2014

The Critical Role of Education in Every Cyber Defense Strategy

Juan Cayón Peña

Luis A. García Segura

THE CRITICAL ROLE OF EDUCATION IN EVERY CYBER DEFENSE STRATEGY

Juan Cayón Peña, PhD. & Luis Armando García[*]

Abstract: The implementation, maintenance, and improvement of a national Cyber defense strategy involve a range of elements in which education has a predominant role right now. The coordination of both the private and public sectors are needed in order to develop and provide the appropriate curriculum necessary for the principal stakeholders involved in the Cyber defense strategy of any modern nation. This article seeks to identify the challenges faced by these stakeholders, as well as provide recommendations regarding these matters.

I. INTRODUCTION

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to develop and maintain intellectual capital, to conduct operations, and to deliver services.[1]

Basically, society has become more and more dependent on Information Technology (IT) resources; thus, the protection of these critical assets is increasingly becoming a topic of national interest. Incidents causing disruption of critical infrastructures and IT services can cause major disturbances in the functioning of society. As such, securing cyberspace has become one of the most important challenges of the 21st century for governments. Consequently, Cyber security is increasingly regarded as a "horizontal and strategic national issue affecting all levels of society."[2]

This article seeks to describe the role education plays in ensuring Cyber security and Cyber defense on a national level through the proper strategies and/or public policies.

[*] Antonio de Nebrija University, Madrid, Spain

[1] GREGORY C. WILSHUSEN, CYBER THREATS FACILITATE ABILITY TO COMMIT ECONOMIC ESPIONAGE (2012), *available at* http://www.gao.gov/assets/600/592009.pdf.

[2] EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., NATIONAL CYBER SECURITY STRATEGIES 4 (2012), *available* at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.

II. CYBER SECURITY STRATEGIES AND ITS RELATION TO CYBER DEFENSE

To some academics, preoccupation with cyber-armed attacks has been counter-experiential up to this point.[3] Yet to others, cyberspace has already become a "full-blown war zone," and cyber attacks are becoming a "key weapon for governments seeking to defend national sovereignty."[4] Some of the world's most prominent nations, including the United States of America (USA), agree that cyber-based threats are evolving and can arise from a wide array of sources. These sources may include business competitors, corrupt employees, criminal groups, hackers, as well as foreign nations engaged in espionage and information warfare. Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives for acting, which range from monetary gain or political advantage.[5]

On this matter, the British House of Commons Defence Committee made the following conclusion in 2013:

> The cyber threat is, like some other emerging threats, one which has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation's security. The Government needs to put in place – as it has not yet done – mechanisms, people, education, skills, thinking, and policies which take into account both the opportunities and the vulnerabilities which cyber presents.[6]

Given the interconnectivity within cyberspace, a comprehensive approach is called for at both the national and international level, in order to reduce the vulnerabilities a specific nation or group of nations might face. The traditional divisions between military and civilian, public and private, and national and international actors are less clear-cut in cyberspace. National security can, for instance, be jeopardized by a large-scale attack on a private organization. To defend against such attacks, cooperation between different parties is necessary, including the affected organization itself, the intelligence services, the criminal investigation services and, in certain cases, the armed forces as well.[7]

[3] (Michael N. Schmitt, '*Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. (forthcoming 2014).

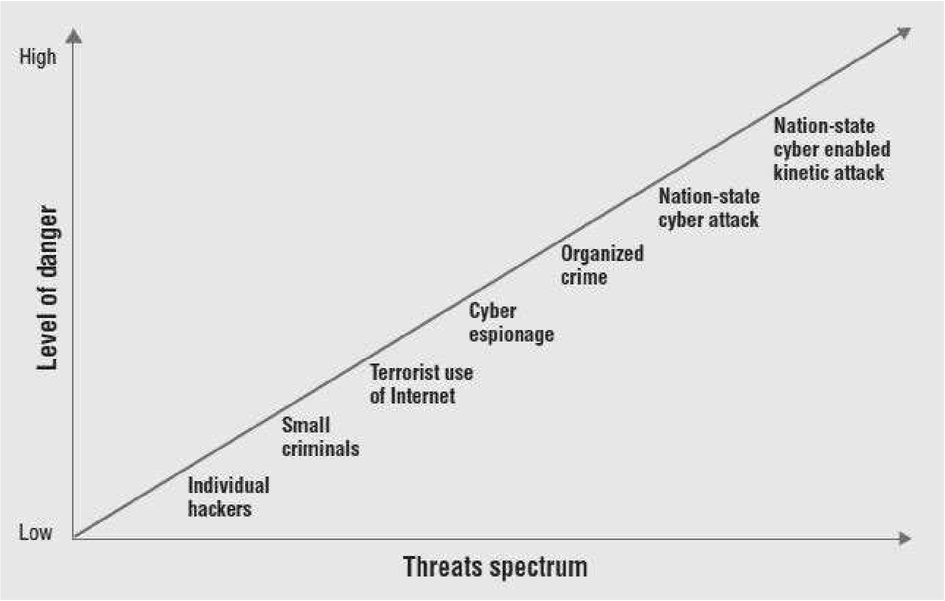
[4] KENNETH GEERS ET AL., FIREEYE LABS, WORLD WAR C: UNDERSTANDING NATION-STATE MOTIVES BEHIND TODAY'S ADVANCED CYBER ATTACKS 2 (2013), *available at* http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

[5] WILSHUSEN, *supra* note 1.

[6] BRITISH HOUSE OF COMMONS DEFENCE COMMITTEE, 1 DEFENCE AND CYBER-SECURITY 7 (2012), *available at* http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf.

[7] DUTCH MINISTRY OF DEFENCE, THE DEFENSE CYBER STRATEGY 5 (2012), *available at* http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.

As we can see in the following graphic, cyber threat sources range from individual hackers, which pose the least amount of danger, to nation states, which are the most dangerous.[8]



In response to these and other potential threats, countries began to implement measures to ensure that the IT infrastructures of both the private and public sector would be least exposed. As a result, national Cyber security strategies (CSS) started to become a reality and in some cases, eventually lead to the development later of national Cyber defense strategies (CDS).

According to the European Union Agency for Network and Information Security, a CSS is a tool that improves the security and resilience of national information infrastructures and services.[9] It is a "high-level, top-down approach to Cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe."[10]

On a similar note, the National Security Framework Manual defines a CSS as "the focused application of specific governmental levers and information assurance principles to public, private, and relevant international ICT systems,

[8] *See* ALAN BALDWIN & JOHN PALFREYMAN, INT'L BUS. MACHINES CORP., CYBER DEFENSE: UNDERSTANDING AND COMBATING THE THREAT 5 (2009), *available at* http://public.dhe.ibm.com/common/ssi/rep_wh/n/AEW03001USEN/AEW03001USEN.PDF.

[9] EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., *supra* note 2, at 4.

[10] *Id.*

and their associated content, where these systems directly pertain to national security."[11]

It is important to point out that the understanding of Cyber security tends to vary from country to country, due to the lack of common understanding and approaches between the nations.[12] To this extent, we find that the definition of Cyber security given by the Government of France as a "desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity, or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible,"[13] is the one definition that most relates to Cyber defense.[14]

Nonetheless, it seems clear that the implementation and improvement of CSS comprises a range of elements that usually include documents of political nature, laws, regulations, and administrative measures within a State. Furthermore, training, education, and international cooperation are important features of every CSS in order to function on an operational and tactical level,[15] as we shall demonstrate.

The NATO Cooperative Cyber Defense Centre of Excellence[16] highlights the most relevant CSS and/or CDS drafted to this day,[17] as we can see in the following table:

[11] THE NATO SCIENCE FOR PEACE AND SECURITY PROGRAMME, NATIONAL CYBER SECURITY FRAMEWORK MANUAL XVI, 29, 42 (Alexandra Klimburg ed. 2012).

[12] EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., *supra* note 2, at 9.

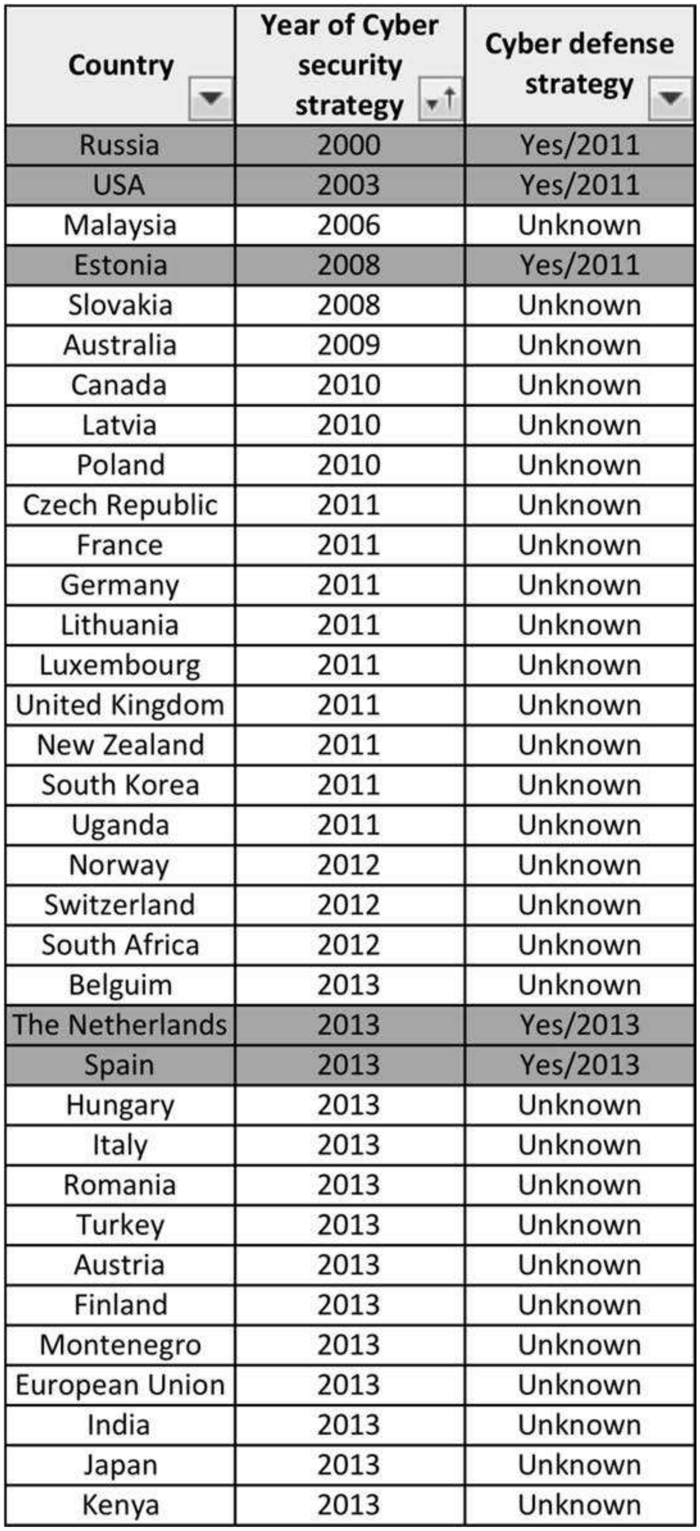
[13] FRENCH NETWORK AND INFO. SEC. AGENCY, INFORMATION SYSTEMS DEFENCE AND SECURITY: FRANCE'S STRATEGY 21 (2011), *available at* http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

[14] *Compare* UNITED NATIONS INT'L TELECOMM. UNION, http://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx (last visited Jan. 19, 2014) (defining cyber defense as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"), *with* US DEPT. OF HOMELAND SEC., NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, http://niccs.us-cert.gov/glossary (last visited Jan. 19, 2014) (defining cyber defense as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation").

[15] THE NATO SCIENCE FOR PEACE AND SECURITY PROGRAMME, *supra* note 11, at XVI, 29, 42.

[16] *See* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, https://ccdcoe.org/328.html (last visited Nov. 19, 2013) (explaining that this organization, established in 2008, is a NATO-accredited International Military Organization dealing with education, consultation, lessons learned, research and development in the field of Cyber security, and is currently sponsored by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the USA).

[17] *See id.*



Country	Year of Cyber security strategy	Cyber defense strategy
Russia	2000	Yes/2011
USA	2003	Yes/2011
Malaysia	2006	Unknown
Estonia	2008	Yes/2011
Slovakia	2008	Unknown
Australia	2009	Unknown
Canada	2010	Unknown
Latvia	2010	Unknown
Poland	2010	Unknown
Czech Republic	2011	Unknown
France	2011	Unknown
Germany	2011	Unknown
Lithuania	2011	Unknown
Luxembourg	2011	Unknown
United Kingdom	2011	Unknown
New Zealand	2011	Unknown
South Korea	2011	Unknown
Uganda	2011	Unknown
Norway	2012	Unknown
Switzerland	2012	Unknown
South Africa	2012	Unknown
Belguim	2013	Unknown
The Netherlands	2013	Yes/2013
Spain	2013	Yes/2013
Hungary	2013	Unknown
Italy	2013	Unknown
Romania	2013	Unknown
Turkey	2013	Unknown
Austria	2013	Unknown
Finland	2013	Unknown
Montenegro	2013	Unknown
European Union	2013	Unknown
India	2013	Unknown
Japan	2013	Unknown
Kenya	2013	Unknown

In regards to this list, the following observations are significant:

1. The majority of the strategies were published in the year 2013.

2. Russia and the USA were among the first countries to draft a CSS, subsequently drafting a CDS in the following years.

3. Only five of the thirty-five countries listed have a proper CDS.

4. Normally, the countries that have a CDS previously implemented a CSS, except in the case of case of Spain, which was almost simultaneously.

Upon the evidence presented so far, it is safe to say that the majority of the countries on the list are most likely to draft a CDS in the very near future, based on the broad goals and objectives of their parent CSS.

Ensuring Cyber security, enforcing rights, and protecting critical information infrastructures require major efforts by the state, both at the national level and in cooperation with international partners. A CSS will only be successful "if all players act as partners and fulfill their tasks together."[18]

Let us have a look at the role that some of these strategies have placed upon industry and society, relating to the education, training and research of a CSS and CDS.

III. CYBER DEFENSE STRATEGIES AND EDUCATION

The Government of France defined the term cyber defense as "the set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical."[19]

Cyber defense capabilities form an important and viable addition to existing military capabilities in that they offer support and reinforcement for operational capabilities in all domains. "These cyber assets strengthen the armed forces' actions for all military functions, including logistics, command & control, intelligence, force protection, maneuver and firepower."[20]

In order to develop Cyber defense capabilities, countries must take into account that they cannot be limited to only a national level and must rely upon a "network of allies with whom real-time information can be exchanged on vulnerabilities, protection mechanisms, attacks and countermeasures that can be

[18] FED. MINISTRY OF THE INTERIOR, CYBER SECURITY STRATEGY FOR GERMANY 4 (2011), *available at* http://www.CIO.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=E8F68C8EEA9C1D6138AF143B7D6CAF54.2_cid289?__blob=publicationFile.

[19] FRENCH NETWORK AND INFO. SEC. AGENCY, *supra* note 13, at 21.

[20] DUTCH MINISTRY OF DEFENCE, *supra* note 7, at 8.

implemented against cyber-attacks led directly or indirectly by States or terrorist groups."[21]

Furthermore, effective mitigation against the threat of cyber-attack can only come from a combination of technical and nontechnical measures. Technical mitigation techniques can include firewalls and network intrusion detection. Nontechnical mitigation usually combines leadership, education, and policy development. "An effective Defense against the ever-evolving threat can only be achieved through a balance between these two complementary techniques."[22]

In 2011, the United States Department of Defense identified five strategic initiatives involving cyberspace and the national Defense strategy.[23] Strategic initiative five strived to "leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation," in line with the following statement:

> The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives. Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations. DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.[24]

Education in Cyber security and Cyber defense settings will normally be linked to research and development (R&D), as is the case for the USA and the European Union (EU). In the EU, the European Agency for Network and Information Security stated in 2012 that European universities and R&D institutions do not produce enough Cyber security experts to meet the increasing needs of this sector. Therefore, the objectives of a training and education program within the EU could include the following:

[21] FRENCH NETWORK AND INFO. SEC. AGENCY, *supra* note 13, at 11.

[22] ALAN BALDWIN & JOHN PALFREYMAN, *supra* note 8, at 3.

[23] U.S. DEPT. OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5-10 (2011), *available at* www.defense.gov/news/d20110714cyber.pdf. (identifying the following: Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential; Strategic Initiative 2: Employ new Defense operating concepts to protect DoD networks and systems; Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government Cyber security strategy; Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective Cyber security; Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation).

[24] *Id.* at 10.

1. To enhance the operational capabilities of the existing information security workforce.

   Action: Create a national register with accredited Cyber security experts with teaching skills.

2. To encourage students to join and then prepare them to enter the Cyber security field.

   Action: Add information security courses to university curricula, not only to the ones related with computer science but also to any professional specialty tailored to the needs of that profession.

3. To promote and encourage the relations between information security academic environments and the information security industry.

   Action: Support the security accreditation and certification of skilled personnel in key working posts in every industrial sector.

Similarly, the Czech Republic CSS of 2012 stated the following on education and training programs:

> Cooperation aimed at creating training programmes focusing on cybernetic security shall be started with the academic and private spheres. Needs for qualification in cybernetic security, opportunities of school and other education shall be evaluated on a regular basis. The issue of cybernetic security will be implemented into all levels of education.[25]

The implementation of Cyber security awareness into all levels of education seems to be one of the focal points of the Czech strategy. The Hungarian CSS of 2013 points in this direction as well, revealing a slight trend within the EU:

> Education, research & development: Hungary pays particular attention to integrating cyber security as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional retraining courses. Hungary strives for strategic cooperation with university and scientific research locations which have achieved outstanding and internationally

[25] GOV'T OF THE CZECH REPUBLIC, STRATEGY OF THE CZECH REPUBLIC IN THE FIELD OF CYBERNETIC SECURITY FOR 2012-2015 8 (2011), *available at* https://ccdcoe.org./328.html (follow "Strategy of the Czech Republic in the Field of Cybernetic Security for 2012-2015" hyperlink).

> recognised results in cyber security research and development and help establish cyber security centres of excellence.[26]

Also in this direction, the Government of France stated that the long-term objective in their CSS is to "raise citizens' awareness of Cyber security issues during the education process," requiring the "implementation of an active governmental communication policy."[27]

On a similar note, the Dutch CDS acknowledges the importance of Cyber security awareness, stating that "all defence personnel must be aware of the risks associated with the use of digital assets."[28] Cyber security awareness will become an integrated part of all defense training courses. To this extent, cooperation with public-sector partners, universities and the private sector will be needed in the areas of R&D and training.[29]

High education institutions, especially universities, will play a prominent role in achieving all of this. That is why the Government of Norway identified in its CSS seven strategic priorities, one of them being the "high quality national research and development in the field of information security" in which all stakeholders should strive to facilitate productive interaction between leading ICT companies and academic environments across sectors.[30]

Another example is the British CSS published in 2011 which drafted an action plan that included the encouragement, support, and development of education at all levels, as well as crucial skills and R&D.[31] Specifically, the strategy looked to establish certification programs for cyber security professionals through postgraduate education.[32]

Based on an interview that the authors of this article had with the commanding General Carlos Gómez López de Medina, the Spanish Joint Cyber Defense Command, which was created in 2013 and which coordinates the Spanish CDS,[33] is developing a Master's Degree in Cyber Defense along with several Spanish public institutions, including the Ministry of Defense. This effort

[26] GOV'T OF HUNGARY, GOVERNMENT DECISION NO. 1139/2013 (21 MARCH) ON THE NATIONAL CYBER SECURITY STRATEGY OF HUNGARY 5-6 (2013), *available at* http://www.nbf.hu/anyagok/Government Decision No 1139_2013 on the National Cyber Security Strategy of Hungary.docx (Last visited: 23/12/2013).

[27] FRENCH NETWORK AND INFO. SEC. AGENCY, *supra* note 13, at 14.

[28] DUTCH MINISTRY OF DEFENCE, *supra* note 7, at 9.

[29] *Id.* at 15.

[30] NORWEGIAN MINISTRIES, CYBER SECURITY STRATEGY FOR NORWAY 17 (2012), *available at* http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_ Norway.pdf.

[31] BRITISH CABINET OFFICE, THE UK CYBER SECURITY STRATEGY PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 9 (2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[32] *Id.* at 42.

[33] ESTADO MAYOR DE LA DEFENSA, MANDO DE CONJUTO DE CIBERDEFENSA DE LAW FUERZAS ARMADAS, http://www.emad.mde.es/CIBERDEFENSA/ (last visited on Dec. 23, 2013).

is in addition to the Cyber defense training programs they are set to develop in 2014 for their personnel, focused primarily on military Cyber security expertise.

Finally, the Indian CSS that was published in 2013 established in the following goals, found in objective J regarding "Human Resource Development":

1. To foster education and training programs both in formal and informal sectors to support the Nation's Cyber security needs and build capacity.

2. To establish Cyber security training infrastructure across the country by way of public private partnership arrangements.

3. To establish Cyber security concept labs for awareness and skill development in key areas.

4. To establish institutional mechanisms for capacity building for Law Enforcement Agencies.[34]

IV. CHALLENGES AND RECOMMENDATIONS

As we have seen, the implementation, maintenance and improvement of a national CDS involves a range of elements in which education has a predominant role right now.

The coordination of both the private and public sectors is needed in order to develop and provide the appropriate curriculum needed for the principal stakeholders involved in the CDS of any modern nation.

Some of the challenges faced by these stakeholders are:

1. Ensuring the trust and cooperation of other countries.

2. Integrating Cyber security awareness in all levels of education.

3. Promoting the development of Cyber security professionals.

4. Ensuring cooperation between state, industry, and society.

In order to overcome these challenges, we recommend the following:

a) Involvement of higher education and R&D institutions, both public and private, in the drafting and implementation of CSS and CDS.

[34] GOV'T OF INDIA, NOTIFICATION ON NATIONAL CYBER SECURITY POLICY- 2013 (NCSP-2013) 9 (2013), *available at* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf.

b) Clear, specific and short term goals for CSS and CDS.

c) Sharing of knowledge and information with the general society towards the goals of CSS and CDS.