A Comparative Analysis to Advancing the National Cybersecurity Strategy in Saudi Arabia

Abdulrahman A Alghamdi
College of Computing and Information Technology, Shaqra Univeristy, 11961, Saudia Arabia.
Alghamdia@su.edu.sa

Abstract

Cyberspace has dramatically expanded due to technological advancement. Nowadays, cyberspace is part of daily life experiences and socio-economical activities. Countries all over the world need to have their own National Cybersecurity Strategies (NCSS) to be protected from cyber risks and threats. NCSS states the strength of a given country's cybersecurity strength concerning the objectives, aims, vision, and cybersecurity mission of a country in question. Previously, many researchers have conducted studies on NCSS by contrasting the National Cybersecurity Strategy between different nations primarily for intercontinental teamwork and coordination of cybersecurity challenges globally. Purposefully, one of the main objectives is to evaluate and assess policy frameworks in various countries to combat the prevailing cyber threats. As a result, from the comparison of many policy frameworks on NCSS of many countries, it was discovered that more effort should put into National Cybersecurity of Saudi Arabia. This paper compares the cybersecurity strategy of Saudi Arabia with the NCSS of other fifteen countries such as the United States of America, Singapore, India, Japan, Malaysia, Kuwait, Canada, UK, China, Egypt, Bahrain, Hong Kong, Russia, Korea, and France. Saudi Arabia rank in cybersecurity has risen to be in the second rank in 2020. Compared to other developed countries, the results found that Saudi Arabia appears to be on the right track in ensuring the safety of its cyberspace. .

Keywords:
Cybersecurity strategy; Comparative study; Cybersecurity; Cybersecurity policy; Communication; Cyber-attack; Saudi Arabia .

1. Introduction

Cyberspace has dramatically expanded due to technological advancement. Nowadays, cyberspace is part of daily life experiences and socio-economical activities. Many people have embraced technology by storing their data and personal information in cyberspace's databanks, thus posing new security perils [1]. Massive data, the 'internet of things (IoT), and online storage are prone to cyberattacks, thereby jeopardizing people's data, company's data, and information if cyber attackers outdo the security protocols of cyberspace. Cyber-attacks are always creative and innovative in modifying their attacks. They have never fallen, and they will never stop attacking cyberspace. Subsequently, every nation should get reliable, resilient, and stable information communication technology (ICT) to counter the emerging cyber-attacks [1]. A country with a weak technological infrastructure is highly prone to cyber-attacks, and every country should enhance its ICT sectors to combat the cyber-attacks. Saudi Arabia somehow enhanced its Information

Communication Technology (ICT) sector to counter the cyber-attacks in the country. However, many organizations' in Saudi Arabia reported information and monetary loss cases linked to cyber threats [2]. Fortunately, Saudi Arabia turned into an IT-based country within ten years due to the rapid technology development started in early 1997. Strategically, in 2007 the Saudi government enforced the use of a computer as a pressing necessity at the individual level, health sectors, education sector, business institutions, and public sector levels. Consequently, the government unknowingly exposed a large number of its population to emerging cyber-attacks. Saudi Arabia raised eleven ranks from 2018 to be along with the UK in the second rank with 99.54 points [7].

The regulatory body of Saudi Arabia and CITC in Saudi Arabia conducted a survey annually, thus capturing alteration in IT penetration levels [2]. A large number of people penetrated computer use in individual and commercial undertakings elevated from 43% to 51% in 2007 and 2009, respectfully [3]. Saudi Arabia fully invested in ITES, the IT-enabled facilities, and IT groundwork. The Saudi government fully resorted to this strategy to improve the United Nation's ECDI, the E-government Development index, and the EPI or the E-participation index. Despite all this good strategy, the Saudi government did not lay down appropriate, resilient, desirable, and practical measures to counter the cyber-attack [3].

Cyberwarfare has emerged as a modern security encounter. Saudi Arabia is a major cyberattack target because of its digital and economic uprising, advancement in technology, and prosperity in the oil and gas industry in the country [4]. As a result, it will discourage a potential investor from investing in an insecure nation. Therefore, the reliable cybersecurity strategy plays an essential role in economic, social, national growth procedures by countering cyber threats. Consequently, it provides monetary security, enhancing nationwide resilience, legalized mandate, partisan imperativeness, shielding government secrets, enhancing international relations, thus promoting a country's public image [3]. Therefore, it is high time for Saudi Arabia to update its strategy to combat national and internal cyber threats in the country effectively. Therefore, this study will evaluate the existing NCSS of Saudi Arabia by comparing it with cybersecurity strategies of other countries of various technological ranks such as Canada, Singapore, United States of America, Kuwait, Egypt, Bahrain, Russia, Japan, Malaysia, India, China, France, United Kingdom, Hong Kong, and Korea. The comparison will find insights on how to improve Saudi Arabia's cybersecurity Strategy.

2. Background of the Study

The 21st century is marked as a technological era. Almost everything nowadays being operated by technology. Technology has advanced rapidly globally regardless of the continent. Technology has improved the living standards of people and the quality of life in modern society. Correspond-

ingly, Saudi Arabia is on the right track by adopting a long-term vision by running everything technologically [4]. Saudi's economy is digitalized, thus boosting the country's productivity. Equally, the state provides communication and information technology services to all sectors in the nation, thus becoming a key source of income by building a solid information technology industry. Unfortunately, the more advanced a country is technologically, the more complex cyber threats it faces [4].

Cybercrimes are not restricted in one country as federal law, and they can camouflage in a country's cyberspace if its cybersecurity is weak and unable to confront it. Therefore, a technological country such as Saudi Arabia exposes its citizen to cyber threats since many of its sectors are technology-based, thus becoming more prone to cyber-attacks. Cyber-attackers malevolently deactivate computers, take data, and use the penetrated computer as a blast-off for their subsequent assault [4]. Cybercriminals use various methods to launch cyber-attacks, including denial of service, phishing, malware, ransomware, and other malicious attacks.

Conversely, in the first three months of 2021, Saudi Arabia recorded over seven million cyber-attacks [4]. The new Kaspersky report postulates that cyber-attack rose by 104% from 983512 to 2000000 in February and March, respectfully. Kaspersky's statistics matched the government announcement on cyber-attack and validated the new Kaspersky report. The report claimed that most cyber-attacks were against the conventions used by workers while getting into their organizations remotely in their digital devices. Therefore, the information raises essentials for cybersecurity mindfulness. Equally, the country witnessed approximately 22.6 million cyber-attacks by cybercriminals on 'remote desktop protocols' (RDPs), the commonly known way of getting into servers or windows while hiding the computer IP addresses. In addition, there has been a loss of cybersecurity attempts in Saudi Arabia. At the G20 summit hosted in 2020, the 'Saudi Data and artificial Intelligence Authority (SDAIA)' stated that it terminated approximately 2,500,000 attacks under-connected gateways in the conference. Therefore, assessing the cybersecurity of Saudi Arabia is necessary to identify the loopholes and how to improve its security strategies [4] . The paper will be looking at how countries have taken profound measures such as creating awareness on cybersecurity to make their NCSS better and how Saudi Arabia's Strategy can be better compared with other countries with weak and robust security strategies, hence evaluating Saudi Arabia's system logically [14].

3. Literature Review

Cybersecurity must be in line with digital transformation. As discussed below, many countries are trying their best to review security strategies to be ready for the impending cyber-attacks.

3.1 Cybersecurity policy

All the stakeholders in a country's economy, such as businesses, companies, organizations, and the country at large, are gov-

erned and ruled by government policies that call everyone to adhere to a country's cybersecurity. Political stability can also be affected by cybersecurity [8] [12]. Whether the policies are favorable or not, policies serve as a guidelines to follow, thus covering the emerging cyber-attacks [26]. Prudent policymakers develop government policies to combat cybercrimes effectively [10]. The cybersecurity policy (NCSS) of Saudi Arabia stipulates suitable regulations and measures that guarantee the Saudi national cybersecurity in the middle of cyberspace full of cybercriminals. As a result, it will safeguard the government's vital data, secretes, and build trust to potential investors in Saudi Arabia as a trusted cyber-attack-free nation.

3.2 Roles of leaders in cybersecurity.

Politically, leaders should provide a strategic and witty lairdship to enforce and address the cybersecurity challenges in their countries. They should propose and publish reliable, resilient, and practical cybersecurity strategies in their nations. As a critical issue, cybersecurity should be endowed with the senior political levels since cyber-attacks directed hit the socio-economic structure of any country. Globally, ministries of interior and defense often oversee cybersecurity in their dockets [26]. For instance, France has centralized its National Cybersecurity Agency (ANSSI) as treated as the essential ministry in the country. The country has a particular unit whose primary task is to deal with cybercrime and everything malicious towards cybersecurity. Equally, in Singapore, the ministry of justice and security are accountable for cybersecurity issues [35]. Therefore, like other countries, the Saudi Arabia government should relocate the cybersecurity docket to a more senior political position and invest more funds. Similarly, Saudi citizens are also responsible for sharing their information to witness crafty activities from malicious cybercrimes to the Cyber-security ministry [33]. As a result, they will defend their local infrastructure since cyber-attacks directly hit socio-economic infrastructures.

3.3 Measures

Internationally recognized NCSS should be developed to counter cybercrime. The enacted laws and regulations should be upheld effectively by ensuring they are practical in curbing cybersecurity [33]. Therefore, the imposed laws, rules, and measures should be internationally recognized while addressing the country's national needs towards cybercrime. The working and practical legal steps will ensure that private and public sectors take cybersecurity matters seriously and no negligence by all sectors [34]. Consequently, it will be appropriate to assess the county's policy frameworks and cyber strategies, which should be revised often and accordingly. Many countries in this study have a clue on strategy review and evaluation, as is mentioned in their policy framework documents. Some country like Malaysia has not created a working strategy yet. As a result, it is prone to cyber-attacks as it lacks security auditing and security policy reviews. Other countries such as the United Kingdom and the Unit-

ed States have bodies responsible for reviewing the security protocols. Similarly, they are accountable for updating security strategies frequently [35].

3.4 National cybersecurity framework

Cybersecurity focus on safeguarding cyber environments, cyberspace, companies' data, and governments' secretes, among other fundamental functions. The national government should try its best to advance its cybersecurity protocols. It should design an impenetrable Cybersecurity system for cybercriminals. Poor cybersecurity leaves everything open for cybercriminals to launch attacks on government institutions, the education sector, business establishments, and private sectors, among other tech-based industries in a country. Equally, national cybersecurity should be keen as cybercrimes jeopardize international relations and lead to diplomacy issues in a nation. As a result, it breeds public relations issues as the attackers tend to steal classified government information. By exposing it in one way or another, two or several countries end up in diplomacy issues [36].

3.5 Significance of the International Telecommunication Union (ITU)

As for cyber-crimes, ITU plays a vital role in coordinating cyber-attack responses globally. Additionally, ITU structured a sub-segment called Global Cybersecurity Index (GCI), which Identifies cybersecurity gaps in countries and proposes how they can be improved and what areas need to be improved in their cyber environment [9]. GCI motivates and helps the less advanced countries strengthen their cybersecurity, harmonizes their practices, and encourages them to develop cybersecurity protocols that can be used globally.

3.6 Allocation of infrastructure and cyber awareness

Every country should invest a considerable funds in ensuring that everything is in place to advance cybersecurity protocols in the country [29]. Also, the government should create awareness of the impending danger of cybersecurity in the country and give the citizens preventive measures on how to deal with this modern problem. All the Cybersecurity strategies reinforce the importance of promoting cyber awareness to the mass population. Countries like the United States, France, Japan, and the United Kingdom promote cyber awareness by training parents and children. Equally, the UK, Malaysia, and India have used social media platforms to promote cyber awareness to the public. Malaysia, the UK, and the US have provided nationwide cybersecurity outreach programs to their citizens, such as cyber safety, getting sage online, and Cybersecurity month respectfully [29]. Japan intends to establish cybersecurity support services for its capacity building. The public can be provided with a civic education about cybersecurity and what actions they should take if they end up as victims of cybercrime. The ruling government should also work hand in hand with all stakeholders in the country, including the private sector while facing cybercrime. Due to a lack of mass awareness to the public about cybersecurity, Saudi Arabia

reported approximately 22 million cyber-attacks [25]. Therefore, Saudi Arabia to promote cyber education to every citizen in cybersecurity matters to counter cyberattacks.

4. Methodology

4.1 Types of research

This study will critically contrast and analyse cybersecurity using comparative research on multiple cybersecurity national strategies, thus identifying the cybersecurity gap in cyberspaces for improvements [11]. Therefore, critical and related research will be surveyed in this study, regarding analysing the cybersecurity strategy of Saudi Arabia in regards to addressing future cybersecurity challenges.

4.2 Research methods

The research method will critically review and analyze existing cybersecurity, cybercrime, and cybersecurity strategies. The work in this paper will cross-compare and critically contrast Saudi Arabia's cybersecurity strategies and policies with counterparts to; the UK, Singapore, Kuwait, Canada, Bahrain, Japan, USA, Malaysia, India, Egypt, Hong Kong, France, Russia, Korea, and China. This includes gathering publically disclosed information from specific domains related to national cybersecurity strategies from the countries mentioned above. As a result, the comparison will help understand the strong point and weaknesses of cybersecurity policies and strategies of Saudi Arabia strategy document [13].

4.3 Criteria used for selecting countries for the study

To make the comparison study effective, 15 countries were selected. UK, USA, and Canada represent developed countries with strong cybersecurity strategies. Malaysia represents a developing country doing well in its cybersecurity strategy. Equally, Egypt being in Africa as a developing country, has been incorporated in the study to assure the practicability of developing a security framework regardless of its condition. Similarly and to broaden the analysis, these countries i.e. Singapore, Japan, Malaysia, Korea, India, Kuwait, China, Hong Kong, France, Bahrain, and Russia, have been considered to compare Saudi Arabia's cybersecurity strategy.

First, the comparison involves categorizing the countries into developed and developing countries and ranking their NCSS according to ITU. The comparison criteria pertain to the countries' relationship at the top of the Cybersecurity ranking and those with low Cybersecurity ranking. Both are selected for comparison. The findings from the comparison should be used to enhance cybersecurity strategy in Saudi Arabia and other countries.

4.3.1 Developed countries for the study

Most countries in this set lead in ITU's Cybersecurity ranking in terms of cyber-readiness. As per UTI ranking, the USA performed remarkably better than France, as shown in Table 1.0.

Cybersecurity strategies from the UK, France, China, and France are globally recognized regarding to defensive and

Table 1. Advanced countries with the highest Cybersecurity ranking [9]

Ranking	Nation
1.0	USA
2.0	Canada
5.0	UK, Japan
9.0	France

offensive cybersecurity action plans. The other countries like Canada, Russia, Korea, India, Japan, Malaysia, Hong Kong, Saudi Arabia, Singapore, and Kuwait were selected. They often use ICT services, thus hiking cyber-attacks and cyber-crime rates in their regions [6]. Therefore, the analysis can help the countries secure and learn from the U.S.A., Canada, UK, and best performing developing countries' strategies. Therefore, the Study of Cyber strategies of these high-ranked countries will help decision-makers design an informed approach while creating the cybersecurity strategy document for their countries, hence preparing for [9]. Saudi Arabia in 2020 achieved the second rank and scored 98.54 points [7].

4.3.2 Developing countries

This set of countries comprises countries with a High Cybersecurity ranking in developing countries as per ITU, as shown in Table 2.1 below. The contrast of approaches from these developing nations highlights how developing countries quickly advanced their cybersecurity strategies to the extent of outshining some developed countries [9].

As seen from Table 2: In Asia, Malaysia is leading in cybersecurity strategies. However, despite so many cybersecurity attacks, India is performing better [9]. Conversely, Egypt has tried its best and is taking position nine, coinciding with France in ITU rank despite being found in Africa. These developing countries pose a significant challenge to some developed nations as to why their cybersecurity protocols are more secure and advanced despite having inadequate resources and infrastructure compared with developed countries.

Table 2. Developing Nations with high cybersecurity [9]

Ranking	Nation
3.0	Malaysia
9.0	Egypt
23.0	India
27.0	Korea
30.0	Hong Kong

4.4 Analysis model for administration structure

The structured research analysis on Assaf's research was conducted in 2008. This study will have scrutinized the institution-based analysis concerning 'Critical Information Infrastructure Protection (CIIP). The study reveals the degree of government intervention and control in the cybersecurity environment, as seen in figure 1 below [11].

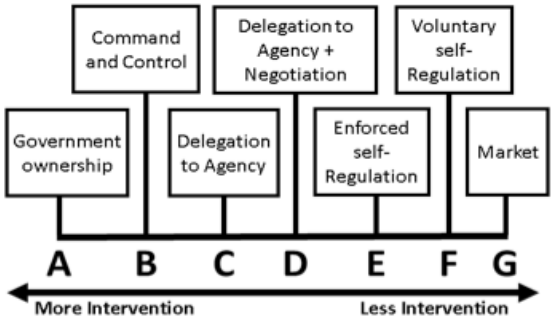

Figure 1: Critical information structure model [11]

In the government ownership structure, the CIIP is possessed and controlled by the government. The command and reg-

ulate policy regulates standards towards observing cybersecurity guidelines and protocols by stipulating rules and penalties upon breaching the laws [11]. Delegation to Agency sets the security standard and monitoring units. It is deputized to governmentally self-governing agencies. In the above policies, government intervention in all policies is the strongest one. However, the sovereignty of info protection by private sectors is limited. Equally, 'delegation to agency and negotiation' is accountable for conveying private corporations when setting specific criteria. The establishment upholds a more precipitative and less restrictive environment for all private and public sectors to harmonize [11]. Enforced self-regulation is a more stringent system that permits private sectors to develop processes, risk, performance, and management measures. The policy is then sanctioned and overseen by managerial companies autonomously. About' deliberate self-regulation strategy, all private organizations free can set standards, laws and implement them with no intervention from the government. Also, the market is self-regulated, and each business sets their standard and execute them [11]. As a result, the government keeps stabilizing the market and implementing cybersecurity measures per the consumers' needs.

On the other hand, the Assaf framework has its share of limitations. The framework only gauges the autonomy of private organizations and government intervention towards protecting and controlling the infrastructure [11]. Consequently, it is difficult to ascertain the model's effectiveness in implementing cybersecurity policies and strategies. The model further jeopardizes and risk countries with weak cybersecurity measures like Saudi Arabia.

4.5 Exclusive comparison measures

Due to the diversity of cybersecurity strategies, the study will compare and analyze cybersecurity of the selected set of countries so as evaluate what Saudi Arabia is missing in its cybersecurity policies and procedures [13]. The paper will compare countries in terms of their structures, policies, and national cybersecurity strategies (NCSS) in United States of America, Canada, India, Japan, Malaysia, Singapore, Bahrain, Kuwait, Hong Kong, Russia, France, United Kingdom, Egypt, Korea, and China.

4.5.1 NCSS comparison of the selected countries

Cybersecurity strategies gained popularity in 2008 when simple cyber-attacks were stated to be sponsored and counter sates globally, besides the already discussed countries [27]. The following is a timeline of the NCSS of the mentioned countries in table 2.3. The data of these nations have been extracted from public documents concerning cybersecurity strategies [17].

Table 3. The NCSS comparison of the selected countries in the study [27]

Country	Achievements, features, and timelines
Canada	It initiated its cybersecurity strategy and the action plan in 2010. The country has both security policies successfully since then. NCSS protects Canadians, the government, and industries from cyber-attacks. The country's NCSS enforces the National when implementing a protection plan for ICT infrastructure in collaborating with private sectors. The Canadian Cybersecurity strategy is characterized by safeguarding government systems, safeguarding its citizens in a cyber-environment, and creating partnerships Strategies and action plans for critical infrastructure policy [23]. The country does beyond the federal habits. Equally, it designed clear duties and responsibilities such as Manufacturing Canada Public security Canada, Guard Investigation and Advance Canada, Canadian Broadcasting Telecommunication command, Integrity Canada, Canadian Cyber response midpoint, Communication Safety Canada, and Canadian Sanctuary aptitude service. The Canadian Action plan calls for implementation procedures to enhance national cybersecurity at all levels and sectors in the country. The country is known for its quick response to cyber incidents. Globally, the government cooperates with international stakeholders in fighting global cyber cyber-attacks. Furthermore, the country creates awareness to the Canadian mass population on cybercrime by initiating cybersecurity studies and projects. The public awareness comprises; Stop. Think. Connect and get cyber safe. Canada created a cyber-Crime Fusion Unit and cyber strategies to fight cybercriminals in the country. Successfully, it developed and implemented a functioning antispam law and Shielding Canadians personal data Act. Canada cooperates with New Zealand, the UK, NATO, the UN, and the G8 in protecting its citizens from cybercriminals.
Japan	NCSS of Japan was amended in 2012. The country's NCSS is crafted from Japan's vigorous and resilient Cyber policy. The main objective in their cybersecurity strategy is to become a cyber-security community with a resilient, robust, and world-leading cyberspace globally. The approach focuses on changing the national cybersecurity policy, cyber environment and promoting cybersecurity security systems in Japan. Japan formulated agencies such as; (*Cyber-attacks analysis Council, National Information security center NISC), Japan CERT,* and *Information Security Centre Council (ISCP))*. The organizations are answerable for handling cybersecurity matters and countering cybersecurity attacks in the country. The organizations provide information security to maintain socio-economic in Japan [32]. Also, the agencies quickly respond to cyber threats and deal with cyber-attacks locally and internationally. The NCSS of Japan aims at improving its cybersecurity, creating cyber awareness to people, and instrument countermeasures. Japan institutes its goals from European Union, the U.S.A., France, the UK, and South Korea.
USA	The US NCSS has been active since 2003. NCSS is manned by the Department of Homeland security (DHS). DHS is responsible for cyberspace security. Also, it combats national cyber-attacks, creating national awareness and securing cyberspace in the US NCSS aims to make the US the only nation globally with a practical global strategy to endorse cyber-security in cyberspace [20].
Malaysia	Malaysian NCSS was sanctioned in 2006. The country's NCSS focus on technology, legislation, corporations, and to be accepted globally. The NCSS is characterized by eight pillars known as (Thrust First Eight) as follows; operative authority [17]. Jurisdictive and supervisory agenda, Cybersecurity outline, security culture, exploration and expansion, compliance and execution of policies, Cybersecurity readiness, and global cooperation [15].

Country	Achievements, features, and timelines
	The Malaysian strategy guards the Malaysian national information in all sectors, cybersecurity predicaments, and info security. Malaysia is the country leading in cybersecurity advancement in Asia as per the ITU ranking.
Egypt	It launched its NCSS in 2017. Egypt's NCSS is manned by the '*Egyptian Supreme Cybersecurity Council (ESCC).'* ESCC is responsible for creating, handling, responding, and combating cyber-attacks in Egypt. ESCC does a great job in making Egyptian cybersecurity strategies competitive as possible [16]. Despite being a developing country from Africa, ITU has been ranked position nine according to cybersecurity advancement.
France	Strategy launched in 2015. They were presented to Europe and the foreign affairs ministry in 2017. It was concerned with governing government secrets, security, and socio-economic facilities and—faced cyber-attacks with no border boundary. The strategy was reviewed in 2018. It is an international tool for France as it promotes cyber diplomacy in France.
India	Strategy formulated in 2020. NCSS aims to improve India's cyber awareness, especially the financial auditors [17]. Also, it aims at efficiently managing cyber crises and protecting the government, individual and Indian establishments.
Hong Kong	At the moment, Hong Kong has not proposed or issued any cybersecurity strategy yet. However, it combats cyber-attacks by the personal Data Ordinance (PDPO) in chapter 486 of its constitution. PDPO handles theft, blackmail, exposure of personal data, burglary, among other measures [17].
Korea	Strategy issued in 2019. Major cybersecurity issues pertain to cyber-terrorism, Cyber fraud, and cyber financial threads [15]. The country counters these issues by putting measures such as reporting mechanisms, government laws, and other initiatives formulated by the government.
Bahrain	Strategy launched in 2017. Due to the digital revolution, cybersecurity serves a major function in the Bahrain Kingdom [17]. The country has as advanced NCSS that General Directorate of the Anti-corruption unit. The NCSS aims at securing the Kingdom's cyberspace.
China	Strategy launched in 2017. China's NCSS is handled by the department of overseas affairs and the cyberspace management of China. The NCSS focuses on identifying plan action and cyberspace peace. China's goals are: Guarding the autonomy of china's security in cyberspace, developing international laws, governing the internet fairly, protecting citizens' rights and interests, and building a secure cyber environment [27].
Russia	Strategy launched in 2015. Russian NCSS aims at developing security for all citizens, creating a digital economy, protecting socio-economic infrastructures, and protecting the Russian interest in cyberspace [20]
Singapore	Strategy launched in 2016. The country's NCCs assure the citizens of their safety [30]. Singapore's cyber attackers are borderless and come from all over the world. It defines the clear goals, mission, and vision of cybersecurity in the cyber environment. The NCSS pillars will enhance information structure reliability, create awareness for cybercrimes, create vibrant cybersecurity, and form interaction associates.
Kuwait	Strategy launched in 2017. Kuwait's objectives are to create safe cyberspace, use cyberspace properly, and maintain socio-economic infrastructures [18].

Country	Achievements, features, and timelines
UK	UK's NCSS was established in 2010 and was later implemented in 2011. UK's *National Security Programme (NCSPP* is manned by the cybersecurity and info reassurance office under the institutionalized Cabinet office. The country has invested more than $ 114,247 million in cybersecurity. The NCSS in the UK combats cybercrime and is the safest place in the world for business. To be more resilient and guard its concern in cyberspace to create conducive cyberspace for UK citizens and have adequate cybercrimes to help implement its objectives [27]. The NCSS of the UK receives support from all stakeholders in-country. The UK promoted cybersecurity awareness by formulating Cyber fundamentals and street programs to create awareness for the public. Usually, it educates the citizens on safely using the internet services, as seen in the literature review of this paper [20]. The UK has invested many funds in scientific research on cybersecurity to advance its cybersecurity systems and strategies.
Saudi Arabia	Strategy Launched in 2013. Saudi Arabia has achieved a lot in ensuring that the country operates in a modernized ICT infrastructure. Since 2018 the government has achieved a 71 percent alphanumeric development in electronic control services [18]. Its digital transformation program goals propel the country toward its vision 2030 aims. Saudi's '*ministry of communication and information technology (MCIT)'* has implemented the technology in the country to the extent that it took the 7th position globally in (*World Economic Forum (WEF)*) for international competitiveness [30]. Significantly, MCIT initiated Yasser Program, which promotes e-commerce services quickly in the country [28]. In 2020, Saudi Arabia achieved the second rank in global scores and ranking of countries [7].

4.5.2 Assessment of the comparison

From comparing the 15 countries above, the countries face explicit and implicit cyberattacks concerning critical national infrastructure, national security citizens' social life, organized crimes, and cyberterrorism, as analyzed in table 4 below.

Table 4. The Explicit attack is marked by a tick and Implicitly attack to: Marked by*[2]

Country	To critical infra structure	National security,	The social life of citizens	From organized crime	from terrorism
USA.	√		√	√	√
UK	√	√		√	
Canada			√		√
Japan	√		√		
Malaysia	√	√		√	√
India	√	√			
Hong Kong	√	√	√	√	√
Kuwait		√	√		
Singapore	*	√	√	√	√
Russia	√	√	√		
China	√	√		√	√

Country	To critical infra structure	National security,	The social life of citizens	From organized crime	from terrorism
Bahrain	√	√	√		√
France	√		√		
Egypt		√	√	√	
Korea	√	√			√
Saudi Arabia	√	√	√	√	√

4.6. Similarity of the country's NCSS and common Ideas.

Both countries had their first NCSS versions, though, at different times since 2008. Both countries encounter cybercrimes from organized criminals. Also, both countries' objectives are focused on ensuring the safety of their citizens in cyberspace [2]. Both countries cooperate in cyber warfare globally. Each nation protects its cyberspace for economic prosperity.

4.7 Differences of NCSS of the selected countries

Developed countries have invested many funds in the Cybersecurity docket [19] . Due to enough funds, the UK and USA can conduct their regular research on Cybersecurity strategies. Countries like Malaysia, the UK, Japan, and the USA have successfully created awareness to the public compared to countries like Kuwait, Singapore, and Bahrain.

4.8 Research and Development in Cybersecurity

Research and development in cybersecurity strategies are essential for innovating cybersecurity measures through research and building cybersecurity strategies and security policies. The United Kingdom and the USA have invested many funds in R&D, thus making their cybersecurity strategies resilient and reliable globally [26]. In contrast to Saudi Arabia, I propose more funds to be invested in the research and development of the country's NCSS.

5. Discussion and Recommendations

The study has been structured in a comprehensive cross-sectional methodology. The study has critically assessed and evaluated cybersecurity policies and strategies of the selected countries [19]. Comparison of the fifteen nations has elicited cybersecurity challenges to countries not doing well as cybersecurity is concerned. Saudi Arabia is one country that experienced many cyber-attacks, approximately 23 million in three months. Therefore, it needs to be examined based on this study. The country should imitate the cybersecurity strategies of nations with solid cybersecurity strategies like the USA, the UK, and Malaysia [31].

Saudi Arabia should incorporate cybersecurity education into its curriculum to create awareness for cybercrime. The country is technological-based, and as a result, it encounters many cases of cyber-attacks as it exposes its citizens to attackers [24]. When

Saudi Arabia creates a civic education by educating its population, it will be safeguarding the mass population, thus safeguarding its socio-economic infrastructure [36].

Saudi's National Cybersecurity Strategy released in 2020 contains regulations and measures that aim to ensure the Saudi national cybersecurity, which is critical for protecting the government's vital data, secrets and building trust to potential investors in Saudi Arabia as a trusted cyber-attack-free nation. In 2020, Saudi Arabia through its National Cybersecurity Authority adopted and implemented a comprehensive approach in its strategy and working to achieve the vision and the national strategic goals that will aid in the protection of the cyberspace of Saudi Arabia and its important interests as outlined in the national cybersecurity strategy 2020. Compared to the other major global players, including the United States (US), United Kingdom (UK), France, and Canada, Saudi Arabia is not much left behind in its national cybersecurity policy 2020. However, internationally, ministries of Interior and Defence are mostly charged with overseeing national cybersecurity matters [26]. For instance, France has centralized its National Cybersecurity Agency (ANSSI), treated as the ministry in the country. The country has a unit whose primary task is to deal with cybercrime and everything malicious towards cybersecurity. Equally, in Singapore, the ministry of justice and security are accountable for cybersecurity issues [35].

Based on the analysis of the results, most countries except for Hong Kong have their NCSS, which are legally structured based on the respective country's legal framework. All have one common objective: safeguarding the county's cyberspace against both internal and external cyber threats/attacks. The USA, UK, Canada, and France are in particular, owing to the number of cyber-attacks they deal with. The Canadian cybersecurity strategy became effective in 2010 and sought to protect Canadians, the government, and industries from cyber-attacks. The strategy emphasizes collaborations and creating partnerships with the private sector. The core mandate of Canadian NCSS is prevention and protection of government systems, safeguarding its citizens in a cyber-environment, and creating partnerships Strategy and action plan for critical infrastructure policy against cyber threats [23]. The cyber approach covers the Manufacturing sector, Guard Investigation and Advance Canada, Canadian Broadcasting Telecommunication command, Integrity Canada, Canadian Cyber response midpoint, Communication Safety Canada, and Canadian Sanctuary aptitude service. The Canadian Action plan calls for implementation procedures to enhance national cybersecurity at all levels and sectors in the country. Another important feature is Canada's collaboration with the international community in dealing with cyber issues. Globally, the government cooperates with international stakeholders in fighting global cyber cyber-attacks. Canada cooperates

with New Zealand, the UK, NATO, the UN, and the G8 in protecting its citizens from cybercriminals. This is besides popular initiatives that aim to create awareness among the population.

Similarly, France launched its NCSS strategy in 2015, and presented it in Europe in 2017. The approach provides information on measures and strategies adopted to safeguard critical information, including government data and critical infrastructures. In contrast, the UK adopted its NCSS in 2010. The UK's National Security Programme (NCSPP) is one of the key features of the UK's strategy as evidenced by its massive funding to a tune of more than $ 114,247 million in cybersecurity. The NCSPP is considered one of the best globally. Like the Canadian Cybersecurity strategy, UK NCSS receives support from all stakeholders, including the private sector in country. Also, the UK promotes cybersecurity through street programs to create awareness for the public by educating citizens on responsible internet use, which is supported by previous literature [5]. The UK government has heavily invested in cybersecurity research, systems, and strategies. Additionally, the US NCSS has been active since 2003, manned by the Department of Homeland security (DHS). It combats national cyber-attacks, creating national awareness and securing cyberspace. Compared to other developed countries, Saudi Arabia in 2020 achieved the second rank in the global scores and ranking of countries with 99.54 points. Saudi Arabia also appears to be on the right track in ensuring the safety of its cyberspace. Having launched its strategy in 2013, Saudi Arabia has achieved a lot while ensuring it is up to date in ICT advancement. Saudi Arabia updated its national cybersecurity in 2020, in line with the Saudi Arabia 2030 visions. Saudi's NCSS 2020 emphasizes on collaboration with private stakeholders and other international stakeholders towards securing its cyberspace according to the 2020 national cybersecurity strategy. This appears to be a common trend with other major developed nations, specifically Canada, the USA, the UK ,and France. Results further indicate that Saudi Attained a 71 % alphanumeric development in electronic control services [18], suggesting that much is yet to be done. Saudi's 'ministry of communication and information technology (MCIT)' has implemented the technology in the country to the extent that it took the 7th position globally in (World Economic Forum (WEF)) for international competitiveness [30].

Summarily, all developed countries had their first NCSS versions, though, at different times since 2008 are focused on ensuring the safety of their citizens in cyberspace [2]. Most countries cooperate in cyber warfare globally, with each nation striving to protect its cyberspace for economic prosperity. Countries appear to invest heavily in cybersecurity [19], an initiative that allows regular research on the field of security, particularly in the UK and US, an area that Saudi Arabia seems to lag. This is besides collaboration and cooperation with the private sectors and spreading massive

public awareness on responsible use of the internet. Based on the national cybersecurity strategy 2020, Saudi Arabia has adopted a framework that will help protect its cyberspaces and critical interests/assets.

The main recommendations of this study can be summarized as follows:

- Saudi Arabia should imitate, compare and study the cybersecurity strategies of nations with solid cybersecurity strategies.
- Saudi Arabia should incorporate cybersecurity education into its curriculum to create awareness.
- Saudi Arabia should establish public-private partnership in the field of cybersecurity.
- Saudi Arabia should have international cooperation, as threats are not within Saudi boundaries.

6. Conclusion

By comparing the NCSS of the selected countries in the study, Saudi Arabia's NCSS is practical and needs some improvements to counter the next generation of cyber-attacks successfully. Making a developing country to be a technologically based country is not an easy task. At the same time, the government has exercised its due care/due diligence in implementing ICT infrastructures in the country [18]. However, the looming challenges of modern cybersecurity have tarnished the excellent effort the country has made towards making itself a technology-based country. Therefore, the Saudi Arabia government needs to improve cybersecurity awareness and outreach efforts to the public and support establishing different yet innovative cybersecurity awareness campaigns [22]. When the public knows the danger, they are facing in cyberspace, then they can take measures in educating and protecting themselves, especially when using their own high-tech devices at homes, schools, work, etc. Also, the country needs to advance its cybersecurity strategy to be globally applicable and coordinate efforts with other countries to make the world a better place to be. Therefore, with an appropriate cybersecurity design, Saudi Arabia can have a more resilient, reliable, and practical cybersecurity strategy that will address its current gaps and enable a safer digital transformational plan [21].

References

[1] G. Group, 2021. "Cybersecurity 2021 | Laws and Regulations | Saudi Arabia | ICLG", International Comparative Legal Guides International Business Reports, [Online]. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/saudi-arabia. [Accessed: 09- May- 2021].

[2] Sarker, K., Rahman, H., Rahman, K.F., Arman, M., Biswas, S. and Bhuiyan, T., 2019. "A comparative analysis of the cyber security strategy of Bangladesh", International Journal on Cybernetics & Informatics (IJCI), 8(2), pp. 1-21, [Online]. Available at: https://www.researchgate.net/publication/332849592_A_Comparative_Analysis_of_the_Cyber_Security_Strategy_of_Bangladesh. [Accessed: 09-May-2021].

[3] Aljuryyed, A., 2022. "Cybersecurity Issues in the Middle East: Case Study of the Kingdom of Saudi Arabia", Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security, pp. 62-82, IGI Global.

[4] Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M., 2016, December. "A survey of cyber-security awareness in Saudi Arabia", in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 154-158). IEEE, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7856687. [Accessed: 09-May-2021].

[5] Min, K.S., Chai, S.W. and Han, M., 2015. "An international comparative study on cyber security strategy", International Journal of Security and Its Applications, 9(2), pp.13-20, [Online]. Available: https://www.researchgate.net/publication/283194459_An_International_Comparative_Study_on_Cyber_Security_Strategy. [Accessed: 09-May-2021].

[6] Han, T., & Zhang, Y, 2020, "Comment and analysis on the major national strategies of cyberspace" World Scientific Research Journal, 6(5) , pp.275-281.

[7] ITU., 2020. "The fourth iteration of the Global Cybersecurity Index (GCI)" International Telecommunication Union (ITU). [Online]. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf[Accessed: 15-Mar-2022]

[8] Nguyen, T.A., Koblandin, K., Suleymanova, S. and Volokh, V., 2022. "Effects of 'Digital'Country's Information Security on Political Stability," Journal of Cyber Security and Mobility, 11(1), pp. 29-52.

[9] ITU., 2017, "Global Cybersecurity Index 2017," International Telecommunication Union (ITU), pp. 1–77. [Online]. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed: 09-Mar-2022].

[10] Leandros, M., 2018. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018.

[11] Hyett, N., Kenny, A. and Dickson-Swift, V., 2014. "Methodology or method? A critical review of qualitative case study reports", International Journal of Qualitative Studies on Health and Well-Being, 9(1), p.23606, [Online]. Available at: https://www.tandfonline.com/doi/full/10.3402/qhw.v9.23606. [Accessed: 09-May-2021].

[12] Goel, S. , 2020. "National Cyber Security Strategy and the Emergence of Strong Digital Borders," Connections: The Quarterly Journal, 9(1), pp. 73-86.

[13] Alhalafi N and Veeraraghavan P, 2021. "Cybersecurity Policy Framework in Saudi Arabia: Literature Review," Frontiers in Computer Science, 9.

[14] Broo, D.G., Boman, U. and Törngren, M., 2021. "Cyber-physical systems research and education in 2030: Scenarios and strategies", Journal of Industrial Information Integration, 21, p.100192. [Online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2452414X20300674. [Accessed: 09-

May-2021].

[15] William, C., 2021. "The cyber-security workforce gap," The Cyber-security Workforce Gap | Center for Strategic and International Studies. [Online]. Available at: https://www.csis.org/analysis/cybersecurity-workforce-gap. [Accessed: 09-May-2021]

[16] Schia, N.N., 2018. "The cyber frontier and digital pitfalls in the Global South", Third World Quarterly, 39(5), pp.821-837. [Online]. Available at: https://www.tandfonline.com/doi/pdf/10.1080/01436597.2017.1408403. [Accessed: 09-May-2021].

[17] Egas, M.R., Ninahualpa, G., Molina, D., Ron, M. and Díaz, J., 2020, June. National cybersecurity strategy for developing countries: case study: Ecuador proposal, in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-7). IEEE.

[18] Alshammari, T.S. and Singh, H.P., 2018. "Preparedness of Saudi Arabia to defend against cybercrimes: An assessment with reference to anti-cybercrime law and GCI index", Archives of Business Research, 6(12), pp. 131-146. Doi: 10.14738/abr.612.5771

[19] Algarni, A.F., 2013. "Policing Internet fraud in Saudi Arabia: expressive gestures or adaptive strategies?", Policing and Society, 23(4), pp. 498-515.

[20] Gharibi, W., & Shaabi, M. (2012). "Cyber threats in social networking websites", arXiv preprint arXiv:1202.2420. [Online]. Available at: https://ui.adsabs.harvard.edu/abs/2012arXiv1202.2420G/abstract. [Accessed: 09-May-2021].

[21] Alghamdi, M.I., 2020. "Best ways to face cyber-attacks for Albaha City, Saudi Arabia". [Online]. Available: http://www.gjstx-e.cn/gallery/85-dec2020.pdf. [Accessed: 09-May-2021].

[22] Aljabri, S, 2021. "Cybersecurity Awareness In Saudi Arabia," International Journal of Research Publication and Reviews, 2(2), pp. 320-330.

[23] Liveri, D. and Sarri, A. 2014. "An evaluation framework for national cyber security strategies". Heraklion: ENISA, p.8.

[24] Alkalabi, W., Simpson, L. and Morarji, H., 2021, February. Barriers and incentives to cybersecurity threat information sharing in developing countries: a case study of Saudi Arabia., in 2021 Australasian Computer Science Week Multiconference (pp. 1-8). [Online]. Available at: https://eprints.qut.edu.au/207852/. [Accessed: 09-May-2021].

[25] Arta, H. 2021. "New technologies, future conflicts", - CBAP. [Online]. Available at: https://cbap.cz/wp-content/uploads/CBAP_NewTechPaper2021FREN.pdf. [Accessed: 09-May-2021].

[26] Shafqat, N. and Masood, A., 2016. "Comparative analysis of various national cyber security strategies", International Journal of Computer Science and Information Security, 14(1), p.129. Available at: https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies. [Accessed: 09-May-2021].

[27] Tar, U.A. (ed.), 2021. Routledge hand-

book of counterterrorism and counterinsurgency in Africa. Routledge.[Online]. Available at: https://www.taylorfrancis.com/books/routledge-handbook-counter-terrorism-counterinsurgency-africa-usman-tar/e/10.4324/9781351271929. [Accessed: 09-May-2021].

[28] Rahman, N., Sairi, I., Zizi, N. and Khalid, F., 2020. "The importance of cybersecurity education in school", International Journal of Information and Education Technology, 10(5), pp. 378-382. [Online]. Available at: http://www.ijiet.org/show-138-1620-1.html. [Accessed: 09-May-2021].

[29] Van Steen, T., Norris, E., Atha, K. and Joinson, A., 2020. "What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?" Journal of Cybersecurity, 6(1), p.tyaa019. [Online]. Available: https://academic.oup.com/cybersecurity/article/6/1/tyaa019/6032830. [Accessed: 09-May-2021].

[30] Alsmadi, I. and Zarour, M., 2018, April. Cybersecurity programs in Saudi Arabia: issues and recommendations, in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[31] Ademola, E.O., 2019. "Insights into cyber policies, Information Technology Governance (ITG) and, Multi-stakeholder Security Governance Scaling (MSGS) for decision-makers within UK SME Aviation", Journal of Behavioral Informatics, 5(4), pp.1-14. [Online]. Available: https://www.researchgate.net/publication/344705190_Insights_into_Cyber_Policies_Information_Technology_Governance_ITG_and_Multi-stakeholder_Security_Governance_Scaling_MSGS_for_Decision_Makers_within_UK_SME_Aviation. [Accessed: 09-May-2021].

[32] Ka tagiri, N., 2022. " Assessing Japan's cybersecurity policy: change and continuity from 2017 to 2020", Journal of Cyber Policy,7(2022), pp.1-17.

[33] Alqurashi, R. K., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J.,2020. "Cyber attacks and impacts: A case study in saudi arabia," International Journal of Advanced Trends in Computer Science and Engineering, 9(1), pp.217-224.

[34] Teoh, C.S. and Mahmood, A.K., 2017, July. National cyber security strategies for digital economy, in 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 1-6). IEEE. [Online]. Available at: https://www.researchgate.net/publication/319052003_National_cyber_security_strategies_for_digital_economy. [Accessed: 09-May-2021].

[35] Alelyani, S. and Kumar, H., 2018. "Overview of cyberattack on saudi organizations," Journal of Information Security and CybercrimesResearch, vol. 1, 2018. Available at: https://journals.nauss.edu.sa/index.php/JISCR/article/view/455. [Accessed 8 October 2019].

[36] Alzubaidi, A., 2021. "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia". Heliyon, 7(1), p.e06016.