Comparative Analysis of Various National Cyber Security Strategies

Narmeen Shafqat
Student, Dept of Information Security, MCS
National University of Sciences and Technology (NUST)
Rawalpindi, Pakistan
narmeen.msis12@students.mcs.edu.pk

Ashraf Masood
Faculty Member, Dept of Information Security, MCS
National University of Sciences and Technology (NUST)
Rawalpindi, Pakistan
ashraf@mcs.edu.pk

***Abstract*—The intrinsic vulnerabilities in the cyberspace and ever-escalating cyber-attacks tend to continuously threaten the national security, economy and daily life of citizens. More than fifty countries, around the world, have formulated their Cyber Security Strategies to address the grave concerns of national cyber security. A cyber security strategy is particularly aimed at securing the national cyberspace from malevolent cyber threat vectors, but owing to the varying threat landscape, considerable variations can be seen in the preventive, defensive and offensive measures and approaches adopted by each country.**

This research paper analyzes and compares National Cyber Security Strategies of twenty countries based on the documented legal, operational, technical and policy-related measures. The majority of the strategies have described the need of appointing an official body for leading the cyber security tasks at the national level and establishment of Computer Emergency Response Teams (CERT/CSIRT) to fight cyber-attacks targeting national cyberspace. However, disparity lies in the understanding of major key terms (particularly cyber security and cyberspace), characterization of the cyber threats, aims and description of cyber awareness and capacity building programs, legislative measures etc. Based on the comparison, the research specifies and recommends best practices for improving the state of national cyber security and resilience. The countries planning to develop or update their cyber security strategies can use this research study to their advantage.

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

I. INTRODUCTION

The Information and Communication Technology (ICT) has brought us great convenience in life and efficacy in governance. With the increasing reliance on ICT and sophistication of attack methods, the trend of cyber-attacks has changed from small-scale intrusion attempts and financial breaches to highly organized state-sponsored attacks. In view of the prominent business leaders and government officials, today cyber-attacks alone can cause more physical and financial loss than physical terrorism. [1]

The prominent cyber-attacks of the past especially the attacks on Estonia's internet infrastructure in 2007, the physical war between Georgia and Russia that turned into cyber war in 2008, and the attack on Iran's nuclear program via the Stuxnet worm in 2010 [2] made many countries realize that the omnipresence of ICT has made their national information infrastructure highly vulnerable to cyber-attacks. It also triggered the establishment of cyber-capability at federal level and preparation of a high-level plan of actions i.e National Cyber Security Strategy (NCSS). The Snowden's revelations of 2013, regarding National Security Agency (NSA) carrying out mass surveillance on the global Internet communications, also made many countries cautious about protecting their digital information and fundamental internet rights of their citizens.

This research study assesses National Cyber Security strategies of twenty countries, from different regions of the world, including Austria, Australia, Canada, the Czech Republic, Estonia, France, Finland, Germany, Iran, India, Israel, Japan, Malaysia, New Zealand, Netherlands, Saudi Arab, Spain, Turkey, UK, and USA. [3] The primary aim of the research is to analyze and compare the different cyber security trends, measures and approaches outlined in the respective publically available strategy documents. Based on this comparison, the later part of the research proposes recommendations/ best practices for lawmakers and executives to further improve the resilience of their national cyberspace. This comparative study will, therefore, be of great help to all the countries, whether designing their first cyber security strategy or updating the existing strategy documents.

II. SELECTION OF COUNTRIES

Since the study aims to highlight the best cyber security practices, a variety of countries that top the ITU's Cyber Security Ranking have been chosen for comparison. This set of the selected countries contains a fraction of each of the following:

A. 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 SECURITY RANKING

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 cyber security strategies of USA, UK, France, Netherlands, and Germany are particularly acknowledged worldwide for mentioning dual aspects of cyber security i.e. both offensive and defensive cyber security action plans [5]. Spain, Canada, Japan and Australia [6] have been selected because they have the highest ICT usage and cyber-crime rate in the world after US and Germany, and thus their analysis can reveal potentially secure approaches for combating cyber-crimes in the country. [7] Besides, the UK and US, the Czech Republic and Estonia are amongst the few countries that have updated their first strategy draft and, hence, it is necessary to look up to their strategies too, especially for the amendments in later versions. Netherlands has been chosen, because like the USA, it too has formulated two separate strategies; one for civil cyber security and the other for military cyber defence. Saudi Arab has lately strengthened its cyber defence and has, therefore, become the part of the research. [8] Finland and Israel, on the other hand, are considered the prime example of cyber excellence according to many security researchers. [9] This all reasons why the strategies of these countries have been selected for the study

B. *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

The researchers regard Malaysia as the most cyber savvy country of Asia and, hence, it is included in the set of countries for research [10]. India and Iran have extremely high cyber-crime rates, so the analysis of their strategies will provide considerable directions for protecting the cyberspace against diverse threats and attacks.

III. 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)

IV. COMPARISON BASED ON IDENTIFIED METRICS

The cyber security strategies exist in various forms and length varying from nine pages (Netherlands Cyber Security strategy of 2011) to ninety pages (Saudi Arabia's Cyber Security strategy of 2013). Most of the countries under study have developed separate strategies for national defence and cyber security, whereas few have added a portion of "cyber security" in the national security strategy or the defence strategy.

In most instances, the cyber security strategies have been published in the English language. The non-native English-speaking countries such as Czech Republic, Netherlands, Finland, Estonia, France, Germany, Turkey, and Spain have also published a draft in English simultaneously.

Subsequent subsections will present more results of the comparison, based on the comparison metrics identified in Section III.

A. Development of the Cyber Security Strategy

The development of cyber security strategies gradually gained momentum after 2008 when the trend of simple cyber-attacks shifted to massive targeted state-sponsored attacks. Table 3 below gives a timeline of NCSS of various national cyber security strategies that have been selected for the research study. With the exception of Iran, Israel and Malaysia, all the countries have published their strategies online. The data for these three countries have been extracted from the public documents pertaining to the cyber security approaches in the country.

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.

The timeline infers that majority of the countries published their cyber security strategy in 2011. The United States of America, on the other hand, published the first strategy draft in 2003, when cyber-attacks were not very common.

However, the continuously changing spectrum of cyber threats has made it imperative to update the cyber security strategy to encompass emerging threats and relevant countermeasures. Countries particularly the UK, USA, Netherlands, Czech Republic and Estonia have consequently published the subsequent versions of their strategy as well, with USA reviewing and updating their documents most frequently.

B. 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.

C. 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: The comparison of selected strategies indicates that for most of the countries, cyberspace is perceived to be a complete network of all virtual and physical ICT devices that can be the target of evil cyber actors. However, for countries like New Zealand, Australia, Germany, Spain and Canada, the cyberspace only refers to the Internet and the pertinent ICT devices.

Furthermore, Estonia and Netherland have only implicitly defined cyberspace in their cyber security strategies and have not provided complete definitions. Also, Finland, being an exception, has used the term "cyber domain" instead of cyberspace in their strategy. Table 4 summarizes the results for this sub-section.

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

2) *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

D. *Level of prioritization assigned to cyber security*

In the last few years, besides terrorism, economic downturn, natural hazards, etc, cyber-attacks, cyber espionage and cyber terrorism have also become a global menace. The comparative analysis reveals that countries have now realized the importance of cyber security and, therefore, regard it as one of the top-tier national security issues. Countries especially USA, UK, Japan, Germany, Australia and France that have inflated rates of cybercrimes, have allocated significantly greater resources to cyber security measures than other countries under study. According to the publically available data, the UK spends £650m annually, India $500 million, France $1.2 billion, Canada $6 billion, and USA with the highest annual cyber security spending in the world amounting up to 10 billion dollars. [14] The facts indicates that despite same prioritization is assigned to cyber security in various documents, extensive variation lies in the budget allocated to national cyber security initiatives. [15]

E. *Characterization of Cyber Security Threats*

For most of the countries, especially Canada, USA, UK, Germany, Netherlands etc the potential risks and threats posed to the cyberspace revolve around organized cybercrimes, state-sponsored attacks, cyber terrorism, unauthorized access to and interception of digital information, electronic forgery, vandalism and extortion etc. For Germany and Netherlands, natural hazards and hardware/software failures too are regarded as the cyber threats. [16]

In the cyber security strategies, there also exist some offenses that varies in terms of severity of the crime in different countries. Since Germany view cyber-attack as the attack on IT systems that compromises confidentiality, availability and integrity of the information systems, USA considers it as an attack on the digital information, ICT devices and cyber networks. Hence, where probing is considered as a cybercrime in Germany, it is not an offense in USA. [17] Thus the varying perception of cyber security and the cyber threat landscape makes it difficult to adopt a holistic global approach to cyber threats and adversary.

Apart from the traditional cyber-attacks, few countries have also taken account of emerging cyber risks in their strategies e.g. France, Japan and India have considered the risks of Cloud Computing, Japan mentions the need of addressing the security of Internet Protocol IPv6 and e-appliances attached to smart grids etc, in the document. Few countries such as Estonia, USA, Germany and Netherlands have also referred to cyber warfare in their documents. However, Finland and France have not defined any cyber threat topology explicitly in the strategy.

F. *Critical Sectors/ Infrastructures*

Critical infrastructure is basically considered to be any physical or digital asset, which if compromised can pose a debilitating effect on the economy, security and prosperity of a nation. In the cyber domain, the criticality of an infrastructure is defined by the services and core values that it provides and the digital information that it processes, stores and transmits.

The choice of critical sectors or infrastructure by any country is highly impacted by the country-specific peculiarities and traditions, cyber threat perception, socio-political factors, and geographical conditions. It is for this reason that a particular subsectors/ assets have been classified so differently by two countries i.e. smart electricity grids might be a vulnerable asset for the developed states but not for many developing nations.

The critical sectors have been clearly listed by UK, USA, Australia, Canada, Netherlands, and Turkey. However, Malaysia despite lacking a dedicated cyber security strategy and a comprehensive Critical Information Protection Policy still outlines vulnerable sectors in the federal documents. Austria, however, has not provided any detail about their critical resources. [18] Currently, following sectors are considered critical for most of the countries.

- 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.

G. 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.

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

For a country to effectively deter targeted cyber threats and incidents, it is essential to have technical teams that efficiently disseminate threat information to the concerned authorities and provide cyber protection and resilience capabilities. Various forms of such teams include Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRT) and Information Sharing and Analysis Centers (ISAC).

The cross comparison of the selected NCSS reveals that all the countries possess their own national CERT/ CSIRT for effectively responding to cyber-attacks. However, the missions and efficiency of these entities greatly vary for one another. Table 7 below provides a timeline of the establishment of CERT/ CSIRTS in the countries under study. [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.

I. *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.

J. *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.

K. *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.

V. 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.

VI. CONCLUSION

In the recent years, cyber security has gained more attention than the issue of national physical security. Countries around the world are, therefore, formulating cyber security strategies to address this grave issue. Almost all documented strategies, selected for the strategy, have mentioned the need of establishing incident prevention and response capabilities at the national level, raising cyber awareness in general public, and promoting public-private partnership for better security of the cyberspace, etc. However, the majority of the countries have practically tried less to achieve the stated objectives.

Despite similar aims and objectives, the research has unveiled numerous differences in the scope and approach of the twenty strategies selected for the study. For instance, the establishment of CERT has been mentioned in all the strategies, but the tasks assigned to it varies from country to country. Similarly, all strategies urge the need of running various cyber awareness programs, but the approach of every country is different from the other.

From the research, it is obvious that the strategies of UK, USA and Germany particularly are better than the rest in terms of development and enforcement of action plans. Despite stating defensive missions in the strategy, they have also emphasized on utilizing their cyber capabilities to defend valuable assets offensively, and this gives them the edge over the other countries.

REFERENCES

[1] *Global Risks Report* Eighth Edition. 2013. Retrieved Nov 27, 2015 from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

[2] Tatar, U. Calik, O. Celik, M. Karabacak, B. A Comparative Analysis of the National Cyber Security Strategies of Leading Nations, *9th International Conference on Cyber Warfare & Security.* 2014. Pg 211-218

[3] Cyber Security Strategies Documents (Australia, Austria, Canada, Czech Republic, Estonia, Finland, France, Germany, India, Iran, Israel, Japan, Malaysia, Netherlands, New Zealand, Spain, Saudi Arab, Turkey, UK, and the USA). *CCDOE.* Retrieved Oct 28, 2015 from https://ccdcoe.org/strategies-policies.html

[4] Global Cybersecurity Index. ITU. 2014. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

[5] Dunn, M. A Comparative Analysis Of Cybersecurity Initiatives Worldwide. *WSIS Thematic Meeting on Cybersecurity.* 2005

[6] Carmen Cristiana Cirlig. *Cyber Defence in the EU- Preparing for cyber warfare?* 2014. Retrieved Nov 29, 2015 from http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

[7] Sumo. *Top 20 Countries Found to Have the Most Cybercrime.* 2014. Retrieved Dec 5, 2015 from http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

[8] Sanjana Sharma. *Cyber Security For The Defence Industry.* 2015. Retrieved Nov 19, 2015 from http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry

[9] Ashley Wheeler. *The Best and Worst of Cyber Security*. 2013. Retrieved Nov 4, 2015 from http://phoenixts.com/blog/best-and-worst-cyber-security/

[10] Nurjehan Mohamed. *Malaysians are the most cyber-savvy among Asians*. 2015. Retrieved Dec1, 2015 from http://www.therakyatpost.com/life/trends-life/2015/08/25/malaysians-are-the-most-cyber-savvy-among-asians/

[11] Lehto, M. The ways, means and ends in cyber security strategies, *Proceedings of the 12th European Conference on Information Warfare and Security*, 2013. pg 182-190

[12] Luiijf, H. Besseling, K. Spoelstra, M, Graaf, P. Ten National Cyber Security Strategies: A Comparison, Critical Information Infrastructure Security, *Lecture Notes in Computer Science* 2013. *Volume* 6983, pg 1-17

[13] Robinson, N. Gribbon, L. Horvath, V. and Robertson, K. *Cyber-security threat characterisation - A rapid comparative analysis. RAND Corporation.* 2013. Available: http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf

[14] Hedborg, M. Comparing Security Strategies, *UI Brief.* 2012. Available: http://www.ui.se/upl/files/77897.pdf

[15] Klimburg, A. *National Cyber Security – Framework Manual.* 2012. CCDCOE.

[16] *The Cyber Index International Security Trends and Realities.* 2013. Retrieved Dec 3, 2015 from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

[17] ITU. *Cyber Wellness Profiles*. 2015. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx

[18] Levin, A. Goodrick, P. and Ilkina, D. *Securing Cyberspace: A Comparative Review of Strategies Worldwide.* Privacy And Cyber Crime Institute.

[19] Liveri, D. and Sarri, A. An evaluation Framework for National Cyber Security Strategies. ENISA. 2014.

[20] OECD. Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy. 2012. Retreived from http://dx.doi.org/ 10.1787/5k8zq92vdgtl-en

[21] ENISA. National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. May 2012.

[22] Asia Pacific Cybersecurity Dashboard. 2015. Retrieved Dec 4, 2015 from http://cybersecurity.bsa.org/2015/apac/index.html

[23] ITU. *National CyberSecurity Strategy Guide*. 2011.

[24] Min, K. Chai, S and Han, M. An International Comparative Study on Cyber Security Strategy, *International Journal of Security and Its Applications* 2015. Vol.9, No.2, pp.13-20

[25] Daniel Benoliel. Towards A Cyber Security Policy Model: Israel National Cyber Bureau, Case Study. *Global Network of Interdisciplinary Internet & Society Research Centers NoC Internet Governance Case Studies Series.* 2014.

[26] Sebastian, F. Mapping the Mind Gap: A Comparison of US and European Security Strategies. *Security Dialogue March.* 2005. vol. 36 no. 1. Pg 71-92

AUTHORS PROFILE

Narmeen Shafqat **is** an Information Security graduate from National University of Sciences and Technology, Pakistan. She did her BE in Electrical telecommunication from NUST, and afterwards worked as research assistant in an R&D company. Her areas of interest are cyber security and digital forensics.

Ashraf Masood is a Professor at the Department of Information Security, National University of Sciences and Technology, Pakistan. His research interests are in the area of cyber security, cryptology and micro-electronics. He is also a founding member of Open Source Foundation Pakistan.