International Journal of Cyber Operations and Cyber Security Governance
Volume 1 Issue 1, 2026

Evaluation of Different Government Cybersecurity Programs

Süleyman Karata
Faculty of Engineering
Department of Management Information Systems

Article Info
Received: 10-11-2025 Revised: 13-12-2025 Accepted: 23-12-2025 Published: 05-01-2026

***Abstract*—** National security, the economy, and the everyday lives of individuals are perpetually at risk due to the inherent weaknesses in cyberspace and the ever-escalating nature of cyber-attacks. In response to the serious threats to national cyber defences, over fifty nations have developed cyber security strategies. While the overarching goal of any cyber security policy should be to protect the nation's online infrastructure from malicious actors, different countries' threat landscapes need different methods to prevention, defence, and offence. Based on the recorded legal, operational, technological, and policy-related indicators, this research report analyses and compares twenty nations' national cyber security strategies. The majority of plans have outlined the need of forming Computer Emergency Response Teams (CERT/CSIRT) to combat cyber-attacks on national cyberspace and designating an official entity to oversee national cyber security activities. The definitions of important terminology (e.g., cyberspace and cyber security), the goals and descriptions of programs to raise cyber awareness and capability, legislative actions, etc., are all areas where there is disagreement. The study draws on the comparison to identify and suggest best practices for bolstering the cyber resilience and security of the country. This research study may be used by governments to their benefit when developing or updating their cyber security strategy.

Keywords-Cyber Security Strategy; Critical national infrastructure; Cyber-crimes; Cyberspace security; Incident response team.

I. INTRODUCTION

Modern advancements in information and communication technology have made many aspects of life easier and made government more efficient. The trend in cyber-attacks has shifted from isolated incursion attempts and financial breaches to well-coordinated state-sponsored assaults, driven by the growing dependence on ICT and complexity of attack tactics. Today, cyberattacks may inflict more material and monetary damage than acts of physical terrorism, according to major government officials and corporate executives. [1]

Many nations have come to realise, due to the pervasiveness of ICT, that their national information infrastructure is extremely susceptible to cyber-attacks. This realisation was prompted by notable cyber-attacks such as the 2007 attack on Estonia's internet infrastructure, the 2008 Georgian–Russian conflict that escalated into a cyberwar, and the 2010 Stuxnet worm attack on Iran's nuclear program [2]. Additionally, it prompted the development of a comprehensive strategy, the National Cyber Security Strategy (NCSS), and the building of cyber-capability at the federal level. Many nations are now more wary than ever of compromising their people' digital information or the basic internet rights after Snowden's 2013 disclosures about the National Security Agency's (NSA) bulk eavesdropping on worldwide Internet communications.

Twenty nations from around the globe—the United States of America, Canada, Estonia, France, Finland, Germany, Iran, India, Israel, Japan, Malaysia, New Zealand, the Netherlands, Saudi Arabia, Spain, Turkey, and the Czech Republic—had their national cyber security strategies evaluated in this study. the third

The major objective of this study is to examine and contrast the various cyber security strategies, policies, and practices described in the publicly accessible papers. The study concludes with suggestions for politicians and executives to strengthen the resilience of their country's online, based on this comparison. Each country may use this comparison research as a starting point for their own cyber security policy or to revise an existing one.

II. SELECTION OF COUNTRIES

Many nations that rank highly in the International Telecommunication Union's Cyber Security Ranking were selected for this research because their cyber defences are considered to be among the strongest in the world. Included in this group of nations are certain percentages of the following:

Developed/ Advanced countries

This includes countries that lead the ITU's ranking with regard to cyber-preparedness [4], as seen in Table 1. The analysis of these strategies will provide a notion of advanced and secure cyberspace practices to be considered while formulating a cyber security strategy document.

TABLE I. DEVELOPED COUNTRIES WITH HIGH CYBER SECURITYRANKING

Cyber Security Ranking	Country
1	USA
2	Canada
3	Australia
4	New Zealand
5	Estonia, Japan, UK, Germany
6	Austria, Israel, Netherlands
8	Finland
9	France, Spain
12	Czech Republic

The United States, the United Kingdom, France, the Netherlands, and Germany have all received international acclaim for their cyber security initiatives, which address both the offensive and defensive sides of cyberspace [5]. We chose to focus on Spain, Canada, Japan, and Australia [6] because, after the United States and Germany, these countries have the largest rates of cybercrime and information and communication technology use, respectively. By analysing their data, we may learn more about how to effectively tackle cybercrime in these countries. [7] It is also important to review other nations' plans, particularly for changes made in subsequent editions, as only a few of countries—including the United Kingdom, the United States, the Czech Republic, and Estonia—have revised their first strategy draft. The Netherlands was selected because, similar to the United States, it has developed two distinct cyber defensive strategies: one for civilian use and another for use by the military. Saudi Arabia is now a part of the study since it has recently fortified its cyber defences. Many security experts, however, hold Finland and Israel up as models of cyber excellence [8]. The strategies of these nations were chosen for the research for all of these reasons [9].

A. Developing countries

This includes countries which have high cyber security ranking, according to ITU, as shown in Table 2. Cross comparison of such strategies will provide necessary information as to how the listed developing nations progressed with such a quick pace, in the cyber domain, leaving even many developed countries behind.

TABLE II. DEVELOPING COUNTRIES WITH HIGH CYBER SECURITY RANKING

Cyber Security Ranking	Country
3	Malaysia
5	India,
7	Turkey
19	Iran

Malaysia is one of the nations being studied since, according to the experts, it is the most cyber-savvy country in Asia [10]. With such high rates of cybercrime, studying India and Iran's approaches may teach us a lot about how to keep the internet safe from all sorts of dangers.

COMPARISON METRICS

All the national cyber security strategies have the identical aim of protecting the cyberspace against adversaries and enhancing cyber resilience. However, the country's cyber threat landscape, socio-political conditions, security trends, traditions, the level of cyber awareness, etc, have brought significant variations in the cyber security approaches of the selected countries. [11] The following set of metrics has been developed to carry out the comparison of the aforementioned cyber security strategies.

- Timeline of development (the year when the Cyber Security Strategy or policy for a particular country was issued,
- Strategic objectives/ aims outlined in the strategy document,
- Understanding of major key terms i.e. cyberspace and cyber security,
- Level of prioritization assigned to national cyber security,
- Country's perception of cyber threats,
- Organizational Overview: i.e the leading organizations and public actors responsible for maintaining the state of cyber security at the federal level,
- Critical sectors and infrastructure listed in the strategy
- Incident response capabilities: i.e. whether Cyber Early Warning systems, Threat Information Sharing approaches, Computer Emergency Response Teams (CERTS) etc exist or not.
- Legal measures: covering evaluation and review mechanisms of the strategy.
- Capacity Building: includes the country's effort for Research and development (R&D), cyber workforce development, cyber awareness etc.
- Collaborations for cyber security (Inter-state, intra-state and international)

III. COMPARISON BASED ON IDENTIFIED METRICS

An example of a cyber security plan is the Netherlands' 2011 document, which is nine pages long. Another example is Saudi Arabia's 2013 document, which is ninety pages long. While some of the nations in the survey have included "cyber security" into their overall national security or defence plans, the vast majority have kept the two domains distinct. English has been the language of publication for the majority of cyber security plans. At the same time, draughts in English were also produced by nations whose national language is not English, including the Czech Republic, the Netherlands, Finland, Estonia, France, Germany, Turkey, and Spain. More comparison findings will be shown in subsequent subsections using the metrics defined in Section

III. A. Formulation of a Plan for Cyber Defence

After a change from basic cyber-attacks to big targeted state-sponsored strikes in 2008, the development of cyber

security techniques gained speed. Table 3 below details the NCSS timelines of the chosen national cyber security plans for the research. All nations have made their plans public on the internet with the exception of three: Iran, Israel, and Malaysia. Information about these three nations' cyber defence strategies is culled from publicly available sources.

TABLE III. TIMELINE OF CYBER SECURITY STRATEGIES

Countries	Year Strategy/ Policy issued
Australia	Strategy 2009, Revised strategy expected in 2015
Austria	Strategy 2013
Canada	Strategy 2010, Action Plan for Strategy (2013)
Czech Republic	Strategy 2011, 2015
Estonia	Strategy 2008, 2014
Finland	Strategy 2013
France	Strategy 2011
Germany	Strategy 2011
India	Policy 2013
Iran	NCSS not public
Israel	Official NCSS not published
Japan	Strategy 2013
Malaysia	Policy 2006 (document not public), NCSS expected in 2017
Netherlands	Strategy 2011, 2013
New Zealand	Strategy 2011
Saudia Arab	Strategy 2013
Spain	Strategy 2013
Turkey	Strategy 2013
UK	Strategy 2009, 2011
USA	Strategy 2003, Strategy Review (2009), Policy 2011, Strategy for critical infrastructure (2014), Dept. of Defence's strategy 2015.

Timeliness suggests that 2011 was the year when most nations unveiled their cyber security plans. However, back in 2003, when cyber-attacks were rare, the United States of America released the first plan draft. Nevertheless, it is crucial to update the cyber security plan to include new threats and appropriate responses due to the ever-evolving nature of cybercrime. Following this, the United Kingdom, the United States of America, the Netherlands, the Czech Republic, and Estonia have all released updated versions of their strategies; the United States of America, in particular, reviews and updates its papers more often.

Strategic Objectives outlined in NCSS

NCSS basically defines the vision of any country for addressing the cyber security challenges at the national level. Since all strategies are directed towards the ultimate goal of safeguarding the national cyberspace, they share many common themes and concerns. Except for Germany, which lists down some priority areas as the objectives, all other countries clearly states their strategic objectives in the document. The common objectives found in almost all NCSS are: [12]

- To maintain a safe and resilient cyberspace,
- To secure critical national cyber assets and infrastructures,
- To define a cyber-security regulatory, legislative and assurance framework,
- To raise cyber awareness amongst citizens, government officials, IT professionals etc,
- To develop cyber security incident detection and response capabilities e.g. Cyber-Security Incident Response Team (CSIRT) etc,
- To develop indigenous cyber-security technology,
- To respect fundamental rights of netizens,
- To promote public-private co-operation for enhancing the cyberspace security,
- To stimulate international co-operation mainly with the neighbouring and regional countries.

Beside the common ones, few strategies have also proposed objectives that are only specific to their country. For instance, France desires to become a world leader in cyber security domain in near future. Also, Japan desires for agile adaptation of evolving cyber threats and introduction of global outreach programs for cyber security, etc.

The thorough study of the selected strategies also brings forward the fact, that with the passage of time, the scope of cyber security strategies is shifting from merely securing citizens or governments against cyber-attacks to securing the whole information society in general.

B. Diverge Understanding of Key Terms

Cyber Security is quite a vast domain. Since there are no globally harmonized definitions of cyber security key terms, almost every country has provided its own definition in the strategy document. This sub-section will compare the definitions of cyber security and cyberspace as defined in the respective strategies.

1) Cyberspace: By comparing the chosen approaches, we find that the majority of nations see cyberspace as an expansive network including all forms of information and communication technology (ICT), both virtual and physical, that may be targeted by malevolent cyber actors. Nevertheless, in the case of nations such as Australia, New Zealand, "Cyberspace" only means the Internet and

related information and communication technology devices in Canada, Spain, and Germany. In addition, neither Estonia nor the Netherlands have offered comprehensive definitions of cyberspace; rather, their cyber security policies just make passing references to the concept. Additionally, one country that has chosen a different approach is Finland, which has substituted the phrase "cyber domain" for cyberspace. Table 4 provides a concise summary of the findings in this subsection.

2)

TABLE IV. CYBERSPACE DEFINED BY VARIOUS COUNTRIES

#	Comparator	Countries
1	Cyberspace includes all virtual and physical ICT devices	USA, UK, France, India, Saudi Arab and Turkey
2	Cyberspace only refers to "internet" and internet connected ICT devices	New Zealand, Australia, Germany, Spain and Canada
3	No clear definition of cyber security is provided	Estonia and Netherland
4	Term "Cyber domain" has been used instead of cyberspace	Finland

3) Cyber Security: Most of the strategies under study have defined "cyber security" as combating every cyber threat within the cyberspace. However, Austria and Finland limit it only to the protection of digital information or critical infrastructure. These varying perceptions lead to multi-faceted approaches for addressing and mitigating cyber-attacks.

In the strategy document, where Australia, France, Germany, Netherland, Saudi Arab and New Zealand have clearly mentioned their definition of cyber security, UK and Canada have used descriptive texts to define their concept of cybersecurity. Moreover, the Czech Republic and Japan have not explicitly defined "cyber security" anywhere in the strategy. [13] The results have been summarized in Table 5.

TABLE V. CYBER SECURITY DEFINED BY VARIOUS COUNTRIES

#	Comparator	Countries
1	Clear definition of cyber security is given in document	Australia, France, Germany, Netherland, New Zealand, Saudi Arab, Turkey
2	Detailed description is provided to define "cyber security"	Canada, UK
3	No definition of cyber security provided	Czech Republic, Japan

C. *Level of prioritization assigned to cyber security*

Worldwide, cyber-attacks, cyber-espionage, and cyber-terrorism have emerged as serious threats in recent years, joining the ranks of terrorism, economic recession, natural disasters, etc. Cybersecurity has recently come to light as a critical concern for national security, according to the comparison study. More resources have been devoted to cyber security measures by the nations with the highest rates of cybercrime, including the United States, the United Kingdom, Japan, Germany, Australia, and France. The United Kingdom spends £650 million per year on cyber security, followed by India with $500 million, France with $1.2 billion, Canada with $6 billion, and the United States with the largest yearly expenditure, reaching up to $10 billion, according to publicly accessible statistics. While cyber security is consistently ranked high in several papers, the amount of money allotted to national cyber security projects varies greatly. [15]

D. *Characterization of Cyber Security Threats*

Cyberterrorism, electronic forgery, vandalism, extortion, state-sponsored attacks, unauthorised access and interception of digital information, organised cybercrimes, and cybercrime in general are the main concerns for most countries, including Canada, the United States, the United Kingdom, Germany, the Netherlands, and others. Natural disasters and software/hardware malfunctions are also considered cyber dangers in the Netherlands and Germany. [16]
As part of cyber defence measures, there are a number of crimes that vary in gravity from one country to the next. While Americans define cyberattacks as threats to computer systems, data, and networks, Germans define them as attacks on information technology systems that jeopardise the availability, confidentiality, and integrity of such systems. In light of this, whereas probing is a criminal in Germany, it is not a crime in the United States. [17] As a result, taking a comprehensive, worldwide strategy to cyber threats and adversaries is challenging due to the diverse understanding of cyber security and the cyber threat environment.
Japan notes the need of addressing the security of Internet Protocol IPv6 and e-appliances attached to smart grids, among other emerging cyber risks; France, India, and Japan have all taken these into consideration in their strategies, in addition to the more traditional cyber-attacks. Some nations have also made reference to cyberwarfare in official papers; they include the United States, Germany, Estonia, and the Netherlands. Nevertheless, neither Finland nor France have specifically included a cyber threat topology in their plan.

E. *Critical Sectors/ Infrastructures*

In a nutshell, any asset—physical or digital—that, if hacked, may cripple a nation's economy, security, and prosperity is deemed critical infrastructure. A vital infrastructure in the cyber realm is one that processes, stores, and transmits digital information, as well as one that delivers services and essential values. Cyber threat perception, socio-political considerations, geographical circumstances, and nation-specific idiosyncrasies and traditions all have a significant role in determining which key sectors or infrastructure a country prioritises. This is why two nations have such varied approaches to categorising the same set of assets—smart electrical networks. might be a weak point for wealthy countries, but it's not for a lot of poor countries.

The vital industries have been identified by the United Kingdom, the United States, Australia, Canada, the Netherlands, and Turkey. Malaysia does not yet have a thorough Critical Information Protection Policy or a specialised cyber security plan, although the government papers do identify susceptible industries. But Austria has remained tight-lipped over its vital assets. [18] in At now, the majority of nations see the following industries as crucial.

Telecommunication and ICT,

- Banking and Finance,
- Government and the pertinent e-services,
- Electricity,
- Water Supply,
- Health Services i.e. hospitals,
- Transportation (especially air, rail and road),
- Emergency and Rescue Services,
- National Security services i.e. police, armed forced

etc The oil and gas sector, judiciary, chemical sector, critical manufacturing sector, dams, food and agriculture sectors have also been regarded as critical sectors by few countries. However, the list of critical sectors for any country is not conclusive, since digitization of ICT infrastructures, the inherent vulnerabilities, the increasing sophistication of cyber-attacks etc. are continuously adding new sectors and infrastructure to this list.

F. Organizational Overview- Lead responsible Authority

This subsection compares the officially recognized organizations or authorities of the selected countries that are responsible for implementing the cyber security strategy, protecting the critical assets and maintaining the state of cyber security at the national level.

The comparative analysis reveals that the majority of the countries have established inter-departmental cyber security response capabilities i.e. they have distributed the task of cyber security amongst multiple existing organizations working under various governmental departments. The establishment of these organizations within the government is greatly influenced by cyber threat perception, resource allocation, defence tradition etc.

France and Estonia, however, have created new coordinating bodies, which centrally deals with cyber threats and attacks. Table 6 gives a general overview of the leading authorities responsible for cyber security tasks in the countries under study. [19]

TABLE VI. LEAD RESPONSIBLE AUTHORITIES

#	Responsible Authority	Countries
1	Head of the state	USA
2	Cabinet office	Australia, Japan, UK
3	Ministry (Information Technology, Interior, Law, Defence etc.)	Canada, Germany, India, Czech Republic, Netherlands, New Zealand, Saudi Arab, Malaysia, Turkey, Iran, Austria, Spain
4	New coordinating bodies	France, Estonia

As observed, on the whole, there is very little consistency across various comparators in terms of the departments entrusted with the task of national cyber security.

G. Technical Measures: (Threat Information Sharing/ Early Warning Approaches.)

Technical teams that provide threat information to the relevant authorities and offer cyber security and resilience skills are crucial for a nation to successfully repel targeted cyber attacks and events. Information Sharing and Analysis Centers (ISACs), Computer Security Incident Response Teams (CERTs), and Computer Emergency Response Teams (CERTs) are all examples of such teams.

According to the chosen NCSS, every country has its own computer emergency response team (CERT) or computer security incident response team (CSIRT) to deal with cyberattacks. The goals and effectiveness of these organisations, however, differ substantially from one another. Table 7 below shows when CERT/CSIRTS were established in the nations that were part in the research. [20]

TABLE VII. EARLY WARNING APPROACHES FOR VARIOUS COUNTRIES

Countries	CERT established
Australia	2010
Austria	2008
Canada	2003
Czech Republic	2011
Estonia	2006
Finland	2014
France	2008
Germany	2012
India	2004
Israel	2014
Japan	1996
Malaysia	1997
Netherlands	2012
New Zealand	2011
Saudia Arab	2006
Spain	2008
Turkey	2007
UK	2014
USA	2003

Few countries have also established coordinating bodies along with CERT/ CSIRTS for information threat sharing. For example Integrated Government of Canada Response Systems by Canada, Cyber Security Strategy Head quarter by Japan, etc.

H. Legal Measures:

To ensure that all public and private entities can handle cybersecurity challenges, it is necessary to establish an appropriate policy framework to frequently evaluate the progress of the proposed objectives of the strategy and revise the strategy accordingly.

The research reveals that except for Spain, most countries within the scope of study have mentioned review and evaluation processes for the strategy in the documents. Since, Malaysia has not formulated the complete strategy yet, it, therefore, lacks annual cyber security audits and policy reviews too. Countries such as Austria, Estonia and Germany have even specified the actors to be involved in reviewing mechanisms. However, in all instances, the details of review mechanisms have been provided as a separate act or in implementation scheme.

Several strategies have also mentioned the frequency of the review cycle i.e. yearly for Netherlands and Slovakia and biannual for Austria and UK. [21]. While USA, UK, Estonia and few other countries update their cyber security strategy very frequently, there are countries that have not even updated their initial cyber security strategies once.

I. Cyber Security Capacity Building

All cyber security strategies mention the need of creating cyber defensive and preventive capabilities to better defend the national cyberspace. This subsection throws light on various cyber security capacity building initiatives e.g. training, awareness, R&D initiatives etc, as documented in the selected strategies.

1) Manpower Development and Cyber Awareness Programs: All cyber security strategies emphasize the need of raising cyber awareness in general public especially businessmen, IT professionals, government officials and lawmakers. But countries especially, Australia, Spain, Japan and the UK pay special attention to the cyber training of children and parents too. [22]

Countries particularly UK, India and Malaysia have mentioned the usage of social media for launching widespread awareness campaigns. However, Netherlands and Turkey emphasize the need of teaching cyber security at all academic levels and have thus suggested making it a part of academic curriculum.

All the nations under study, except for the Czech Republic, have defined nation-wide cyber-security outreach programs for their citizens, where they provide cyber security tools and practical education. The most notable programs amongst them are Stay Safe Online campaign of Australia, Malaysia's "Cyber Safe" Program, "Get Safe Online" program of UK, and organization of "Cyber Security Month" annually by Austria, UK, and US. [23]

The study also reveals Japan's desire for establishing various cyber security support services for the capacity building. Moreover, countries especially UK, Netherlands, India, Saudia Arab, Malaysia, and Turkey emphasize the need of commercial security certifications/ trainings for professionals and experts in their NCSS. [24]

2) Research and Development: To prevent inherent vulnerabilities of the ICT devices from being exploited by adversaries, it is required to lay stress on the development of local security products, thereby enhancing cyberspace security. The comparative study shows that except for Australia, Saudia Arab, Czech Republic, UK and Finland, all other countries have officially recognized entities for promoting R&D work at the national level. The tasks of the R&D divisions as mentioned in the various strategies are to sponsor academic and industrial projects related to cyber security, develop indigenous cyber security products, promote security standards and best practices at the national level, etc.

J. Cooperation

Cybersecurity requires multi-stakeholder approach for effectively tackling cyber issues and increasing cyber resilience. Because of the global nature of cyberspace, apart from intra-nation cooperation (public, private sectors, ISP's etc), intra-state and international collaboration are also required. [25]

1) ***Public-Private Partnership (PPP):*** Public-Private Collaboration is necessary since private sector owns most of the internet infrastructure. Hence, the public and private sectors should effectively cooperate to defend the cyberspace. Research shows that it has been introduced as a concept in NCSS of Canada, Australia, UK, Saudi Arab and Netherlands, and as a part of the action plan in France's NCSS.

However, except for Iran, Czech Republic, Finland and Spain, all the countries under the study, have defined Public Private Partnership plans in the strategy with an aim to address the issue of cyber security at the national level.

2) ***Cooperating with ISPs****:* The strategies of countries like USA, UK, Japan, Saudi Arab and Australia emphasize greatly on the need of government's partnership with Internet service and telecom providers for better security of national cyberspace from internal and external cyber preparators. Others do not explicitly mention this in the strategy.

3) International Collaboration: Since it is impossible to guarantee security of the national cyberspace in an insecure global cyber environment, almost all the strategies have laid stressed on the need of international collaboration in the domain of cyber security, especially with neighboring and regional countries. Where other strategies have merely proposed it as an objective and have not provided details, cyber security strategies of USA, UK, Germany and Australia also mentions action plan to improve global cooperation.

IV. RECOMMENDATIONS

With the cyber preparators gaining strength day by day, cyber-attacks are continuously evolving at a faster pace. No nation can, therefore, stay safe from cyber-attacks. Following recommendations if adhered, while formulating or revising the cyber security strategy can help mitigate cyber risks to the national cyberspace. [26]

- Clearly define the scope, objectives and definitions of major key terms in the document in accordance with the country's actual threat landscape.
- Do not confine the strategy only to the protection of critical assets, rather focus on securing the entire

national cyberspace and defending fundamental rights of internet users.

- Redefine the words "critical infrastructures" in the strategy because the existing definition i.e. “infrastructures that adversely affects the national economy and security when compromise”, leaves many critical computer networks out of the scope of critical infrastructures.
- Attempt to focus on the protection of cyberspace from new threat vectors e.g. smartphones, cloud computing, big data etc in the document.
- Incorporate the principle of agility by subjecting the strategy to regular reviews, and input from industry to keep pace with the technological advances and increasing cyber risk sophistication.
- Include input from all national stakeholders; government, military, telecom providers, financial institutions, judiciary, civil society, religious leaders, cyber security experts etc, on domestic cyber security strategy or action plans.
- Support the strategy by articulating a comprehensive plan of cyber actions, with clearly defined stakeholders, authorities, accountabilities, milestones; investments, outcomes etc,
- Emphasize on the need of reforming national legal framework, in the strategy, to effectively deal with cyber-criminals and offenders,
- Ensure that there are effective technological controls for people, management, facilities, operations, etc in place, at all levels,
- Lay stress on the need of establishing information sharing framework to effectively share information regarding security incidents and breaches between the government and private sector.
- In the strategy, clearly define tasks and responsibilities of the CERTS/ CSIRTS from disseminating information about security advisories and cyber breaches to raising cyber awareness and forensically responding to cyber incidents, etc.
- Recommend various educational and training programs, cyber security toolkit etc, in the strategy, for netizen’s self-training and raising cyber awareness in the country,
- Encourage the development and promotion of indigenous security services and products
- Give advice on reinforcing private-public partnership to ensure continued cyber resilience of the national cyberspace.
- Propose acceptable cyber norms in the strategy document to increase international collaboration and prevent cyber warfare in the future.

V. CONCLUSION

Cybersecurity has recently overtaken national physical security as a matter of paramount importance. In light of the gravity of the situation, governments worldwide are working on cyber security policies. Nearly all of the methods that were considered for the strategy have stressed the need of public-private partnerships in bolstering cyber security, increasing public awareness of the need to take precautions online, and bolstering national incident prevention and response capabilities. Nevertheless, most nations have made hardly any effort to accomplish the goals that were set forth.

Although all twenty techniques were chosen with identical goals in mind, the research has shown that there are significant disparities in their scope and approach. As an example, although all the methods touch on the idea of CERT, the specific duties it is tasked with differ from one nation to another. Cyber awareness programs are a necessary, according to all plans, but each nation takes a somewhat different approach.

According to the findings, when compared to other countries' strategies, the United Kingdom, the United States, and Germany stand head and shoulders above the competition when it comes to creating and implementing action plans. While the policy does include defensive objectives, its emphasis on aggressive cyber defence of key assets offers them an advantage over other nations.

REFERENCES

[1] Eighth Edition of the Global Risks Report. 2013. This report was retrieved on November 27, 2015, from the following URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf.”

[2] In the 9th International Conference on Cyber Warfare & Security, Tatar, U. Calik, O. Celik, M. Karabacak, and B. conducted a comparative analysis of the national cyber security strategies of leading nations. year 2014. Australia, Canada, the Czech Republic, Estonia, Finland, France, Germany, India, Iran, Israel, Japan, Malaysia, the Netherlands, New Zealand, Spain, Saudi Arabia, Turkey, the United Kingdom, and the United States are all represented in cyber security strategy documents (pp. 211-218). The following sources were used for this article: [4] The Global Cybersecurity Index, 2014, ITU. [5] Dunn, M. A Comparative Analysis Of Cybersecurity Initiatives Worldwide, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf. Symposium on Cybersecurity at the World Summit on International Security (WSIS). Cyber Defence in the EU: Are We Gearing Up for Cyber Warfare? [6] Carmen Cristiana Cirlig, 2005.Accessed November 29, 2015, from the following URL: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

The twenty nations with the highest rates of cybercrime, according to Sumo [7]. 2014. Sanjana Sharma retrieved the information from http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ on December 5, 2015. Cyber Defence: 2015 Standards for the Defence Sector. The information was retrieved on November 19, 2015, from the

following source: http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defense-industry [9] Ashley Wheeler. The Best and Worst of Cyber Security. 2013. The information was retrieved on November 4, 2015, from the following source: [10] Nurjehan Mohamed's blog: http://phoenixts.com/blog/best-and-worst-cyber-security/. Asians as a whole aren't as tech-savvy as Malaysians."The ways, means and ends in cyber security strategies" was published in 2013 and was retrieved from http://www.therakyatpost.com/life/trends-life/2015/08/25/malaysians- are-the-most-cyber-savvy-among-asians/ on December 1, 2015. Critical Information Infrastructure Security, Lecture Notes in Computer Science 2013, pages 182-190. [12] Luiijf, H. Besseling, K. Spoelstra, M., and Graaf, P. Ten National Cyber Security Strategies: A Comparison. An expedited comparative study of cyber-security threat characterisation (Volume 6983, pages 1–17) [13] Robertson, Gribbon, L., Horvath, V., and Robertson, K. We are the RAND Corporation.Hedborg, M. (2012). Comparing Security Strategies, UI Brief. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR 235/RAND_RR235.pdf. References: [15] Klimburg, A. National Cyber Security - Framework Manual. 2012 CCDCOE. [16] The Cyber Index International Security Trends and Realities. 2013. http://www.ui.se/upl/files/77897.pdf. Cyber Wellness Profiles, 2015, available at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx, retrieved December 3, 2015, from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf. [17] International Telecommunication Union.

The authors of the article "Securing Cyberspace: A Comparative Review of Strategies Worldwide" are Levin, Goodrick, and Ilkina. The institute for privacy and cybercrime.
The ENISA assessment framework for national cyber security strategies was developed by Liveri and Sarri [19]. year 2014.
[20] In their report "Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy," the OECD examines the current state of cybersecurity policymaking. 2012, retrieved from http://dx.doi.org/ 10.1787/5k8zq92vdgtl-en [21] ENISA. The goals of the United States government's cyber defence initiatives are outlined in its national cyber security strategies. The Asia-Pacific Cybersecurity Dashboard was last updated in May 2012. that year 2015. Information Technology U.S. National CyberSecurity Strategy Guide, retrieved December 4, 2015, from http://cybersecurity.bsa.org/2015/apac/index.html. 2011. [24] In the International Journal of Security and Its Applications (2015), pp. 13–20, Min, K., Chai, S., and Han, M. conducted a comparative study of cyber security strategies on a global scale. [25] Daniel Benoliel was cited. As a Case Study, the Israel National Cyber Bureau Contributes to the Model for Cyber Security Policy. The Internet Governance Case Studies Series is a product of the Global Network of Interdisciplinary Internet and Society Research Centers (NoC). year 2014. Mapping the Mind Gap: Comparing US and European Security Strategies (Sebastian, F., 2006). March 2005, volume 36, issue 1, pages 71–92, Security Dialogue.