doctor of Business Administration, Victoria University, Melbourne, Australia.

Chan, N., Coronel, S., Ong, Y.C., 2003. The Threat of the Cybercrime Act 2001 to Australian IT Professionals. In: 1st Australian Undergraduate Students Computing Conference, Melbourne, Australia, pp. 25–33.

Nicholls, R., 2012. Right to privacy: telephone interception and access in Australia. IEEE Technol. Soc. Mag. 31, 42–49.

Watts, D., Casanovas, P., 2019. Privacy and data protection in Australia: a critical overview. In: Workshop on Privacy and Linked Data, Cambridge, Massachusetts, United States, pp. 1–5.

Malbon, J., Nottage, L., 2013. Consumer Law & Policy in Australia & New Zealand. Federation Press.

Haidar, A.M., Muttaqi, K., Sutanto, D., 2015. Smart Grid and its future perspectives in Australia. Renew. Sustain. Energy Rev. 51, 1375–1389.

Bailetti, A.J., Craigen, D., Hudson, D., Levesque, R., McKeen, S., Walsh, D.A., 2013. Developing an innovation engine to make Canada a global leader in cybersecurity. Technol. Innovat. Manage. Rev. 5–14.

Bell, C., 2006. Surveillance strategies and populations at risk: biopolitical governance in Canada's national security policy. Secur. Dialogue 37, 147–165.

Phillips, M., 2018. International data-sharing norms: from the OECD to the general data protection regulation (GDPR). Hum. Genet. 137, 575–582.

Jaar, D., Zeller, P.E., 2008. Canadian privacy law: the personal information protection and electronic documents act (PIPEDA). Int. In-House Counsel J. 2, 1135–1146.

M. Lukings and A.H. Lashkari. Understanding Canadian Cybersecurity Laws: measuring up — Outlining existing federal cybersecurity legislation in Canada, the UK, Australia, and the US (Article 8) 2022 [Online]. Available: https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-measuring-up-outlining-existing-federal-cybersecurity-legislation-in-canada-the-uk-australia-and-the-us-article-8/440343

King, D., 2012. Chip-and-PIN: success and challenges in reducing fraud. Retail Payments Risk Forum 1–26.

Weiland, R., 2001. The uniform electronic commerce act: removing barriers to expanding e-commerce. Appeal: Rev. Current Law Law Reform 7, 6–12.

Frieden, R., 2005. Lessons from broadband development in Canada, Japan, Korea and the United States. Telecomm Policy 29, 595–613.

Perrin, B., 2009. Taking a vacation from the Law? Extraterritorial criminal jurisdiction and section 7 (4.1) of the criminal code. Canad. Criminal Law Rev. 13, 175–209.

Piché, C., Saumier, G., 2018. Consumer collective redress in Canada. Japanese Yearbook Int. Law 61, 231–259.

Streich, M.E., 2010. Green energy and green economy act, 2009: a Fit-ing policy for North America. Int. In-house Counsel J. 33, 419–452.

Feng, Y., 2019. The future of China's personal data protection law: challenges and prospects. Asia Pacific Law Rev. 27, 62–82.

Subsorn, P., Limwiriyakul, S., 2012. A case study of internet banking security of Mainland Chinese banks: a customer perspective. In: 4th International Conference on Computational Intelligence, Communication Systems and Networks, Phuket, Thailand, pp. 189–195.

Kshetri, N., 2013. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electron. Comm. Res. 13, 41–69.

A. Huld. China cybersecurity regulations – what do the new draft regulations say? [Online]. 2022 Available: https://www.china-briefing.com/news/china-cybersecurity-regulations-what-do-the-new-regulations-say/

Chen, J., Sun, J., 2021. Understanding the Chinese Data Security Law. Int. Cybersecurity Law Rev. 2, 209–221.

Swartz, N., 2007. Canada reviews PIPEDA. Inform. Manag. 41, 8.

Austin, G., 2018. Cybersecurity in China: The next Wave. Springer, Cham.

Huang, W., Li, X., 2019. The E-commerce Law of the People's Republic of China: e-commerce platform operators liability for third-party patent infringement. Computer Law Secur. Rev. 35, 105347.

Wang, M., Wang, M., 2005. Introduction to the electronic signatures law of people's republic of China. Digital Evidence and Electronic Signature Law Rev. 2, 79–85.

Parasol, M., 2018. The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. Comput. Law Secur. Rev. 34, 67–98.

Fujikawa, H., 2013. Dependable and Trustworthy Information System under Regional Restrictions. In: International Conference on Signal-Image Technology & Internet-Based Systems, Kyoto, Japan, pp. 667–672.

Brown, M.A., Zhou, S., Ahmadi, M., 2018. Smart grid governance: an international review of evolving policy issues and innovations. WIREs: Energy and Environment 7, e290.

Prasad, R., Manoharan, G., Sahay, N., 2016. Topical Issues in the Regulation of E–commerce in India. US-India Business Council Legal Serv. Newslett. winter 2016, 1–21.

Bilbao-Osorio, B., Dutta, S., Lanvin, B., 2014. The Global Information Technology Report 2014: Rewards and Risks of Big Data. Johnson Cornell University, Geneva, Switzerland.

Sumanjeet, D., 2010. The state of e-commerce laws in India: a review of Information Technology Act. Int. J. Law Manage. 52, 265–282.

Rajvanshi, G., Singhal, M.M., 2016. Data privacy law and growth of E-Commerce: an Indian perspective. Bharati Law Rev. 2, 1–36.

Srikanth, V., Dhanapal, R., 2011. A business review of e-retailing in India. Int. J. Business Res. Manage. 1, 105–121.

Dalei, P., Brahme, T., 2014. Cyber Crime and Cyber Law in India: an Analysis. Int. J. Human. Appl. Sci. (IJHAS) 2, 106–109.

Kumar, P.R., Raj, P.H., Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Comput. Sci. 125, 691–697.

Patel, N., Conners, S.E., 2008. Outsourcing: data security and privacy issues in India. Issues Information Syst 9, 14–20.

B. Mohanty, "The encryption debate in India," *Carnegie Endowment*, pp. 1–10, 2019.

Patidar, S., 2013. The Consumer Protection Act, 1986 of India-25 Years of Enactment: a Critical Study. Pacific Business Review International 6, 1–5.

DSCI. 2022 Legal and Policy Issues in Cloud Computing - Discussion Paper based on Data Security Council of India (DSCI)-BSA Workshop [Online].

Wahid, S.D.M., Buja, A.G., Jono, M.N.H.H., Aziz, A.A., 2021. Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: a structural equation modeling. Int. J. Adv. Technol. Engin. Explor. 8, 73–81.

Binti Mohamed, D., 2013. Combating the threats of cybercrimes in Malaysia: the efforts, the cyberlaws and the traditional laws. Computer Law Secur. Rev. 29, 66–76.

P. Pătraşcu, "The appearance and development of national cyber security strategies," in *ELearning and Software for Education*, 2018, pp. 53–59.

Shahwahid, F.M., Miskam, S., 2015. Personal data protection act 2010: taking the first steps towards compliance. J. Manage. Muamalah 5, 64–75.

Saripan, H., Hamin, Z., 2011. The application of the digital signature law in securing internet banking: some preliminary evidence from Malaysia. Procedia Comput. Sci. 3, 248–253.

Hussein, S.M., 2000. The Malaysian Communications and Multimedia Act 1998-Its Implications on the Information Technology (IT) Industry. Informat. Commun. Technol. Law 9, 79–88.

Abdullah, F., Mohamad, N.S., Yunos, Z., 2018. Safeguarding Malaysia's cyberspace against cyber threats: contributions by cybersecurity Malaysia. OIC-CERT J. Cyber Secur. 1, 22–31.

Yusoff, S.S.A., Isa, S.M., Aziz, A.A., 2012. Legal approaches to unfair consumer terms in Malaysia, Indonesia and Thailand. J. Soc. Sci. Human. 20, 43–55.

AlAhmad, A.S., Kahtan, H., Alzoubi, Y.I., Ali, O., Jaradat, A., 2021. Mobile cloud computing models security issues: a systematic review. J. Netw. Comput. Appl. 190, 103152.

Rosenzweig, P., Lieberman, S.J., 2012. Cybersecurity Act of 2012: revised cyber bill still has problems. In: The Heritage Foundation - Issue Brief, 3675, pp. 1–2.

Knapp, K.J., 2009. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions: Threat Analysis and Response Solutions. IGI Global.

Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C., 2011. Future e-enabled aircraft communications and security: the next 20 years and beyond. Proc. IEEE 99, 2040–2055.

Crandall, R.W., 2005. Competition and chaos: US Telecommunications Since the 1996 Telecom Act. Brookings Institution Press.

S.Y. Laurent, *Conflicts, Crimes and Regulations in Cyberspace* vol. 2: Wiley, 2021.

Buchanan, W.J., 2011. Introduction to Security and Network Forensics. CRC Press.

N. Wilson, "Australia's National Broadband Network–A cybersecure critical infrastructure?," *Comput. Law Secur. Rev.*, vol. 30, pp. 699–709, 2014.

Li, R., Zhao, Z., Sun, Q., Chih-Lin, I., Yang, C., Chen, X., 2018. Deep reinforcement learning for resource management in network slicing. IEEE Access 6, 74429–74441.

Srinivas, J., Das, A.K., Kumar, N., 2019. Government regulations in cyber security: framework, standards and recommendations. Future Generation Comput. Syst. 92, 178–188.

C.B. Casagran, *Global Data Protection in the Field of Law enforcement: an EU Perspective*: Routledge, 2016.

Alshammari, S.T., Albeshri, A., Alsubhi, K., 2021. Integrating a High-Reliability Multicriteria Trust Evaluation Model with Task Role-Based Access Control for Cloud Services. Symmetry (Basel) 13, 492.

Badotra, S., Sundas, A., 2021. A systematic review on security of E-commerce systems. Int. J. Appl. Science and Engineering 18, 1–19.

Hartono, E., Holsapple, C.W., Kim, K.-Y., Na, K.-S., Simpson, J.T., 2014. Measuring perceived security in B2C electronic commerce website usage: a respecification and validation. Decis Support Syst. 62, 11–21.

Villa, E., Ruiz, L., Valencia, A., Picón, E., 2018. Electronic commerce: factors involved in its adoption from a bibliometric analysis. J. Theoret. Appl. Electron. Comm. Res. 13, 39–70.

Tan, C., Lee, S.Z., 2021. Adoption of enterprise risk management (ERM) in small and medium-sized enterprises: evidence from Malaysia. J. Account. Organizat. Change 18, 100–131.

Basu, S., Jones, R., 2003. E-commerce and the law: a review of india's information technology act, 2000. Contemp South Asia 12, 7–24.

Min, K.-S., Chai, S.-W., Han, M., 2015. An international comparative study on cyber security strategy. Int. J. Secur. Its Appl. 9, 13–20.

Persadha, P., Waskita, A., Yazid, S., 2015. Comparative study of cyber security policies among malaysia, australia, indonesia: a responsibility perspective. In: Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, pp. 146–150.

Chaimaa, B., Najib, E., Rachid, H., 2021. E-banking overview: concepts, challenges and solutions. Wireless Personal Commun. 117, 1059–1078.

Kiljan, S., Simoens, K., Cock, D.D., Eekelen, M.V., Vranken, H., 2016. A survey of authentication and communications security in online banking. ACM Comput. Surv. (CSUR) 49, 1–35.

Binding, J., Purnhagen, K., 2011. Regulations on E-commerce consumer protection rules in China and Europe compared-same same but different. J. Intellect. Property, Inform. Technol. E-Commerce Law 2, 186–194.

Albrecht, D., 2018. Chinese cybersecurity law compared to EU-NIS-directive and German IT-security Act. Comp. Law Rev. Int. 19, 1–5.

van de Weijer, S.G., Leukfeldt, R., Bernasco, W., 2019. Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. Europ. J. Criminol. 16, 486–508.

Wang, X., Liang, Q., Mu, J., Wang, W., Zhang, B., 2015. Physical layer security in wireless smart grid. Secur. Commun. Networks 8, 2431–2439.

Gunduz, M.Z., Das, R., 2020. Cyber-security on smart grid: threats and potential solutions. Comp. Networks 169, 107094.

Miedema, T.E., 2018. Consumer protection in cyber space and the ethics of stewardship. J. Consumer Policy 41, 55–75.

Chin, O.T., Yusoff, S.S.A., 2016. Remedy as of Right for Consumer Protection. Mediterr. J. Soc. Sci. 7, 142–148.

Kerber, W., 2016. Digital markets, data, and privacy: competition law, consumer law and data protection. J. Intellect. Property Law Practice 11, 856–866.

McIntosh, C., 2015. Cyber-security: who will provide protection? Comput. Fraud Secur. 2015, 19–20.

Idowu, K.-.I., 2019. The insurance data security model law: strengthening cybersecurity insurer-policyholder relationships and protecting consumers. Roger Williams UL Rev 24, 115–142.

Walton, S., Wheeler, P.R., Zhang, Y., Zhao, X., 2021. An Integrative Review and Analysis of Cybersecurity Research: current State and Future Directions. J. Inform. Syst. 35, 155–186.

Haddad, C., Binder, C., 2019. Governing through cybersecurity: national policy strategies, globalized (in–) security and sociotechnical visions of the digital society. Österreichische Zeitschrift Für Soziologie 44, 115–134.

NCSC. Cyber Security Information Sharing Partnership (CiSP). National Cyber Security Center. https://www.ncsc.gov.uk/cisp, viewed 30 January 2022 [Online].

Dizon, M.A.C., Upson, P.J., 2021. Laws of encryption: an emerging legal framework. Comput. Law Secur. Rev. 43, 105635.

Wang, M., Zhang, Z., Chen, C., 2016. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme. Concurr. Comput. 28, 1237–1245.

Segal, A., 2016. In: China, Encryption Policy, and International Influence, 1610. Hoover Institution, pp. 1–16.

Prasad, R.S., 2022. Criticism Forces Government to Roll Back Its Draft Encryption Policy. The Indian Express https://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/.

Devi, S., 2019. Cyber security in the national security discourse. World Affairs 23, 146–159.

Chatterjee, S., Sarkar, P., 2011. Identity-based Encryption. Springer Science & Business Media.

Relyea, H.C., 1986. Access to government information in the information age. Public Adm. Rev. 46, 635–639.

Neama, G., Alaskar, R., Alkandari, M., 2016. Privacy, security, risk, and trust concerns in e-commerce. In: Proceedings of the 17th International Conference on Distributed Computing and Networking, pp. 1–6.

Yee, G., 2006. Privacy Protection For E-Services. IGI Global.

Cole, D., Fabbrini, F., Schulhofer, S., 2017. Surveillance, Privacy and Trans-atlantic relations. Bloomsbury Publishing.

Yang, P., Xiong, N., Ren, J., 2020. Data security and privacy protection for cloud storage: a survey. IEEE Access 8, 131723–131740.

Tsesis, A., 2019. Data subjects' privacy rights: regulation of personal data retention and erasure. UniversityColorado Law Rev. 90, 593–629.

Hoffman, S.K., McGinley, T.G., 2010. Identity theft: a Reference Handbook. ABC-CLIO, California, USA.

Steel, C.M., 2019. Stolen identity valuation and market evolution on the dark web. Int. J. Cyber Criminol. 13, 70–83.

Somani, U., Lakhani, K., Mundra, M., 2010. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In: 1st International Conference On Parallel, Distributed and Grid Computing (PDGC), Solan, India, pp. 211–216.

Alzoubi, Y.I., Osmanaj, V.H., Jaradat, A., Al-Ahmad, A., 2021. Fog computing security and privacy for the internet of thing applications: state-of-the-art. Secur. Privacy 4, e145.

Dunham, M., Bradshaw, A., 2004. The Spam Act. Law Society of South Australia.

Beardwood, J., Stern, G.M., 2014. Entry into Force of Canada's Anti-Spam Law. Comput. Law Rev. Int. 15, 44–47.

Kigerl, A.C., 2015. Evaluation of the CAN SPAM ACT: testing deterrence and other influences of e-mail spammer legal compliance over time. Soc. Sci. Comput. Rev. 33, 440–458.

GCSCC. 2022 Assessing national cybersecurity capacity [Online]. Available: https://gcscc.ox.ac.uk/cmm-dimensions-and-factors

Dutton, W.H., Creese, S., Shillair, R., Bada, M., 2019. Cybersecurity capacity: does it matter? J. Information Policy 9, 280–306.

Naseir, M.A.B., 2021. National Cybersecurity Capacity Building Framework For Counties in a Transitional Phase. Bournemouth University.

Collett, R., 2021. Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. J. Cyber Policy 1–20.

F. Nakhli. Cybersecurity development areas of action: an overview [Online]. 2022 Available: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2019/Workshop%20Kyiv/5%20%D0%A4%D0%B0%D1%80%D0%B8%D0%B4%20ITU%20Workshop%2016%20May%20-%20Farid%20Nakhli.pdf

ENISA. National cybersecurity capabilities: new self-assessment framework to empower EU member states [Online]. 2022 Available: https://www.enisa.europa.eu/news/enisa-news/national-cybersecurity-capabilities-framework

GFCE. 2022 Assessing and developing cybersecurity capability [Online]. Available: https://thegfce.org/initiatives/assessing-and-developing-cybersecurity-capability/

UNODA. UNODA and cybersecurity tech Accord announce "Apps 4 digital peace!" contest [Online]. Available: 2022 https://www.un.org/disarmament/update/unoda-and-cybersecurity-tech-accord-announce-apps-4-digital-peace-contest/

Fishburn, P.C., 1967. Additive utilities with incomplete product sets: application to priorities and assignments. Oper. Res. 15, 537–542.

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., Apostolopoulos, T., 2018. A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. Comput. Secur. 74, 371–383.

Shafqat, N., Masood, A., 2016. Comparative analysis of various national cyber security strategies. Int. J. Comp. Sci. Inform. Secur. 14, 129–136.

Kurt, A., 2015. Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study. Carnegie Mellon University.

Turner, K., Stough, C., 2020. Pre-service teachers and emotional intelligence: a scoping review. Austral. Educat. Research. 47, 283–305.

T. Stratford and Y. Luo, "3 ways cybersecurity law in china is about to change," *Law360*, pp. viewed 20 January 2022, https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-to-change, 2016.

Goi, C.L., 2005. E-Banking in Malaysia: opportunity and challenges. Journal of Internet Banking and Commerce 10, 1–11.

Carroll, P., Kellow, A., 2021. The OECD: A Decade of Transformation: 2011–2021. Walter de Gruyter GmbH, Berlin.

Al-Garadi, M.A., Varathan, K.D., Ravana, S.D., 2016. Cybercrime detection in online communications: the experimental case of cyberbullying detection in the Twitter network. Comput. Human Behav. 63, 433–443.

Tissir, N., El Kafhali, S., Aboutabit, N., 2021. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J. Reliable Intel. Environ. 7, 69–84.

Alok Mishra is Professor in Informatics and Digitalization at Molde University College (A Specialized University in Logistics) Norway. He is also associated as Professor in Software Engineering at Atilim University, Turkey. His-areas of research interests are in software engineering, information system, information technology and artificial intelligence. Prof. Mishra is an editorial board member of many reputed journals including Computer Standards and Interfaces (Elsevier), Journal of Universal Computer Science, Computing & Informatics, Data Technologies, and Applications Journal etc. He is actively involved in editing special issues of reputed journals in his areas of research interest. Prof. Mishra had also extensive experience in online education related to Computing and Management disciplines. In teaching, he has received excellence in online education award by U21Global Singapore while in research he has been awarded by Scientific and Research Council of Turkey and Board of Management of University for outstanding publications in Science and Social Science Citation Indexed (Thomson Reuter) journals. He is a recipient of many scholarships, international awards and research projects.

Yehia **Alzoubi** received the M.*Sc*. degree in Information Technology from Central Queensland University Sydney, Rockhampton, QLD, Australia, and the Ph.D. degree in Information Management from the University of Technology Sydney, Sydney, NSW, Australia. He is an Assistant Professor with the Department of Management Information Systems, American University of the Middle East, Egaila, Kuwait. He has published in a number of international research journals and conferences, including Information and Management, the Journal of Strategic Security, IEEE Access, the Pacific Asia Conference on Information Systems, and the International Conference on Information Systems Development. His-research interests include agile development, information security and privacy, and big data processing.

Memoona Javeria Anwar is Ph.D. from the University of Technology Sydney, Sydney, NSW, Australia. Head of Compliance & Digital Strategy at Datazoo Australia. Memoona started her career as a passionate software developer and carries 7 years of extensive coding and software development experience in multiple programming languages. Memoona's area of expertise include privacy, information security, regulatory compliance, fraud prevention, blockchain and digital identity.

Asif Gill is an associate professor and director of the DigiSAS Lab, School of Computer Science, University of Technology Sydney. He received his Ph.D. from the University of Technology Sydney. He is also certified as a CISM, DVDM, ITILv3, and TOFAG. He specialises in agile software development, adaptive enterprise architecture and information security. He is academic cum practitioner with extensive experience in successfully delivering projects in various sectors including banking, consulting, education, finance, government, non-profit, software and telco. He conducts practice-oriented research that targets the challenges of academia, industry, government, and society. His work has appeared in major academic and industry conferences and journals. He is serving as a coordinating editor, a section editor, and an editorial board member of several academic journals.