# Project Deliverable

**Project Number:** 611014  
**Project Acronym:** CONNECT2SEA  
**Project Title:**  
Supporting European Union and Southeast Asia ICT strategic partnership and policy dialogue: Connecting ICT EU-SEA Research, Development and Innovation Knowledge

<table>
<thead>
<tr>
<th>Instrument:</th>
<th>Thematic Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordination and support action</td>
<td>ICT</td>
</tr>
</tbody>
</table>

**Title**

**D3.3 Report on horizontal pilot actions, with assessment and feedback to the policy recommendations**  
**TOWARD SEA-EU COOPERATION IN CYBER SECURITY**

<table>
<thead>
<tr>
<th>Contractual Delivery Date:</th>
<th>Actual Delivery Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Month 27 (February 2016)</td>
<td>Month 28 (March 8, 2016)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Start date of project:</th>
<th>Duration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December, 1st 2013</td>
<td>30 months</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization name of lead contractor for this deliverable:</th>
<th>Document version:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITI-VNU</td>
<td>V3.0</td>
</tr>
</tbody>
</table>

**Dissemination level (Project co-funded by the European Commission within the Seventh Framework Programme)**

<table>
<thead>
<tr>
<th>PU</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP</td>
<td>Restricted to other programme participants (including the Commission)</td>
</tr>
<tr>
<td>RE</td>
<td>Restricted to a group defined by the consortium (including the Commission)</td>
</tr>
<tr>
<td>CO</td>
<td>Confidential, only for members of the consortium (including the Commission)</td>
</tr>
</tbody>
</table>

| X |
Authors (organizations):
ITI-VNU, Vietnam (responsible), FORTH, Greece (chapters on EU priorities and cybersecurity forum interactive session)
Contributors: ASTI (The Philippines), NECTEC (Thailand), USM (Malaysia), BPPT (Indonesia), inno TSD (France)

Abstract:
This report aims to clarify the policy recommendations for further cooperation among all countries, especially among ASEAN and EU countries in the progress of common actions against cyber threats. The research was done by both theoretical and empirical studies, based on the information and data provided by CONNECT2SEA partners from ASEAN and EU countries, in addition with data surveyed by 2 dashboards on R&D and policy aspects within ASEAN. The sources to compile this paper also referred to European Union’s 7th Framework programme (ICT part) and Horizon 2020 programmes (ICT parts), and the ASEAN ICT Master Plan. The literature reviews are also done for examination of the situation and solutions given by ASEAN countries in development of SWOT analyses against cyber-attacks. The contribution of various experts across ASEAN and EU countries via 2 workshops in Hanoi, Vietnam and Manila, Philippines, plus the exchange information via email, website... helped to finalise this report. The findings indicated some weaknesses among ASEAN at capability on collaboration, networking and common actions against cyber threats. The counties with lower development in ASEAN also have weaker regulation, strategy and organization against cyberattacks. The industry involvement is also weak in ASEAN. The new technology which are popular in Europe seem need more time to be well known in ASEAN and in some case, ASEAN should put forward pilot implementation, especially in e-Government, e-Commerce. The results also give out several proposals of policy recommendation on cyber-security, in the area of cryptography technology, public private partnership models and human resource improvement.

Keywords:
Cyber-Security; Policy; R&D; Weakness; Challenge; Horizon 2020; ASEAN ICT Master Plan; Dashboard; Workshop.

Disclaimer
THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Any liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed. No license, express or implied, by estoppels or otherwise, to any intellectual property rights are granted herein. The members of the project CONNECT2SEA do not accept any liability for actions or omissions of CONNECT2SEA members or third parties and disclaims any obligation to enforce the use of this document. This document is subject to change without notice.

© 2015CONNECT2SEA Partners
This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement No 611014
Revision History
The following table describes the main changes done in the document since it was created.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
<th>Author (Organisation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 2015</td>
<td>Simple version with matrix, lack of dashboard</td>
<td>ITI-VNU</td>
</tr>
<tr>
<td>2.0</td>
<td>October 2015</td>
<td>Collected dashboard, EU input</td>
<td>ITI-VNU, FORTH</td>
</tr>
<tr>
<td>2.1</td>
<td>November 2015</td>
<td>additional analyses, dashboard filled, experts input</td>
<td>ITI-VNU, FORTH, contributions from CONNECT2SEA partners</td>
</tr>
<tr>
<td>2.2</td>
<td>February 2016</td>
<td>Integration of materials from cybersecurity forum in Manila, the Philippines</td>
<td>ITI-VNU, FORTH</td>
</tr>
<tr>
<td>3.0</td>
<td>March 2, 2016</td>
<td>Final version with recommendations and lessons</td>
<td>ITI-VNU</td>
</tr>
</tbody>
</table>
Executive Summary

This document presents a report on some common priorities to promote cooperation regarding the cyber-security between Europe and ASEAN countries. The sources that have been used in order to compile this Report are the H2020 work programmes on cyber-security, and Information and Communications Technology (ICT) in general, of Europe and data, information that has been provided by CONNECT2SEA partners from ASEAN countries; specifically those countries include Philippines, Malaysia, Thailand, Indonesia and Vietnam. In addition, the report also uses a lot of working papers, publications which have content relating to ASEAN ICT sector, especially in cyber-security. By a systematic analysis, we have found 28 R&D fields and activities which are partly matched among EU and 5 ASEAN countries. Among those, there are 7 R&D fields and activities fully matched among all EU and all 5 ASEAN countries. The report also proposes several projects and actions based on these 7 full matches to promote further cooperation between EU and ASEAN in terms of cyber-security. The R&D questionnaires and policy dashboard also shows that the ASEAN countries are lagging behind the European countries. The projects with public private partnerships might be interested in ASEAN, especially in implementation of policy and human resources promotion and improvement. Regarding R&D interests among ASEAN, the report found top 12 R&D issues which are of the highest interest in ASEAN countries. In particular, the new advanced R&D trends, such as Cloud Computing, Big Data, Internet of Things, Cryptography, e-Services are highly interested by ASEAN countries. The report also presents the lessons learned from the 2 workshops organized in Hanoi (Vietnam) and Manila (Philippines). The discussions in these 2 workshops show the weaknesses in networking and community cooperation to cope up with cyber-security in ASEAN.
Table of Contents

1 INTRODUCTION ........................................................................................................................................... 8
    1.1 PURPOSE OF THIS REPORT ....................................................................................................................... 8
    1.2 STRUCTURE OF THIS DOCUMENT ............................................................................................................. 8
    1.3 SCOPE ...................................................................................................................................................... 8
    1.4 CONTRIBUTORS ......................................................................................................................................... 9

2 CYBER-SECURITY TRENDS AND POLICY IN THE WORLD ................................................................. 10
    2.1 CYBER-SECURITY TRENDS ...................................................................................................................... 10
    2.2 CYBER-SECURITY POLICY MAKING ....................................................................................................... 12

3 ASEAN’S APPROACH TO CYBER-SECURITY ..................................................................................... 14
    3.1 NEEDS FOR CYBER-SECURITY ................................................................................................................ 14
    3.2 ASEAN’S STRENGTHS IN CYBER-SECURITY ......................................................................................... 15
    3.3 ASEAN’S WEAKNESSES IN CYBER-SECURITY ...................................................................................... 16
    3.4 ASEAN’S OPPORTUNITY IN CYBER-SECURITY ...................................................................................... 17
    3.5 ASEAN’S CHALLENGES IN CYBER-SECURITY ...................................................................................... 19

4 EUROPE’S CYBER-SECURITY PRIORITIES IN HORIZON 2020 ....................................................... 20
    4.1 FUTURE AND EMERGING TECHNOLOGIES (FET) ................................................................................ 20
    4.2 EUROPEAN RESEARCH INFRASTRUCTURES, INCLUDING E-INFRASTRUCTURES (EINFRA) ........... 21
    4.3 INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) ......................................................... 22
    4.4 INTERNATIONAL JOINT COLLABORATIONS ........................................................................................... 23
    4.5 NANOTECHNOLOGIES, ADVANCED MATERIALS, ADVANCED MANUFACTURING AND PROCESSING,
        AND BIOTECHNOLOGY (FoF) .................................................................................................................. 24
    4.6 INNOVATION IN SMES (INNOSUP) .......................................................................................................... 24
    4.7 SOCIETAL CHALLENGES - SECURE, CLEAN AND EFFICIENT ENERGY (LCE) ................................. 24
    4.8 SMART, GREEN AND INTEGRATED TRANSPORT (MG) .......................................................................... 25
    4.9 CLIMATE ACTION, ENVIRONMENT, RESOURCE EFFICIENCY AND RAW MATERIALS (SC) ............ 25
    4.10 SECURE SOCIETIES – PROTECTING FREEDOM AND SECURITY OF EUROPE AND ITS CITIZENS (DSR) .. 26
    4.11 DIGITAL SECURITY: CYBER-SECURITY, PRIVACY AND TRUST (DS) ............................................... 26
    4.12 DIGITAL SECURITY POLICY ................................................................................................................... 27
    4.13 THE WORK PROGRAM 2016 - 2017 ON LEADERSHIP IN ENABLING AND INDUSTRIAL TECHNOLOGIES
        INFORMATION AND COMMUNICATION TECHNOLOGIES ............................................................. 29
    4.14 NEW IN 2016-2017: SCIENCE WITH AND FOR SOCIETY .................................................................. 30
    4.15 NEW IN 2016-2017: CROSS-CUTTING ACTIVITIES (FOCUS AREAS) ............................................. 30
    4.16 STATE-OF-THE-ART OF SECURE ICT LANDSCAPE-NIS PLATFORM ............................................... 31

5 EUROPEAN TECHNOLOGY PLATFORMS AND CYBER-SECURITY PRIORITIES .................. 32
    5.1 ARTEMIS INDUSTRY ASSOCIATION ........................................................................................................ 32
    5.1.1 ARTEMIS High Level Vision 2030 ........................................................................................................ 32
    5.1.2 ARTEMIS Strategic Research Agenda ................................................................................................... 33
    5.2 ENIAC JOINT UNDERTAKING .................................................................................................................. 34
        5.2.1 ENIAC Annual Work Programme 2013 ............................................................................................ 34
6 CYBER-SECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE ................................................................. 44

6.1 R&D PRIORITIES IN THE CYBER-SECURITY STRATEGY ........................................ 44

6.2 INTERNATIONAL COOPERATION IN THE CYBER-SECURITY STRATEGY .................. 45

7 ASEAN’S CYBER-SECURITY PRIORITIES ..................................................................... 46

7.1 CYBER-SECURITY EMERGENCY READINESS.............................................................. 46

7.2 CYBER-SECURITY PROTECTION ............................................................................... 47

7.3 CRITICAL INFRASTRUCTURE PROTECTION .............................................................. 48

7.4 PUBLIC SECURITY AND SAFETY .............................................................................. 49

7.5 ASEAN’S MEASURES TOWARD CYBER-SECURITY .................................................... 49

8 COMPARATIVE ANALYSIS OF EU AND ASEAN CYBER-SECURITY PRIORITIES ........ 51

8.1 THE PRINCIPLE AND OUTCOMES OF COMPARATIVE MATRIX .............................. 51

8.2 THE TABLE OF COMPARATIVE MATRIX .................................................................. 53

9 RECOMMENDATIONS FOR POSSIBLE EU-ASEAN JOINT COOPERATION ............. 78

9.1 PARTICIPATE IN LARGE VISIONARY PROJECTS ......................................................... 78

9.1.1 Promote Research and Development on the enterprise infrastructure protection in the evolution toward SDN ................................................................. 78

9.1.2 EU-ASEAN Cyber Security Professional Training and Technology Transfer ............. 79

9.1.3 ASEAN Technical support center for secure key enterprise applications and open sources 79

9.2 RECOMMENDATIONS EXPAND THE CYBER-SECURITY COOPERATION ............ 80

9.2.1 Recommendations to EU and ASEAN bodies ......................................................... 80

9.2.2 Recommendations to ASEAN and/or EU Member states ...................................... 81

9.2.3 Recommendations to the ASEAN RDI organizations .............................................. 81

9.3 RECOMMENDATIONS FOR CYBER-SECURITY ACTIVITIES PROMOTION .......... 81

9.3.1 Linked-In Community of Practice .......................................................................... 81

9.3.2 ASEAN body (Committee) on Cyber-security ......................................................... 83

9.3.3 Pilot technical assistance and Cyber Security Architecture Framework .................. 84

10 CYBER-SECURITY POLICY ANALYSIS .................................................................... 85

10.1 THE ASEAN CYBER-SECURITY DASHBOARD ......................................................... 87

10.2 THE ANALYSES OF EU CYBER-SECURITY POLICY DASHBOARD ......................... 90

11 ASEAN CYBER-SECURITY R&D ANALYSIS ............................................................ 92
11.1 THE R&D CYBER-SECURITY DASHBOARD .......................................................... 92
11.2 CYBER-SECURITY R&D DASHBOARD ANALYSES ........................................... 94

12 LESSONS LEARNT FROM THE EVENTS ORGANIZED BY CONNECT2SEA PROJECT .... 97

12.1 LESSONS LEARNT FROM HANOI WORKSHOP (DECEMBER, 2015) ......................... 97
12.1.1 Summary of Hanoi Workshop .............................................................................. 97
12.1.2 Lessons learnt from Hanoi Workshop ................................................................ 98
12.2 LESSONS LEARNT FROM MANILA CYBERSECURITY FORUM (JANUARY 2016) ............... 99

13 CONCLUSIONS ....................................................................................................... 102

14 REFERENCES AND SOURCES .............................................................................. 103

ANNEX A TABLE OF ACTIVITIES IN EU HORIZON 2020 RELATED TO CYBER-SECURITY .... 106

ANNEX B MANILA EU-SEA CYBERSECURITY FORUM SURVEY ....................................... 112

List of Figures

Figure 1: Over view of current emerging cyber-threats ..................................................... 11
Figure 2: Megatrends and key trends in cyber-security ...................................................... 32

List of Tables

Table 1: Matrix of matching priorities among ASEAN and Horizon 2020 ......................... 54
Table 2: ASEAN Cyber-security Policy Dashboard .............................................................. 87
Table 3: ASEAN Cyber-security R&D Dashboard ............................................................... 92
Table 4: Top 12 issues with highest points in ASEAN ......................................................... 95
1 Introduction

1.1 Purpose of this report
The CONNECT2SEA report is intended to communicate and recommend the prioritized strategic requirements of ASEAN, aligned with European objectives, to further cooperation in cyber-security.

1.2 Structure of this Document
This deliverable is structured as follows:
Section 1 makes an introduction
Section 2 describes the trends of cyber-security and policy in the world
Section 3 describes ASEAN approach to cyber-security
Section 4 summarises the cyber-security priorities identified from analysing European Horizon 2020 work programme
Section 5 summarises the European Technology Platforms and cyber-security priorities
Section 6 discusses about Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace
Section 7 describes ASEAN’s cyber-security priorities
Section 8 provides a comparative analysis of the EU and ASEAN priorities
Section 9 summarises the recommendations and actions in support of possible future EU-ASEAN joint cooperation in the cyber-security area
Section 10 discusses about Cyber-security Policy Analysis in ASEAN using the dashboard of cyber-security policy maturity
Section 11 discusses about ASEAN Cyber-security R&D Analysis
Section 12 collects some lessons learned from the workshops and Forums organized by CONNECT2SEA in Hanoi (December 2015), Manila (January 2016), Jakarta (March 2016).
Section 13 gives out conclusions
References with website links are provided in the final section for the roadmaps and other sources in ASEAN and the EU that were utilised in preparing this report.

1.3 Scope
The scope of this deliverable is to summarise data and information provided from 5 countries in ASEAN (Philippines, Malaysia, Thailand, Indonesia and Vietnam) with reference to the prioritised fields and activities in the Horizon 2020 work programme on cyber-security, and ICT in general, of Europe.
1.4 Contributors

The deliverable was prepared with contributions from many CONNECT2SEA project partners, each playing an important role in preparing the contents:

ITI-VNU is the lead editor for the document and organised the data gathering.

FORTH forms the first framework for matching R&D interests between EU and ASEAN, and contributes with the presentation of EU landscape and priorities in cybersecurity.

Inno TSD establishes the communications, give guidance and methodological support and helps to collect information.

NECTEC, ASTI, USM, BPPT provide contributions related to cybersecurity in their respective countries, to establish a common view.

We would like to thank all ASEAN experts who provided feedback and contributions for this report, including but not limited to the cybersecurity policy maturity questionnaire.

We also would like to thank Dr Gerd Meier zu Köcker, Director, Institute for Innovation and Technology, Germany, Advisory Board member of CONNECT2SEA project, and Dr Brett Lempereur, Lecturer in Computing at Liverpool John Moores University, specialist in Digital Forensics and Computer Security, for the review of the initial version of this report and useful suggestions.
2 Cyber-security Trends and Policy in the World

2.1 Cyber-security Trends

The threats to the fast changing technologies are also evolving quickly. The cyber criminals have found unprecedented ways to damage users’ applications and infrastructure. According to a research done by SOPHOS (2015), namely “Security Threat Trends 2015”, the following 10 big things will have significant impact in 2015 and beyond:

1. **Exploit mitigations reduce the number of vulnerabilities**: Today web based infection and browser based exploits are a clear leader in delivery for malicious code instead of the spams. Microsoft has invested in exploit mitigations such as DEP and ASLR to prevent the execution of attacker code in certain parts of a computer’s memory and to make writing attack code difficult by shuffling memory around. A huge number of improvements have been made in Windows 8 and Windows 8.1.

2. **Internet of Things attacks move from proof-of-concept to mainstream risks**: In 2014 there were more evidence that manufacturers of Internet of Things (IoT) devices have failed to implement basic security standards. As the consumers continue to grow their awareness of this issue, the protection against these attacks becomes a commercial requirement.

3. **Encryption becomes standard, but not everyone is happy about it**: Full-disk encryption becomes a default feature provided by the OS vendors or in hard disks and managed by security vendors.

4. **More major flaws in widely-used software that had escaped notice by the security industry over the past 15 years**: A number of impactful bugs outside the standard Microsoft platforms has been found and attract attention of the security industry. The events of 2014 have boosted the cybercriminals’ interest in less considered software and systems in the coming years. So the enterprises and the vendors should have a response strategy for it.

5. **Regulatory landscape forces greater disclosure and liability, particularly in Europe**: The European Union has implemented tough new standards in 2015, with enforcement commencing in 2016. The recent surveys in Europe reveal that the majority of businesses do not know that this is coming, even the failure to protect data could result in heavy punitive fines up to €100 million or 5% of annual revenue.

6. **Attackers increase focus on mobile payment systems and stick more to traditional payment fraud**: Mobile payment systems were the talk of 2014 after Apple stormed ahead with Apple Pay. Undoubtedly, there will be implementation mistakes in these new protocols, but these implementations provide greater convenience and improve upon the security standards of many of the world’s credit or debit cards.

7. **Global skills gap continues to increase, with incident response and education a key focus**: Mandatory disclosure of the data breaches and attacks becomes more common. The cyber-security skills shortage is becoming more critical.

8. **Attack services and exploit kits arise for mobile (and other) platforms**: In the last few years, the products and services to make hacking and exploitation point-and-click easy on mobile devices has risen. More crime packs and tools focusing on the mobile devices will be seen soon.
9. *The gap between ICS/SCADA and real world security only grows bigger:* Industrial control systems (ICS) are at least 10 years behind the desktop environment in terms of security. These platforms lack authentication, encryption or integrity-checking. The only viable security strategy is to keep them isolated. Unfortunately, on surprisingly many occasions these systems have ended up inadvertently connected to outside networks.

10. *Interesting rootkit and bot capabilities may turn up new attack vectors:* Many of the attacks over the past few years have been at the application layer (even DDoS attacks were substantially focused on the application layer rather than the transport layer). We are in the process of changing major platforms and protocols and these changes are bringing flaws. For example, the IPv6 stack on Windows 7 and Windows 8 is vulnerable to a resource exhaustion flaw which allows an attacker to send continuous random router advertisements and consume 100% CPU of the system. Most people don’t even know the flaws is present.

The report of ENISA Threat Landscape 2014 (ETL2014) presents top threats, their current ranking and trend based on previous reports and their complexity. It also includes information about successful attacks in critical services of the Internet.

![Figure 1: Overview of current emerging cyber-threats](https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014)

Source: ENISA Threat Landscape 2014

---

The above picture presents briefly the findings of the ENISA ETL2014 report. Moreover, those findings are also in line with the Strategic Research Agenda of European Technology Platforms (ETPs)\(^2\) and especially the ETP research agendas, which deal with ICT and systems security. Most ETPs are related with vast amount of data and computing power, meaning many security and privacy issues as stated in their agendas.

### 2.2 Cyber-security Policy Making

According to report given by OECD (2012), namely “Cyber-security Policy Making at a Turning Point: Analysing a New Generation of National Cyber-security Strategies for the Internet Economy”, cyber-security has become a national policy priority. The analysis of this new generation of national cyber-security strategies reveals a fundamental evolution in government policy making where cyber-security is elevated among the government priorities. According to these strategies, governments’ general assessment is that:

- The Internet and ICTs are essential for economic and social development and form a vital infrastructure. The whole economy and society, including governments, become increasingly reliant on this digital infrastructure.

- Cyber threats are evolving and increasing at a fast pace. They are still initiated by criminal actors but also come from new sources, such as foreign states and political groups. Malicious actors are better organised, in particular to conceal their tracks, and the degree of sophistication has increased significantly, showing clear signs of professionalism.

As a consequence, the scope of almost all new cyber-security strategies has evolved from solely protecting individuals and organisations as distinct actors, to also protecting society as a whole. This change results from the evolution of the role of the Internet in society.

Regarding the policy making, the Cyber-security strategies of OECD members (also according to report given by OECD (2012)) generally adopt the action plans aimed to strengthen the following key priority areas:

1. **Government security**: Action plans include a series of initiatives, from the development of a situational awareness capacity to the rationalisation of government network infrastructures, and the generalisation of audits in the public sector.

2. **Protection of critical information infrastructures**: Action plans generally include measures related to the protection of critical information infrastructures.

3. **Fight against cyber-crime**: Action plans include many initiatives to develop law enforcement capacities; improve the legal framework and foster international cooperation on the basis of the Budapest Cyber-crime Convention.

4. **Awareness raising**: Action plans include many initiatives targeting specific populations such as children, SMEs and decision makers in government and critical infrastructures.

\(^2\)http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=etp
5. **Education**: Action plans recognise in particular the need for a stronger cyber-security workforce. The development of cyber-security skills is identified as a key priority by several countries.

6. **Response**: Strategies recognise the role played by Cyber-security Incident Response Teams (CSIRTs), and create a national CSIRT or strengthen it where it already exists.

7. **Research and Development (R&D)**: Being benefited from a relatively low level of attention in an OECD survey carried out in 2004 is elevated to much higher level of priority in new cyber-security strategies, generally focusing on better organisation and co-ordination of existing cyber-security R&D efforts in partnership with the private sector. One country, the United States, adopted a strategic plan for its cyber-security R&D programme.
3 ASEAN’s Approach to Cyber-security

The ASEAN’s state members have been acknowledged that ICT will continue to be the driver in all aspects of nation building in the next few decades. ICT is regarded as a growth sector for the region, employing nearly 12 million people and contributing more than USD 32 billion to ASEAN’s GDP (Caitriona, 2013), with expected significant future increase. ASEAN is interested in the wave of innovation and technology in general and ICT, in particular. Nevertheless, the expanding ICT usage leads to cyber vulnerabilities all over the ASEAN region. The following items continue to discuss much more and deeply about relevant issues to concern.

3.1 Needs for Cyber-security

In the recent years, the growth of ICT in Southeast Asia is already not too far behind the US, Europe and other countries in Northeast Asia like Japan and Republic of Korea. According to ASEAN E-Commerce Database Project released in 2010, ASEAN countries represent 6% of the Internet world users and the sum of global penetration level of ASEAN members countries are 20%, with Brunei Darussalam, Singapore and Malaysia having the biggest share of internet penetration, and Indonesia, Philippines, and Vietnam having the greatest numbers of internet user at more than thirty millions.

With this rate, ASEAN is in a good position to build an advanced ICT region with internet businesses run on it. Moreover, ASEAN has made a considerable progress in ICT development. ASEAN incorporates ICT development as one of the connectivity aspect in its recent master plan on building of ASEAN Community 2015. The Master Plan on ASEAN Connectivity encompasses physical, institutional and people-to-people connectivity with ICT as integral part of physical connectivity. In addition, the ASEAN ICT Master Plan 2011 - 2015 which gives more detailed information on how ASEAN wants to develop its ICT sector. ASEAN’s vision to build the ICT sector is to create a technologically advance and well-connected region. But, at the same time, ASEAN’s development on ICT does not pay enough attention to the security aspect. Knowing the important yet fragile system of ICT, ASEAN needs to be ready to face cyber threat that might occur. So far, all ASEAN member countries have Computer Emergency Response Team (CERT). ASEAN’s CERTs of countries also are members of Asia Pacific Computer Emergency Response Team (APCERT), a regional organization.

With proper instruments available in most of ASEAN member countries, the question remains whether the instruments are compatible enough to deal with the Secure Connection reality of cyber threat.

In Malaysia, the cyber-security organizations have reported that a total of 6,800 cyber-security incident reports as of July 2015 with fraud, intrusions and cyber harassment topping the list. The other cyber-security incidents were content-related, denial of service (DDoS), intrusion attempt, malicious codes, spam and vulnerabilities report. Nowadays, Malaysian exposure to the risk of cyber threat is higher as almost all private and public sectors are increasingly depending on the ICT in their business operations and services (Amirudin, 2015).
In Singapore, the adequate attention on the cyber domain is critical in view of government and society. As a developed, highly-networked country which relies on its reputation for security and stability to serve as a hub for businesses and attract talent, it is particularly vulnerable to such attacks. Singapore has faced growing cyber threats targeting government and non-government entities, including 2013 attacks by the global hacker group “Anonymous” and assaults on the websites of the office of the prime minister and president by its own citizens. The Vice President for Southeast Asia at McAfee, estimated that Singapore’s economy lost around $1.25 billion to cyber criminals annually.

In Indonesia, cyber-attacks had infiltrated around 80% of the public domain, including the top leaders of the country, and Indonesia has become the country with the highest risk in information technology security. For instances, there is increasing amount of defacement to Indonesia website (domain .id). If in 2012, the average monthly defacement attacks around 887 attacks, in 2013 the number of attacks rose 37% on average per month to reach 1384 attacks. In January 2013, hackers have defaced more than 12 government websites in Indonesia, that include several ministries and national police websites, following the arrest of an alleged hacker in East Java. Weak security and strong solidarity among underground hacker networks are at the heart of the problem. But those website defacement issues are just the tip of the iceberg, as it common knowledge that the most government websites are not secured and an easy target for low skilled hackers. Other crimes, such as e-commerce crimes or threats to critical national infrastructures, are more serious issues that have to be addressed by Indonesian government.

In Vietnam, according to a report released by Pricewaterhouse Coopers’ Technology Consulting, there were 280,000 cyber-attacks recorded in Ho Chi Minh City in 2014, a record of 300% increase from 2013. A report by AIG’s Asia Financial Lines also warned that Vietnam ranked 12th in the list of countries facing the most cyber-attacks. In addition, Vietnam ranked third in the list of countries with the most virus-infected applications downloaded for the Android operating system. Vietnam suffers yearly losses of nearly $380 million from cyber-attacks due to inadequate information security protection, according to AIG. A survey conducted by the Vietnam Information Security Association (VNISA) has stated that 55% of Vietnamese firms and institutions failed to establish procedures on information security. In fact, 45% of them were infected with self-spreading malicious codes. According to another survey by Ernst &Young, 49% of Vietnam’s firms did not see privacy as a top priority while 40% failed to research security issues.

### 3.2 ASEAN’s Strengths in Cyber-security

ASEAN has much strengths and opportunities in international cyber-security.

First, ASEAN is a central region for cooperation, especially among strong power countries such as US, China or Japan. Picturing ASEAN to be a connected region in ICT infrastructure is a great vision of an ICT hub. ASEAN’s centrality in the regional architecture of the wider Asia Pacific region as a neutral broker is significant in terms of international cyber-security cooperation. Since recently U.S. and China have political focus on cyber threats, ASEAN can work together with the United States and China to resolve the targeted cyber threats in the Asia Pacific region.

Second, while citizens in many areas of the region still do not have access to ICT, there is a lot of expanding room for development in ASEAN. According to the 2013 Impact Assessment...
report accompanying the European Commission’s Proposal for a Directive on network and information security, of the 2.1 billion Internet users worldwide, most are located in Asia (922.2 million). The next most significant region in terms of numbers of Internet users is Europe with 476.2 million users. China alone has 485 million Internet users - more than any other country or region (including Europe and the rest of Asia) - and an Internet penetration of only 36.3%. ASEAN, comprising ten Member States, has a total population of slightly over 600 million. Recent indicators forecast that the population growth rate is higher in most of the ASEAN countries than the Asian average.

Third, the strong commitment for cooperation in ICT in general and ICT security in particular among ASEAN state members as indicated in previous section. The Secure Connection vision, as stated in ASEAN ICT Master Plan 2011 - 2015 is heading “Towards an Empowering and Transformational ICT: Creating an Inclusive, Vibrant and Integrated ASEAN”. The first one is to equalize the infrastructure, knowledge and competence on ICT in ASEAN member countries, and the second one is to prepare the safety procedure for running a connected region that lies on ICT. The establishment of ASEAN ICT connectivity might be addressed for economic and social development of the region and placed below the pillar of economic with ASEAN Telecommunications and IT Ministers Meeting (TELMIN) as the one in charge for drafting master plan, but this arrangement will be prone to security implication if it does not have a proper protection from cyber-crime threats. The TELMIN is good mechanism for agreement on how ASEAN will secure its future ICT connectivity. Since most countries in ASEAN already have their CERT team, that can be imply the countries have realized the significance of securing their cyberspace. ASEAN realized that the cooperation among those teams is also necessary because cyber-crime is a contemporary threat to security which runs on a borderless cyberspace. The agreement also have to cover the borderless nature of cyber-crime, enables ASEAN member countries to investigate cyber-crime case in neighbouring countries in the region and processed the case according to regional agreement.

### 3.3 ASEAN’s Weaknesses in Cyber-security

There are some weaknesses which might affect the cooperation within the ASEAN region against cyber-security as below:

1. **Lack of networking activities**: the country each recognizes well the importance and takes strong action against cyber-security. In the regional, there is also strong cooperation commitment among all ASEAN state members in the combat against cyber threats. However, the real actions, the implementation with full cooperation and trans-borders activities against crimes in ICT sector is still weak. Although, there are many mechanism, forum, and dialogues in ASEAN Integration process and in ICT sector but there is still no committee at ASEAN level for cyber-security alone. There is also no e-community for common moves and mutual benefit cooperation to link all experts within ASEAN for joint actions against cyber-crimes. The weaknesses in networking will also impede current and future international cooperation efforts on cyber-security that are required to deal effectively with the cross-border nature of cyber incidents.

2. **Lack of region-wide cohesiveness**: National and regional moves to adopt comprehensive cyber-security strategies have been somewhat slow and fragmented
across the globe. This lack of region-wide cohesiveness does not help the region’s security and impairs the ASEAN Economic Community Blueprint to become a single market and production base. Indeed, an ASEAN-wide comprehensive cyber-security framework has yet to be well developed. In fact, the official public documents in cyber-security are still vague within ASEAN.

3. Lack of ICT experts and innovators: ASEAN is general still lack of ICT experts, professionals and innovators within ASEAN, which could be a weak point for cyber-security implementation. Furthermore, accrediting IT and cyber-security professionals with a regionally-recognised certification should also be considered to allow for regional cohesiveness. As it stands, ASEAN has completed eight Mutual Recognition Arrangements (MRAs) to facilitate the free movement of skilled labour in the region, albeit to varying degrees of cooperation in recognition of qualifications. However, of the eight professional groups listed, computer scientists and IT professionals are not listed (although engineering services are included). It is also worth considering the European Commission’s recent proposal under the February 2013 Cyber-security Strategy of the European Union of a roadmap for a “Network and Information Security Driving Licence”. Furthermore, the Commission also plans to organise with the support of the European Network and Information Security Agency (ENISA) in 2014, a “cyber-security championship” where university students across the region will compete in proposing network and information security solutions.

4. Less developed common standardization and no clear mutual approach for cyber threats. By this developing area of ASEAN, it is in the common interests of ASEAN states and the wider international community to adopt common standards and mutual recognition arrangements (MRAs) as regional initiatives for cyber-security to tackle cross-border cyber threats. The current lack of region-wide cohesiveness and a comprehensive framework is detrimental not just to the realisation of the ASEAN Economic Community but also to the overall security of the ASEAN region.

5. The diversified characteristics in culture, language, economic disparity might deter the combat against cyber-crime in ASEAN. The much differences among ASEAN state members lead to clear statement that the engagement in cyberspace transcends nation states in a borderless world is not practical. In reality, interactions in cyberspace remain within sovereign borders where national laws and regulations still apply. The cyber threat has existed for over a decade, but policymakers have been slow to address it, nationally and internationally. While each nation should continue to contribute to the formulation of international norms, priority should now be given to getting it right at home. These considerations need to be taken into account when addressing a cyber-resilience blueprint for ASEAN (Tim, 2014).

3.4 ASEAN’s Opportunity in Cyber-security

The cyber-security issues increasingly become very important factor in ASEAN security and attract the top interests by all member states.

Firstly, ASEAN is now interested fully in non-traditional security issues. In the ARF (ASEAN Regional Forum), under the principles of comprehensive security, a key purpose of ASEAN is to respond effectively to non-traditional security issues, thus, ARF clearly indicating the
cyber-security in ICT. The ICT is now important for social development, is promoted under the ASEAN Socio-Cultural Community Blueprint. ASEAN will become a single market and production base, a highly competitive economic region, and one that is fully integrated into the global economy. In order to sustain such regional economic growth and competitiveness, the Economic Community Blueprint identifies the importance of creating a secure and connected information infrastructure, and areas of cooperation include enhanced infrastructure and communications connectivity.

Secondly, the ICT sector becomes one of top sectors with much common agreement and becomes top priority to cooperate to promote the connectivity and development in ASEAN. The leaders of ASEAN approved the ASEAN ICT Master Plan 2011 - 2015 and now finalizing the ASEAN ICT Master Plan 2016 – 2020. The ASEAN Ministers who are responsible for Telecommunications and Information Technology unify to implement the plan of action to combat transnational crime, adoption of a common framework for ASEAN cyber-crime enforcement. James (2013) reported that while “cooperation among Asian countries in combating cyber-crime may in some ways be easier to obtain than cooperation in other aspects that are more closely linked to state power and competition, the utility of cyber-crime as a proxy for pursuing state goals could also limit the scope of any agreement or compliance with it”.

Thirdly, ASEAN is expanding the usage of ICT equipment and services as one of the quickest region in the world. ASEAN raises the probabilities of increased demands for ICT usage. Within the region, Internet users have high speed of growth rate in the world. It is estimated that mobile broadband subscriptions will be close to 70% of the world’s total population by 2017 (Heinl, 2013). Region targets for ASEAN are set for “exponential growth” in ICT adoption and a ramping up of infrastructure and human capital development is intended to achieve these targets. Furthermore, in order to improve speed as well as to lower interconnectivity costs, the region is currently assessing the feasibility of developing an ASEAN Internet-Exchange Network - a platform to facilitate intra-ASEAN Internet traffic “to facilitate peering among ASEAN Internet access providers”. The critical infrastructure protection will be essential, particularly in consideration of plans for the region which include establishing “an integrated and regional connectivity”.

Fourthly, the cyber-security has strong commitment by all ASEAN governments and has clear framework measures to take unified actions. The Framework for Cooperation on Network Security and Action Plan adopted for Information Technology was agreed in November 2012, under the Mactan Cebu Declaration. The measures include: (1) International and regional collaboration to enhance security of the ASEAN information infrastructure for “sustainable economic and social development”. (2) Working towards a “conducive, safe, secured and trusted environment and harmonised ICT rules and regulations that will promote trade, investment and entrepreneurship”. (3) Providing safe and secured fixed and mobile broadband. (4) Cooperating in the building and promotion of a secure online environment to enhance cyber-security and counteract online threats within and among ASEAN Member States. (5) Facilitating robust and resilient information infrastructure through the development and implementation of National Frameworks on Submarine Cable Connectivity Protection and Risk Mitigation. (6) Further enhancing policy framework development, cooperation and sharing of best practices on data protection and the protection of information infrastructures to safeguard the network among Member States. (7) Continue
collaboration among ASEAN CERTs such as the ASEAN CERTS Incident Drills so as to enhance incident investigation and coordination among CERTs.

3.5 ASEAN’s Challenges in Cyber-security

The digital divides and differing levels of ICT development and adoption should be the first obstacle upon prospects of regional cyber-security cooperation. They deter efforts in seriously tackling cross-border cyber related threats in ASEAN. The regional cooperation efforts can stimulate progress, fuelling collective security and the further enhancement of national cyber-security measures no matter where a state is on the spectrum of ICT development. In fact, such disparity in ICT development can advantage countries with a less developed ICT infrastructure and less connected critical infrastructure. As less digitally developed countries become more connected, lessons may be applied from other states’ experiences in countering cyber related threats, best practice policies and measures may be implemented, and both security and data privacy by design may be incorporated from the inception.

According to a report given by Heinl (2013), namely “Primary Global Cyber-security Challenges of Common Interest to ASEAN Members: Recent Status & Emerging Trends”, published by Rajaratnam School of International Studies of Singapore, in dealing with cyber threats, some of the most significant global challenges of common interest to ASEAN Member States include:

- The increasing volume and complexity of threats nowadays;
- The dilemma of accurate attribution;
- An increasing number of state and non-state actors;
- The lack of harmonised definitions and understanding of “cyber” terminology;
- Achieving effective public-private sector cooperation;
- Insufficient levels of R&D;
- The inadequacy and unavailability of expertise;
- Insufficient public awareness;
- The disparity in protection of civil liberties.
4 Europe’s Cyber-security Priorities in Horizon 2020

European Union, directly the European Commission released the Digital Agenda, in which, it is said that the securing network and information systems in the EU is essential to ensure prosperity and to keep the online economy running. The EU sees the Digital technologies and the Internet are the key factor of the development of society and economy and key enablers of prosperity and freedom. The agenda said clearly that the high level of network and information security across the EU is essential to ensure consumer confidence and to keep the online economy running. The European Union works on a number of fronts to ensure cyber-security in Europe, from providing the delivery of better internet for kids to implementing the international cooperation on cyber-security and cyber-crime.

To implement the R&D and solutions to cope up with the issues on cyber-security and promote cooperation, the Horizon 2020 is the recent initiative of EU Research and Innovation programme with nearly €80 billion of funding available over 7 years (2014 to 2020) – in addition to the private investment that this money will attract. It promises more breakthroughs, discoveries and world-firsts by taking great ideas from the lab to the market.

In the Horizon 2020 2014-2015 ICT Work programme, there are a lot of research sectors which are prioritized to push the research and innovation. Those priorities are also expected in the ICT Work programme for 2016-2017. Some of them may directly involve to cyber-security are described one by one in the following items.

4.1 Future and Emerging Technologies (FET)

Cyber-security as an application field needs a lot of enabling technologies. Future and Emerging Technologies (FET) programme has three complementary lines of action to address different methodologies and scales, from new ideas to long-term challenges:

- **FET Open**: focus on new ideas for radically new future technologies, at an early stage when there are few researchers working on a project topic. This can involve a wide range of new technological possibilities, inspired by cutting-edge science, unconventional collaborations or new research and innovation practices.

- **FET Proactive**: seeking to establish a critical mass of European researchers in a number of promising exploratory research topics. This supports areas that are not yet ready for inclusion in industry research roadmaps, with the aim of building up and structuring new interdisciplinary research communities.

- **FET Flagships**: hundreds of excellent European researchers unite forces to focus on solving an ambitious scientific and technological challenge.

Among three topics of action above, the first topic as FET Open has three priorities of research and innovation related to cyber-security, they are:

- Encourages new high-potential actors & high-tech SMEs: Recognising and stimulating the driving role of new high-potential actors in research and innovation, such as women, young researchers and high-tech SMEs, is also important for nurturing the scientific and industrial leaders of the future, including the R&D in cyber-security.
- Collaborative research and innovation actions in high-risk: FET supports collaborative research projects to open up new and promising fields of research, technology and innovation

- Research and innovation toward long-term vision: The combination of a game-changing long-term vision and technological concreteness positions FET research between blue-sky science on the one hand, and research driven by societal challenges or by industrial competitiveness on the other. It will bring closer science, engineering and society and accelerate the transition from upstream research to technology development and transformational impact.

In fact, FET Open supports early-stage joint science and technology research around new ideas for radically new future technologies. It will build up a diverse portfolio of targeted projects to explore a wide range of new technological possibilities, inspired by cutting-edge science, unconventional collaborations or new research and innovation practices.

4.2 European Research Infrastructures, including e-Infrastructures (EINFRA)

This section requires integration of different equipment, services and data sources, as well as extensive transnational collaboration. The aim is to promote the use and management of research infrastructures, including e-infrastructures, which will make a significant contribution to boosting Europe’s research and innovation potential.

The European countries approach to research infrastructures which has made remarkable progress in recent years with the implementation of the European Strategy Forum on Research Infrastructures (ESFRI) roadmap. The ESFRI Roadmap identifies new Research Infrastructures (RI) of European interest corresponding to the long term needs of the European research communities, covering all scientific areas, regardless of possible location.

The cyber-security involve directly to e-infrastructures aspect among EINFRA section. In the item of “EINFRA-5-2015 – Centres of Excellence for computing applications”, the Centres of Excellence (CoE) aim to integrate the encompassing not only HPC (High Performance Computing) software but also relevant aspects of hardware, data management/storage, connectivity, security, etc.

Also in the item of “EINFRA-7-2014 – Provision of core services across e-infrastructures”, the security is interest for EU toward the development and promotion of the uptake of a Digital Identifier e-infrastructure for digital objects (articles, datasets, collections, software, nomenclature, etc.). In this item, the appropriate researches should aim to overcome technical, organisational and legal obstacles for the implementation of an integrated and interoperable authentication and authorisation infrastructure (AAI) and to lower barriers for entry of organisations not already participating in identity federations, e.g. by providing scalable policy negotiation mechanisms, as well as legal guidance notably in data protection. It should also encourage the use of security token translation services to enable interoperability of different AAI’s, as well as accounting services for enabling interoperability and aggregation in recording the usage of resources securely and reliably, including for the highly distributed heterogeneous infrastructures envisaged for global research data.
In the “Specific features for Research Infrastructures” item, there is an important content regarding on e-Infrastructures. In which, the priority for joint research activities are focusing on the innovative solutions for communication network (increasing performance, improving management, exploiting new transmissions and digital technologies, deploying higher degrees of security and trust).

The Work Programme 2016-2017 was announced and we have identified the following items that also mention the security aspect:

EINFRA-12-2017: Data and Distributed Computing e-infrastructures for Open Science: The main objective is “to make research data discoverable, accessible, assessable, intelligible, useable, and wherever possible interoperable.” There is a specific target of the call that is focused on the security of the data in the distributed computing infrastructures. The call proposed should address the point of: “reliably address the aspects of privacy, cybersecurity and information assurance supporting multiple compartments with private, public or industrial corpus of data, protected from unauthorized access by secure interfaces”

EINFRA-22-2016: User-driven e-infrastructure innovation: The call is focused on exploiting e-Infrastructures for user-driven innovation in respond to community specific challenges. The call also aims in the cybersecurity assurance towards integrated identity management at global level.

4.3 Information and Communication Technologies (ICT)

In the pillar, namely “Industrial Leadership”, which aims to speed up development of the technologies and innovations, there is one sub-item located in the section of “Leadership in Enabling and Industrial Technologies”, name as “Information and Communication Technologies”. This ICT sub-item concentrate on the progress in electronics, microsystems, networking, the ability to master increasingly complex cyber-physical systems and robots, and progress in data processing and human machine interfaces. The cyber-security can appear almost everywhere in this sub-item of ICT.

There is one specific group, namely “ICT 32 – 2014: Cyber-security, Trustworthy ICT”, which focuses on the security issues. The challenge is to find solutions guaranteeing end-to-end security that withstands progress for the lifespan of the application it supports, regardless of improvements in attacker hardware or computational capabilities.

The concentrations on Research & Innovation Actions as below:

- Security-by-design for end-to-end security: providing end-to-end security, across all hardware and software layers of an ICT system and application and business services. Automated security policy governance for such environments has to be addressed, allowing for run-time verification, customisation and enforcement between operators or virtual entities, in multi-layer and multi-service systems, spanning multiple domains or jurisdictions.

- Cryptography: address the key challenges to guarantee the security for the lifespan of the application it supports, to stay ahead of the evolution of the ICT environment and keep pace with the performance increase of ICT technology.

- Activities supporting the Cryptography Community: To complement the research activities in cryptography support and coordination actions should address the following aspects.

The prioritized projects have to demonstrate a net increase in performance, or reduction in energy or power consumption, compared to state-of-the-art approaches and have to validate
the proposed technology in realistic application scenarios, taking into account the current trends in ICT like cloud, mobile, IoT, etc. Activities may include methods for provable security against physical attacks, as well as research toward security certification.

4.4 International Joint Collaborations

The H2020 – EUB – 2015, namely “EU-Brazil Research and Development Cooperation in Advanced Cyber Infrastructure” within EU and Brazil cooperation in ICT is a major element for the implementation of EU-Brazil cooperation in the area of future networks and e-infrastructures. There are 3 topics in this joint collaboration as below:

- EUB 1 – 2015 “Cloud Computing, including security aspects”: this focuses on the joint research in the development of innovative technologies combining advanced Clouds and Big Data approaches to address the challenges stemming from different application domains in business and societal contexts.

- EUB 2 – 2015 “High Performance Computing (HPC)”: the priorities focus on the security aspects of all application work of HPC on societal challenges and in areas such as transport, energy, environment, climate, health and bio-sciences, prediction and simulation of natural disasters, disaster prevention and crisis management, urban development etc.

- EUB 3 – 2015 “Experimental Platforms”: the security related to the current tools and platforms in support of end-to-end experimentation, creating a pool of, and giving open access to, shared experimental resources.

The other noticeable joint collaborations, namely “EU-Japan Research and Development Cooperation in Net Futures”, identified by H2020 – EUJ – 2014, also mention a lot of cybersecurity issues. There are 4 following topics which contain the security issues are set as top priorities:

- EUJ 1 – 2014 “Technologies combining big data, internet of things in the cloud”: the joint research on the specific challenge in Big Data, Internet of Things. Information gathering, processing and computing of massive amounts of data generated from and delivered to highly distributed devices (e.g. sensors and actuators) creates new challenges, especially for services and data hosted and executed across borders.

- EUJ 2 – 2014 “Optical communications”: the research activity focuses on technologies of optical communication networks and allow coping with the expected significant traffic growth and meet the flexibility requirements imposed by major trends in the evolution of network usage.

- EUJ 3 – 2014 “Access networks for densely located users”: the topic focus on technologies and system approaches to realize high speed/high capacity dense local networks, as may be encountered in very high density locations where many users use high-capacity broadband applications.

- EUJ 4 – 2014 “Experimentation and development on federated Japan – EU testbeds”: Connecting, federating and sharing experimental platforms created Smart ICT in order to carry-out global large-scale experimentations. Enhancing the federation of existing Internet of Things, Smart ICT, etc.
4.5 Nanotechnologies, Advanced Materials, Advanced Manufacturing and Processing, and Biotechnology (FoF)

The section focuses on security aspects about nanotechnologies, advanced materials, production and support actions. This also mention about secured applications in specific societal challenges or focus areas as well as safety, outreach, structuring, business models and other innovation issues. Researches prioritize the scalable real-time architectures to master complexity and data security of the supply network and underlying logistics resources.

The Research & Innovation Actions also support for open standards targeting security and interoperability of shared engineering data. The aim to focus on integrated knowledge-based systems covering the complete product life-cycle with advanced analytics, smart decision support systems and self-learning capabilities exploiting the availability of "big data" from smart sensors, historical process files, or human-authored data. The aim also focus on the addressing the aspects of interactivity, real-time, data-fusion, imprecise computing, compressed sensing, advanced visualisation, security and privacy.

4.6 Innovation in SMEs (INNOSUP)

In the sub-item of “INNOSUP 6 – 2015: Capitalising the full potential of online-collaboration for SME innovation support”, there is obviously the security issues for online application and services. In this sub item, the online collaboration suggests that the training modules are established as web-based self- or collaborative learning modules that are supported by case studies in the form of videos. The qualification profiles and training modules shall be published under a creative commons license.

Projects proposing new service designs for “assistance to online collaboration for innovation” should indicate on which platform the new service would be tested and in how far the newly developed service could be scaled-up, in addition with how to protect the cyber threats toward the online collaboration. It is important to ensure security for assistance all online collaboration for innovation for SMEs.

In the sub-item of “INSO-9-2015 Innovative mobile e-government applications by SMEs”, there are also the security issues for e-government applications and services. In the sub-item of “INSO-10-2015 SME business model innovation”, there are also the security issues for innovation activities related to ICT provided by SMEs.

4.7 Societal Challenges - Secure, Clean and Efficient Energy (LCE)

In this section, the sub-item of “EE 11 – 2014/2015- New ICT-based solutions for energy efficiency” provides some smart application to save energy based on ICT equipment and services. The security issues related to ICT applications is absolutely the important issues. In order to motivate and support citizen's behavioural change to achieve greater energy efficiency taking advantage of ICT while ensuring energy savings from this new ICT-enabled solutions are greater than the cost for the provision of the services. In this sub-item, the focus is on the creation of innovative IT ecosystems that would develop services and applications making use of information generated by energy consumers or captured from sensors and micro-generation. These applications range from Apps for smart phones and tablets to serious games to empower consumers stimulate collaboration and enable full participation in the market.
In addition, in the section of modernising the European electricity grid, at the sub-item of “LCE 23 – 2015: Supporting the community in deploying a common framework for measuring the energy and environmental efficiency of the ICT-sector”, the ICT application comprises a lot of security challenges. The development of framework of metrics, methodologies and best practices in measuring the energy and environmental efficiency of the ICT-sector accompany with cyber threats. The community (particularly by smaller organisations, notably SMEs) of the above framework, the appropriate liaisons will be established with the relevant bodies that developed the above framework to ensure the availability of the relevant expertise when needed. Thus, the security issues will include (but will not be limited to) those of data centres, networks and security issues.

In the section of “Smart cities and communities”, the challenge of deploying solutions related to the energy, transport and ICT sectors, including those which are at the intersection of these three sectors, in an urban environment is to overcome the local specificities. In which, the sub-item, namely “SCC 1 – 2014/2015: Smart Cities and Communities solutions integrating energy, transport, ICT sectors through lighthouse (large scale demonstration - first of the kind) projects” provide the EU policy and regulatory framework in the sectors of energy, transport and ICT supports the development of sectoral solutions. Thus, the Applications and Communication on Smart Cities and Communities expose on a lot cyber threats what need to research carefully.

4.8 Smart, Green and Integrated Transport (MG)

Located in the Societal Challenges section, the item of “Smart, Green and Integrated Transport” contain several security priorities given in ICT application. In the item of “MG.3.5-2014. Cooperative ITS for safe, congestion-free and sustainable mobility”, ITS (Intelligent Transportation Systems) need a lot of IT application and services in order to solving problems related to congestion, traffic safety and environmental challenges if people, vehicles, infrastructure and businesses were connected into one cooperative ecosystem combining integrated traffic and transport management with new elements of ubiquitous data collection and system self-management. Thus, it copes up with the cyber threats and security issues. The applications of ICT have to propose robust built-in data privacy and security measures based on appropriate public engagement in the project.

Also in the item of “MG.3.6-2015. Safe and connected automation in road transport”, the automated and progressively autonomous driving applications in road transport, actively interacting with their intelligent environment could provide a lot of useful applications and also rise lots of cyber-security issues.

In the item of “MG.7.1-2014. Connectivity and information sharing for intelligent mobility”, the aims are to come up with new, efficient, affordable, safe, secure and accessible solutions taking advantage of the ever growing connectivity of people and objects, the availability and the advances in cloud computing, big, linked and open data and the propagation of Internet and social media. Indeed, ‘Big Data’ management (availability, collection, storage, distribution and use) will progressively become a major challenge in intelligent transport communications as will the wider issues related to data ownership, user acceptance and privacy concerns. In parallel, the application based on ICT toward connectivity and information sharing for intelligent mobility will lead to a lot of cyber-security issues.
4.9 Climate Action, Environment, Resource Efficiency and Raw Materials (SC)

In the item of “WASTE-1-2014: Moving towards a circular economy through industrial symbiosis”, there are a lot of ICT applications about systemic and cost-effective solutions which will benefit from innovative ICT solutions for waste traceability, waste material flow management, and the estimation of the availability, composition and quality of waste. Therefore, they push the ICT applications toward much cyber-security threats.

In addition, the item of “WATER-1-2014/2015: Bridging the gap: from innovative water solutions to market replication”, the potential of ICT by developing and deploying advanced ICT solutions for water resources management in agriculture and/or urban areas are exposed by cyber threats.

At the strategy of EU near-zero waste stakeholder platform, the roadmaps addressing specific waste streams, including the electronic waste coming from the ICT sector, should be developed. They define some areas of waste technologies to be clustered, and proposing actions for strengthening links between research funding programmes across the EU.

4.10 Secure societies – Protecting Freedom and Security of Europe and its Citizens (DSR)

In the section of “Secure societies – Protecting freedom and security of Europe and its citizens”, there are a lot of cyber-security issues. In the item, namely “FCT-1-2015: Forensics topic 1: Tools and infrastructure for the extraction, fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation”, the aim is to provide solutions at and beyond the state-of-the-art in the areas of intelligent use and management of complex and large amount of data for the discovery of correlated evidences to support forensic investigation on one hand and for the operational and situational awareness of law enforcement agencies on the other. Thus, the cyber-security are exposed frequently to get resolved.

In the item of “FCT-3-2015: Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials”, the “mobile, remotely controlled” characteristics of the technologies should be developed to enable the assessment of hazardous scenes.

4.11 Digital Security: Cyber-security, Privacy and Trust (DS)

In the Call of H2020-DS-2014/2015, the European Strategy for Cyber-security highlights a set of actions to promote a single market for cyber-security products and fostering R&D investments. The EU see the Cyber-security as a multi-faceted issue, involving critical economic and civilian stakes; cyber-crime; defence; fundamental rights protection; norms of behaviour.

This item is as a call of EU to focus on demonstrating and promoting the viability and maturity of security, privacy and trust solutions. The intention is to find the security concepts, processes and solutions work in a real life environment, in large scale demonstrators and directly involving end users who would ultimately benefit the most from
the outcome, should increase the prospects for an ICT security market and demonstrate the validity and effectiveness of security. These results in turn will reduce the risks of a negative economic impact due to a cyber-incident. Securing and increasing the trust in the digital society are the EU’s central concern. It entails preventing cyber-attacks on any component of the digital society (networks, access devices, IT services...).

4.12 Digital Security Policy

Regarding the EU digital security policies, the EU prioritizes 7 following topics:

- **DS-1-2014: Privacy**: promote solutions to protect individuals’ privacy by default while empowering the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving them control over how their data will be used by service providers.

- **DS-2-2014: Access Control**: development and testing of usable, economic and privacy preserving access control platforms based on the use of biometrics, smart cards, or other devices.

- **DS-3-2015: The role of ICT in Critical Infrastructure Protection**: the malfunctioning or disruption of the communication channel or of an IT system will have a cascading effect, on several other infrastructures or services that depend on it.

- **DS-4-2015: Information driven Cyber-security Management**: encourage the tools and techniques should leverage the state-of-the-art in areas such as SIEM, data analytics (including Big Data) and visualisation, threat intelligence, malware analysis and cyber-security information exchange.

- **DS-5-2015: Trust e-Services**: prioritize the implementation of trust e-Services in specific applications areas like health, public administration, e-Commerce includes the provision of electronic signatures, e-seals, timestamps or certified electronic delivery.

- **DS-6-2014: Risk management and assurance models**: the focus is to assess, manage, reduce, mitigate and accept risk is paramount for an effective protections against cyber-security threats and incidents.

- **DS-7-2015: Value-sensitive technological innovation in Cyber-security**: encourage the new and innovative cyber-security technologies are designed to incorporate European values and fundamental rights.

In fact, EU sees digital security as an issue cutting across all ICT technology, components, applications or services. Further research is thus needed to address these more fundamental and ubiquitous questions.

At a consumer and business level, SEA countries are some of the most dangerous places to be online, and in some cases lack well-developed law enforcement capacity to respond to this challenge [19]. As this is an area where Europe at the administrative level and member states largely excel, there is an opportunity to provide European expertise in knowledge transfer, training, and commercial sales of technologies to improve this situation in SEA; an opportunity that other regional powers are seeking to capitalise on [20]. Given the international nature of the Internet and its lack of respect for borders, improving regional LEA and corporate readiness provides benefits beyond the country of implementation,
benefitting European citizens and the economy by decreasing overall levels of cyber-crime [21]. In addition, further cooperation between states in Europe and ASEAN is required to build understanding of how best to react to the cyber threat to nation states [22], including their respective national critical infrastructure.

In Thailand, the government have identified four key strategies including optimising infrastructure, nurturing vibrant business, development smart government, and capitalising on ICT human resources [23]. In Vietnam and other ASEAN nations, similar efforts are underway to develop e-Government systems [24]. Given that trustworthiness is seen as a contributing factor towards positive citizen engagement with e-Government systems, there is scope for productive collaboration between projects under DS-5-2015 and ASEAN nations.

Europe is in a leading position of supporting fundamental privacy rights in the digital age and ensuring the provision of uncensored access to the Internet [25, 26]. In light of this, and the legal frameworks in place in some South East Asian countries [27, 28], particularly where this affects rights to free speech, it is important for European partners to consider the goals of DS-7-2015 when engaging in research with international partners and governments. Conversely, SEA partners should be aware of the ethical constraints placed on European organisations.

Regarding the Digital Security call the new 2016-2017 Work Programme includes the following topics. The name of the call is “Digital Security Focus Area H2020-DS-2016-2017” and the specific topics include:

- “DS-02-2016: Cyber Security for SMEs, local public administration and Individuals”
- “DS-03-2016: Increasing digital security of health related data on a systemic level”
- “DS-04-2016: Economics of Cybersecurity”
- “DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation”
- “DS-06-2017: Cryptography”

The call is also open to international collaborations like the “Support the EU-Japan ICT dialogue in the area of cybersecurity”, and “encourage and facilitate an exchange of views between the relevant EU and the US stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges; identify and map the relevant legislation and policies in place stimulating the innovation and deployment of cybersecurity solutions.”
4.13 The Work Program 2016 - 2017 on Leadership in Enabling and Industrial Technologies Information and Communication Technologies

In this Work Program, there is an important item about cyber-security, namely “Digital Security Focus Area Call”. In which, there are 2 focuses as “DS1 – 2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components” and “DS2 – 2017: Cryptography”.

In the item of “DS1 – 2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components”, the work program stated that it should concentrate on the solutions to assert the one ICT systems are secure and trustworthy by design and have certified levels of assurance in security. It also has accompanies with the research on architectures and methods to improve efficiency of assurance in parallel with lower the costs for communities. In the draft, there are several priorities in these fields as: Security requirements specification and formalization; Security properties formal verification and proofs at design and runtime; Secure software coding; Assurance - aware modular or distributed architecting and algorithmic; Software code review, static and dynamic security testing; Automated tools for system validation and testing; Attack and threat modelling; Vulnerability analysis; Vendor (third-party) application security testing; Penetration testing; Collection and management of evidence for assessing security and trustworthiness; Operational assurance, verification and security policy enforcement; Adaptive security by design and during operation. Regarding the innovation actions of security certification, the work program prioritize the proposals which should address the challenge of improving the effectiveness and efficiency of existing security certification processes for state-of-the-art ICT components and products including the production and delivery of the corresponding guidance materials. The proposal also proof their effectiveness and address the emerging threats, compositional certification and reuse of components in the context of certified systems and certification throughout the operational deployment of a product or a service.

In the item of “DS2 – 2017: Cryptography”, the work program prioritize the proposals which mention into some topics as: functional encryption solutions to process encrypted data on the Internet. The proposals should aim to deal with measurement of information leaked when allowing for flexibility and preserving data formats; ultra-lightweight cryptology, ultra-high-speed cryptographic algorithms with parallelizable and energy efficient, such as quantum cryptography; development of toolkits that integrate encryption seamless, physical cryptanalysis, including tampering, side channel, faults injection attacks taken into account in the early phases of a development of hardware or software; authenticated encrypted token research for mobile payment solutions and related applications; innovative cryptographic primitives and complementary non–cryptographic privacy preserving mechanisms to enforce privacy at various levels; new techniques, such as quantum cryptography, which are secure from quantum computers and other advances in computing and cryptanalysis; automated proof techniques for cryptographic protocols.

In addition with those 2 above items, there are some other fields of ICT in the work programme of 2016-2017, which have direct aspects relating to cyber-security, such as cloud computing, big data, media and content convergence, future Internet and 5G infrastructures,... The research and innovation in these fields in terms of cyber-security are also important areas for cooperation between ASEAN and EU in next 2 years of 2016-2017.

The 2016-2017 Work Programme has some new calls that request proposals where the cyber security dimension should be also addressed. That call is the “Science with and for Society” and its “aim is to build effective cooperation between science and society, to recruit new talent for science and to pair scientific excellence with social awareness and responsibility”.

Below someone can find the relevant topics of the call:

“SwafS-22-2017: The ethical dimensions of IT technologies: a European perspective focusing on security and human rights aspects”. The topic seems to request research on topics where an enormous personal data are gathered from many sources thus raising the issues of security and privacy (“This raises multidimensional questions related to how to effectively implement the Charter of Fundamental Rights in our e-society while balancing the interest of all socio-economic stakeholders, promoting innovation, enabling high quality job creation and ensuring a high level of privacy and cyber security.”)

It is also mentioned in the scope of the topic that the work undertaken shall analyse (among others) “the existing and future possible ethical tensions between the technological evolution in the ICT field and the protection of human rights, in particular as regards privacy and personal data. Such analysis shall take into account the increasing number and unprecedented intensity of threats to public and private cyber security and the responses given by the competent international, European and national bodies”.

4.15 New in 2016-2017: Cross-cutting activities (Focus Areas)

Another new call in the 2016-2017 Work Programme is the “Cross-cutting activities (Focus Areas)”. This call includes IoT topics which are summarized below:

The “IoT-01-2016: Large Scale Pilots” topic which is interested in “the validation of user acceptability by addressing, in particular, issues of trust, attention, security and privacy through pre-defined privacy and security impact assessments, liability, coverage of user needs in the specific real-life scenarios of the pilot”.

The “IoT-02-2016: IoT Horizontal activities” topic that mentions “privacy, security, user acceptance, standardisation, creativity, societal and ethical aspects” as issues of horizontal nature and topics of common interest that need to be addressed within this topic and the pilots implemented in order to maximize the output of the proposal.

The “IoT-03-2017: R&I on IoT integration and platforms” topic through one of its scopes which is named “IoT security and privacy” requests from the proposals “advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. Approaches must be holistic and include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels. They should address relevant security and privacy elements such as confidentiality, user data awareness and control, integrity, resilience and authorisation.”
4.16 STATE-OF-THE-ART OF SECURE ICT LANDSCAPE-NIS PLATFORM

On April 2015 the second version of the state of the art of secure ICT landscape (NIS platform) was published. The first version had been published on 2014. We checked the cybersecurity topics that have been mentioned in the document and we include them in this sections so that someone can compare them with the rest of the H2020 priorities and whether they comply with the ASEAN priorities or not. The document identifies 17 areas of interest related to security. We have included the topics where we think that cybersecurity has been identified in the NIS platform as of high importance. Those topics (in our understanding) are:

- Critical Infrastructure Protection
- Cyber security threat technologies / Offensive technologies
- Energy Grids
- Smart Grids
- Smart Transport / Automotive
- Banking and finance
- Dual Use Technologies
- Food
- Drinking water and water treatment systems
- Cyber security awareness and training
5 European Technology Platforms and Cyber-security Priorities

5.1 ARTEMIS Industry Association\(^3\)

5.1.1 ARTEMIS High Level Vision 2030

One of the major findings of the ARTEMIS ETP that has been included in the produced publications is related to security and cyber-security. In the “High Level Vision 2030\(^4\)” document produced 7 items have been identified as “megatrends” for the next years. One of those megatrends is the Cyber-security. Key trends of the Cyber-security megatrend include the chip security which is in line with Software by Design calls already included in the HORIZON 2020 Work Programme and network protection in order to strengthen computing and data infrastructures against espionage and terrorism.

![Figure 2: Megatrends and key trends in cyber-security](image)

Other areas that have been identified Cyber-security as critical for the future includes:

- Digital Society and Virtualization of communities and societies.
  
  “,Security and safety, privacy and identity theft are important challenges for all future systems based on Digital Technology”

- Embedded and Cyber-Physical Systems Technology

  “Embedded systems will raise expectations as well as concerns about potential failures and safety, privacy and security so the quality and dependability of embedded systems are key issues. In that context additional protocols and communication structures may be needed to guarantee the required quality of service”

\(^3\)[https://artemis-ia.eu/]
5.1.2 ARTEMIS Strategic Research Agenda

The agenda identifies twenty one (21) “Major challenges for technological research” for the future. Below there is a list of those challenges and we have highlighted those that address the security aspect as important

1. Embedded System architecture
2. Systems design
3. Validation
4. Design for safety
   • “Security aspects of safety-relevant Embedded Systems (e.g., protection of temporal properties of hard real-time systems, timing effects of security mechanisms)
   • Platform technologies for safety-relevant embedded systems: communication services, diagnostic services, robustness services, security services) as a stable baseline for the development of safety relevant embedded applications”

5. Dependability

Security is identified as major category of the Dependability challenge. The breakdown of the security challenge is then analyzed in seven (7) sub-categories that are of high importance for the agenda including:

• “interoperability between trusted and non-trusted environments
• tamper-proof and tamper-resistant technologies from physical to software
• enhanced technologies for fault adaptation, tolerance and recovery
• flexibility and scalability to execute multiple and diverse security protocols
• reliable operation despite attacks from intelligent adversaries who intentionally search for undesirable failure modes;
• seamless and secure interactions and cooperation of Embedded Systems over heterogeneous communication infrastructures, essential to implement the future concepts of the ‘internet of things’
• Intrusion-proof architectures, allowing secure upgradeability, trusted dependable, reliable/resilient security/privacy evaluation (composable security and dependability).”

6. Communication
7. Silicon scaling
8. Heterogeneous parallel systems
9. Sensors and actuators
10. Smart environments and systems
11. Man-Machine interfaces

12. Distributed computing platform
13. Self-organising and Autonomous systems
14. Systems of systems
15. Certification
16. Resource management
17. Energy and power
18. Interoperability
19. Tool integration
20. Cloud computing
   • “A well-managed ‘Cloud’ promises computational services comparable to PC at a fraction of its cost. The division of work between a smart object and the cloud will be determined by the privacy and the energy considerations as well as aspects related to information security, autonomy, response time, reliability and cost”
21. From syntactic to semantic interoperability

5.2 ENIAC Joint Undertaking

“The ENIAC Joint Undertaking (JU) is a public-private partnership focusing on nanoelectronics that brings together ENIAC Member/Associated States, the European Commission, and AENEAS (an association representing European R&D actors in this field).”

5.2.1 ENIAC Annual Work Programme 2013

The Work Programme of the ENIAC ETP identifies eight (8) innovation priorities for 2013. Many of them highlight the aspect of security as part of their innovation success and we will mention here some of them. The 8 innovation priorities and their grand challenges are:

1. Automotive and Transport
   a. Intelligent Electric Vehicle
   b. Safety in traffic
   c. Co-operative Traffic Management

Expected Achievement/Description

“New innovative concepts and prototypes of co-operative traffic management interacting with systems in other application domains like Internet or logistics are expected”

High Priority Research Areas
   o intelligent electronics for security and privacy protection

---

6http://www.eniac.eu
2. Communications & Digital Lifestyles
   a. Internet Multimedia Services
   b. Evolution to a Digital Lifestyle
   c. Self-Organizing Network
   d. Short range convergence

3. Energy Efficiency
   a. Sustainable and Efficient Energy Generation
   b. Energy Distribution and Management - Smart Grid
      Expected Achievement/Description
      “To effectively measure and communicate energy consumption in buildings, cities and districts, user profiles or future needs, dedicated sensors and communication networks have to be developed.”

High Priority Research Areas
   “The smart energy grid will only work smartly, if it is not only a power-network, but at the same time a communication network, which contains security features, grid monitoring and payment features”
   c. Reduction of Energy Consumption

4. Health and the Ageing Society
   a. Home Healthcare
   b. Hospital Healthcare
   c. Heuristic Healthcare

5. Safety & Security
   a. Consumer and Citizens Security
      Expected Achievement/Description
      “Considering the growing demand for mobile connectivity, identity and data protection of citizens, health & transport services, e-banking & e-government and moreover for global security as a whole.”

High Priority Research Areas
   o “Communication technologies: Secure spontaneous networking, Security of wireless protocols (IEEE 802.X,...UWB, RFID,...), Trust and integrity
   o Secure servers and personal devices: Multi-level security, Trusted virtualization and compartmented operation systems, Privacy-enabled Trusted Personal Devices (Fixed, mobile), Integrated trust and security hardware and firmware features for embedded computing platforms
   o Smart-sensors and actuators: Integrated authentication against fraud,
   o Privacy-enabling technologies: Anonymization, P3P (Platform for Privacy preferences..), Digital signatures”
b. Securing the European Challenging Applications

Expected Achievement/Description

“In all new fields of application, electronic control and data exchange show an obvious need for more security.”

High Priority Research Areas

o “Energy Efficiency and smart energy grids

Liked with that customer usage profile data collection, distribution and usage has to be severely protected in order to protect privacy, avoid massive fraud. Remote control by users or by the overall management systems has to show resilience to many threats or associated risks covering security (wrong access, billing fraud…) but also safety (people at risk if home equipment are incorrectly driven either by fraud or failure.

o Health & Ageing Society

When life sustaining equipment is to be used control (local or remote) of such equipment will be highly critical and the highest level of security has to be achieved

o Automotive & Transport

o Communication

A new security paradigm is requested by more and more communicating applications, more mobile users and more distributed data. Thus securing services or data and providing proper protection evidences is becoming increasingly important and difficult in advanced, open wireless and fully mobile devices

o Other leading applications

Other new applications for trusted Future Internet, new e-Payment, e-ID … are also developed at European level. Security is a core technology for these applications.

c. Enabling Technologies for Trust, Security and Safety

Expected Achievement/Description

Security and Safety being generalized in any applications, a methodology for integrating basic security bricks in more complex systems (microsystems such as SoC or macrosystems) with capabilities of proof, early validation, simulation, etc has to be developed; Secure by Design approaches are generic terms for these developments.

High Priority Research Areas

o Embedded Sensors technologies for security and safety

o Secure new high data rate interfaces for MtoM and RFID

6. Design Technologies

a. Managing Complexity
b. Managing Diversity

c. Design for Reliability and Yield

7. Semiconductor Process and Integration
   a. Know-how on Advanced and Emerging Semiconductor Processes
   b. Competitiveness through Semiconductor Process Differentiation
   c. Opportunities in System in Package

8. Equipment, Materials and Manufacturing
   a. Advanced CMOS - 1Xnm & 450mm
   b. More than Moore
   c. Manufacturing”

5.3 EPoSS: ETP on Smart Systems Integration

“EPoSS is an industry-driven policy initiative, defining R&D and innovation needs as well as policy requirements related to Smart Systems Integration and integrated Micro and Nanosystems. EPoSS is contributing to EUROPE 2020, the EU’s growth strategy for the coming decade, to become a smart, sustainable and inclusive economy”

5.3.1 EPoSS Strategic Research Agenda

The EPoSS Strategic Research Agenda has identified six (6) large domains as important for future ICT. Some of them include security related features. We have extracted those domains:

1. Bio-based Economy
   N/A for security

2. Energy
   “It must be emphasized the role that smart grids can play in increasing electricity reliability: adequacy and security.

   • It is not feasible to accommodate significant embedded renewable and micro-generation on the network and maintain system security without moving towards a more dynamic approach to network operations

   • Cyber-security must be considered as part of a larger smart grid deployment strategy

3. Environment
   N/A for security

4. Information and Communications Technologies

http://www.smart-systems-integration.org

The main benefit of Smart Systems for communications identified in the EPoSS SRA is that they act as key enablers to improve the quality of life for citizens through: Secure access to various services in different domains (digital economy, health systems, sustained energy and the protection of the environment, security and safety, life at home, in the cities, and in transportation systems).

5. Production and processes

Humanoid and animal-like robots: Robotics, emphasizing mechatronics, human assistance, cognition, and security, will target automotive companies, rehabilitation/hospital structures, electronics and hardware companies.

6. Transport

Management and control systems addressing safety and security, equipment health monitoring, automated or self-assessed operation, and vehicle-infrastructure interaction”

5.4 ETP4HPC: ETP for High Performance Computing

“An industry-led initiative, a European Technology Platform (ETP) for High Performance Computing, is being formed to address these issues. This ETP will define research priorities for the development of a globally competitive HPC technology ecosystem in Europe. It will propose and help to implement a Strategic Research Agenda, while acting as the “one voice” of the European HPC industry in relations with the European Commission and national authorities. The creation of this ETP fits perfectly with a European Commission’s recommendation made in its recent communication about HPC.”

5.4.1 ETP4HPC Strategic Research Agenda

Technical Research Priorities of the ETP4HPC SRA include the following:

1. HPC System Architecture and Components
2. System Software and Management
   “System security aspect has been addressed and they have defined a related milestone (M-SYS-OS-3: System security management). Research topics identified include System security” and “System management which will also have to ensure system integrity, with system security being a major factor”.

3. Programming Environment
4. Energy and Resiliency
5. Balance Compute, I/O and Storage Performance
6. Big Data and HPC Usage Models
   Security is also addressed in this priority which has been included in the research agenda. “Issues such as data integration, data security and privacy will have to be
integrated with the underlying HPC computations”. The need for privacy has been also addressed through the following statement “HPC resources need to adopt high security standards as non-scientific, i.e., social and private data is handled.”

5.5 EU Robotics AISBL

“EuRobotics aims to promote excellence in robotics by providing many networking opportunities to its members from both industry and academia, to exchange knowledge within the robotics community and to shape the future of robotics in Europe through cooperation between all sides”

5.5.1 EU Robotics Strategic Research Agenda

In the EU Robotics SRA robots have been categorized through the End User Market domain that those robotics may be used. Those domains include the following and some of them claim that they need some security related features to be properly considered.

1. Agriculture
2. Civil Robots

“This high level domain covers the use of robots within government and public agencies (B2G) for example, civil infrastructure, search and rescue, environment, law enforcement, emergency services, and science support. These application areas are typically managed by civil authorities and the robot systems would be operated by regional and national services or by contractors engaged to do so. They will be operated by trained personnel and may be operating in hazardous or extreme environments where people may be at risk. Applications in this high level domain range from the monitoring and maintenance of water, sewerage, and gas pipelines; electricity networks, rivers and harbors to emergency disaster recovery and civil security applications.”

3. Commercial Robots
4. Logistics and Transport
5. Consumer Robots

“Applications range from helping the elderly stay safely mobile in their own homes to the automation of every day household chores and the provision of remote monitoring and security for the home”

6. Military Robots

5.6 NEM: New European Media

“Intention of NEM Vision documents is to present the vision statement of the Networked and Electronic Media (NEM) Initiative, which includes the key challenges that the NEM sector will have to face in the long-term. The description of the NEM picture today and the
vision from industry for the future is based on the input from stakeholders of the NEM field, including broadcasters, telecom operators, manufacturers of professional equipment, and manufacturers of consumer electronics, academia, and standardisation bodies. Current version of the vision document presents the long-term statement of the NEM Initiative and expected developments in the NEM area for the time-period 2010 – 2020”

5.6.1 NEM Strategic Research Agenda

NEM Strategic Research Agenda has identified some topics of high importance in H2020 Work Programme 2016-2017. Those topics include:

1. Media-related applications and business models
   a. Social Networking and Media Sharing
   b. User Satisfaction and Quality of Experience
2. Content Creation
   a. New Forms of Content
   b. Representation of Content
   c. Tools for content creation and manipulation
3. Networking and delivery infrastructure
   a. Intelligent Delivery
4. Content search and media presentation
   a. User-system interaction
   b. Authentic, true-to-original media reproduction including Virtual Reality
5. Technology drivers and enabling technologies
   a. Data security and personal privacy
   b. Identity management and AAA (authentication, authorization and accounting)
   c. Personalization/profiling: Smart user profiles across all services & devices
   d. Power management technologies – energy saving in/by ICT
   e. Machine-Machine Communication

Some of them address the need of security and privacy of the created and stored content (e.g. “Data security and personal privacy”) but many of those topics present security related issues like other domains of other ETPs due to the fact that they make use of modern networking infrastructures.

NESSI: The Networked European Software and Services Initiative

“NESSI, the Networked European Software and Services Initiative, provides input to the EU Institutions on research actions and technology matters of particular importance to the software domain, and the overall aim is to enable the software and services sector help vitalize the great potential of the European economy and society.”

NESSI Strategic Research Agenda

The recent Strategic Research agenda of the NESSI platform has focused on the following areas:

1. Quality in cloud-based heterogeneous service scenarios
   
   Objective: “Investigate Service Level Agreement (SLA) handling, resource management, and service development mechanisms, methods and tools to improve the quality offered by heterogeneous cloud infrastructures in support of complex and mission-critical cloud-based service setups”
   
   Expected Impact: “Resolving most critical issues around quality, security and compliance will help to increase exploitation of cloud services in Europe and thus will contribute to the growth of the European cloud market;”

2. Services benefiting from Programmable Networks

3. Service usage in a fast changing business world

4. Collaborative Service Engineering based on convergence of software and data

5. New ways to increase software performance and energy-efficiency
   
   Objective: “Develop method and tools to make it easier to get an overview of the performance and scalability of complex systems, so that performance and scalability refinement can be targeted at the weak spots and not on the whole system – this will balance development costs and other non-functional requirements like security on the one hand and performance, scalability and energy efficiency on the other hand”

6. Integration of Big Data Analytics into Business processes
   
   Objective: “There are several open issues regarding the analysis of Big Data, from data acquisition and filtering, validation, privacy and security, near-real-time analysis, analytics on mobile devices, and database design for the facilitation of the analysis”
   
   Expected Impact: “More effective public services and control mechanisms by making use of Big Data, in areas such as fraud detection and prevention, tax collection, economic forecasts and policy, monitoring of healthcare spending, security and threat identification, etc”

7. Trust and security for global digital infrastructures and services

16http://www.nessi-europe.eu

17http://www.nessi-europe.com/Files/Private/NESSI_SRIA_Final.pdf
Objective: “Prepare the new generation of trust and security mechanisms and solutions capable of taking up the challenges brought about by the future evolution of current technology trends such as Cloud Computing, Big Data, IoT and their gradual convergence”.

Expected Impact: “Mitigated impact of security threats for European citizens and businesses through improved awareness and understanding of existing and future solutions as well as easy-to-use and standardized tools” and “Strengthened European cyber-security sector leading global understanding and handling of new security challenges imposed by the development and convergence of Cloud Computing, Big Data and IoT”.

5.8 Networld2020 ETP

“NetWorld2020 is the European Technology Platform for communications networks and services. Communications networks enable interaction between users of various types of equipment, either mobile or fixed; they are the foundation of the Internet. The NetWorld2020 European Technology Platform gathers players of the communications networks sector: industry leaders, innovative SMEs, and leading academic institutions.”

5.8.1 Networld2020 Strategic Research Agenda

The Networld2020 ETP identifies in its Strategic Research Agenda the following research priorities. All of them mention the security as a prerequisite characteristic that should be fulfilled in order for those priorities to succeed.

1. Converged Connectivity

   “Security is a crosscutting topic that needs to be carefully considered by design from the start. Secure mechanisms must be developed that allows access to only authorized parties (both in human form or through agents) in creating/configuring a virtual network. It must be flexible enough to accommodate the increased and multi-dimensional dynamics introduced by fine-grained virtualization. Additionally, isolation between virtualized networks has to be guaranteed as well as providing trust for the virtual infrastructure users on the virtual service enablement”

2. Wireless Subsystem

   “An explicit (striving to be implicit) consideration for security and resilience, considering all aspects of availability, confidentiality and integrity”

3. Virtualization

   “Sharing common physical infrastructures creates security concerns that have to be addressed to ensure isolation among virtual resources and services”

Especially for the future 5G networks they also identify three major challenges including privacy and/or security as important points of those challenges.

18http://networld2020.eu
Privacy by design challenge:

“Provide accountability within the communication substrate and enable truly private communication when needed, aligned with policy constraints in terms of data management and ownership, ensured by the infrastructure operators that realize the overall service”

Quality of Service challenge:

“In order to allow for optimizing the Quality of Experience (QoE) for the end user, 5G should provide differentiated services across various dimensions such as through put, latency, resilience, availability and costs per bit as much as possible independent of users’ location with respect to the antennas deployment geography. This includes increased security, availability, resilience and delivery assurance for mission critical applications such as health-related or emergency applications, but also ultra-low cost solutions for emerging countries with less stringent QoE requirements”

Resource management challenge:

“Provide access agnostic control, policy and charging mechanisms and protocols for dynamic establishment, configuration, reconfiguration and release of any type of resource (Bandwidth, Computation, Memory, Storage), for any type of devices (e.g. terminal, car, robot, drone, etc.) and services (e.g. Network, Security, Data, Knowledge, Machine, and Thing as eService), including in end-to-end (E2E) fashion when necessary”
6 Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace

In 2013, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued the EU’s vision and the actions to cope up with the cyber-security, namely “Europe’s Cyber-security Priorities Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace”. In this strategy, the EU’s vision and actions also mention about the R&D priorities and the international cooperation with other countries and organization, such as ASEAN.

6.1 R&D Priorities in the Cyber-security Strategy

In the strategy of “Europe’s Cyber-security Priorities Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace”, the EU’s strategy is offering some R&D priorities for the EU’s activities in cyber-security as below:

- **Identifying the NIS (Network and Information Security) vulnerabilities**: the EU Commission promote activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.

- **Promoting a single market for cyber-security products**: promote the production of the ICT devices which are satisfied the EU standards about security. The EU launched a public-private platform on NIS solutions to develop incentives for the adoption of secure ICT solutions and the take-up of good cyber-security performance to be applied to ICT products used in Europe. The ICT products, hardware and software are used in critical services, infrastructure and mobile devices must be trustworthy, secure and guarantee the protection of personal data.

- **Fostering R&D investments and innovation**: in this regards, the EU aims to make the best of the Horizon 2020 Framework Programme for Research and Innovation. The priorities try to support security research related to emerging ICT technologies, provide solutions for end-to-end secure ICT systems and develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.

- **Supporting the development of cryptography**: the strategy aim to not only crate next generation of cryptography, but also translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

- **Provision of advanced solutions for end-to-end secure ICT systems**: the strategy aim to provide solutions for end-to-end architecture and highly secure ICT systems, services and applications; EU’s actions also provide the incentives for the implementation and adoption of existing solutions and address interoperability among network and information systems.
6.2 International Cooperation in the Cyber-security Strategy

In this strategy, the EU's vision and the actions also bring some priorities for the EU's international cooperation in cyber-security, also with ASEAN as below:

- **Promote the international cooperation, develop industrial and technological resources to produce the ICT products**: Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. Thus, the EU encourage the cooperation between Europe and other partners to harmonize the EU standards about security and ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

- **Establish a coherent international cyberspace policy for the European Union and promote EU core values**: EU aims to apply its core values of freedom, openness and fundamental rights in cyberspace. EU asserted the cyberspace is regarded as an area of freedom and fundamental rights. Expanding access to the Internet should promote democratic reform worldwide. The EU believes that increased global connectivity should not be accompanied by censorship or mass surveillance.

- **Promote cooperation on standardization in cyber-security, expanding usages of EU laws, norms and core values**: The EU engages with international partners and organisations, the private sector and civil society to support global capacity-building in third countries. It includes improving access to information and to an open Internet, and preventing cyber threats.

- **Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy**: To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. The EU tends to contribute intensifying the on-going international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and the private sector. EU tries to promote developing the capacity building on cyber-security and resilient information infrastructures in third countries.

Thus, in the “Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace”, EU plans to promote international cooperation with ASEAN and focus on several R&D trends as mentioned above.
7 ASEAN’s Cyber-security Priorities

On the direction toward an ASEAN Community, the ASEAN member states see ICT as a key factor to communicate each other. Therefore, the ASEAN state members approved the “ASEAN ICT Master Plan 2015” which is valid until 2015 and now they are composing the new “ASEAN ICT Master Plan 2020”. In the current Master Plan in force, there is an Initiative numbered at 2.4. Build Trust which is located in Strategic Thrust 2: People Engagement and Empowerment. Within this Initiative, there are 2 actions to promote ICT security among those countries.

- The first action is “Promote secure transactions within ASEAN”. This action describes the activities on development of mutual recognition arrangements for cross-certification of digital certificates within ASEAN. It also mentions about promotion of the use of two-factor authentication.

- The second action is “Outreach campaign to promote awareness of cyber-security”. This action describes 3 descriptions. They are to create public awareness through education about online security; forge joint collaboration with industry and other stakeholders; and to ensure the personal data protection.

Also in the “ASEAN ICT Master Plan 2015”, there is a Strategic Thrust 4: Infrastructure Development. There is a commitment under Initiative 4.2: Promote network integrity and information security, data protection and CERT cooperation. In which, there are 5 actions to promote cyber-security. They are:

- Establish common minimum standards for network security to ensure a level of preparedness and integrity of networks across ASEAN;

- Develop a network security “health screening” programme for ASEAN to be implemented at regular intervals;

- Develop best practice models for business continuity and disaster recovery for all sectors;

- Establish the ASEAN Network Security Action Council (multi-stakeholder) to promote CERT cooperation and sharing of expertise, amongst others;

- Share best practices on the protection of data and information infrastructure across ASEAN.

In the view of steering ICT development over the next five years will greatly impact ASEAN, especially in the lead up to this region becoming an Economic Community, the Cyber-security is an essential issue within the region. In line with the region’s aim to establish an ASEAN Community by 2015, the ASEAN ICT Master plan envisions the creation of a global ICT hub. A cohesive and comprehensive effort to tackle cyber-security issues is a prerequisite for an ASEAN Community and is in the shared interests of ASEAN member states.

7.1 Cyber-security Emergency Readiness

In ASEAN, almost all countries have their own CERT (Computer Emergency Response Team) organization. The active organization in the region are typically MyCERT (Malaysian
Computer Emergency Response Team, ThaiCERT (Thai Computer Emergency Response Team), SingCERT (Singapore Computer Emergency Response Team), VNCERT (Vietnam Computer Emergency Response Team),... In 2012, Lao PDR also established its own National CERT, namely Lao Computer Emergency Response Team (LaoCERT). Other active CERT players are BruCERT (Brunei Computer Emergency Response Team), mmCERT (Myanmar Computer Emergency Response Team),...

In Indonesia, there are 2 organizations, namely ID-CERT (Indonesia Computer Emergency Response Team) and ID-SIRTI/CC (Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center) to cope up with the cyber-security issues.

ASEAN has close cooperation and mechanisms on CERT, the members closely support each other at all action about cyber-security related entity, regardless of the region and organizational structure, which can support and contribute to common CERT operations and functions.

### 7.2 Cyber-security Protection

In addition with cooperation given by CERT, ASEAN also has many mechanisms, dialogues and documents to protect the region against cyber the security. According to report given by ASEAN Secretariat at Octopus Conference on “Cooperation against Cyber-crime” in December 2013 at Strasbourg, France, there are some of them may include:

- ASEAN Ministerial Meeting on Transnational Crime (AMMTC): review work by various ASEAN bodies on transnational crimes - set pace, direction for regional collaboration on combating such crime
- ASEAN Senior Officials Meeting on Transnational Crime (SOMTC): review policy strategies and implementation of its Work Programmes - report the development of their work to AMMTC
- ASEAN Regional Forum (ARF): foster constructive dialogue and consultation on political and security issues of common interest and concern - make significant contributions to efforts towards confidence-building and preventive diplomacy in the Asia-Pacific region
- ASEAN Telecommunications Regulators Council (ATRC): to provide the telecommunications regulators and authorities within the region a platform for cooperation within the mutual interest to the administration of the ASEAN Member States (AMSs), also to identify and promote areas of potential cooperation in telecommunications amongst ASEAN member states (AMSs) and facilitate the exchange of information through work programs.


There are several ATRC Projects with ASEAN Dialogue Partners, such as the Project on Cyber-crime Legislation in ASEAN Member States (2008); ASEAN – EU Training for Law Enforcement, Judges and Prosecutors on Cyber-crime (2011); Annual ASEAN-Japan Network Security Workshop (2009) and annual ASEAN-Japan Information Security Policy Meeting
(since 2008) hosted on rotation basis amongst Japan and ASEAN Member States; Annual ASEAN-China Network Security Seminar (since 2009) in China.

ASEAN aims to strengthen the telecommunication regulations to cover non-commercial and commercial sectors, and to standardize data retention policies for service providers; and develop a clear code of conduct and referral system or inter-agency coordination mechanism in monitoring, reporting and handling cases and victims of cyber pornography and cyber prostitution in ASEAN Member States.

7.3 **Critical Infrastructure Protection**

Regarding infrastructure, the telecommunications and IT sector in ASEAN continue to work collectively to enhance high speed connectivity between the ASEAN Member States. Focus has been placed on improving broadband access, cost effective communications and deployment of advanced ICT infrastructure in the ASEAN region. The local digital content is considered as a driving force for broadband which can help to bridge the digital divide and contribute to a stronger and integrated ASEAN Community. The work aims to deepen and strengthen regional initiatives and activities toward enhancing the enabling infrastructure of an ASEAN information society. The work also stresses the importance of establishing the foundation for ICT applications, services and solutions in the ASEAN region. A wide range of projects have been proposed which focuses, among others, on information infrastructure and e-commerce, ICT accessibility and affordability as well as the use of ICT applications to increase the quality of life of people in the ASEAN region.

ASEAN, in Asia (2015), has an initiative on Critical Information Infrastructure Protection (CNIP)/Cyber-security under the view of the ever increasing threat from cyber-attacks on critical infrastructure and large corporations. In fact, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber-security strategy of an organisation or CNI operator. Cyber-security in Southeast Asia is being given greater attention; however, measures pertaining to cyber-security are found more at national, rather than international level. While one ASEAN CERT does exist (for all AMSs, not each country), it is not entirely effective. Critical Information Infrastructure Protection looks at the potential threats on these fragile systems, from cyber-attack, interoperability of new generation technologies and integration.

ASEAN also has a Master Plan on ASEAN Connectivity which was adopted by the ASEAN Leaders at the 17th ASEAN Summit in 2010. The Master Plan serves to achieve a bold and long-term strategy to improve the region’s physical, institutional and people-to-people connections. The Master Plan on ASEAN Connectivity encompasses the three key elements of: 1. Physical connectivity: Transport; Information and Communications Technology (ICT); and energy; 2. Institutional connectivity: Trade liberalisation and facilitation; investment and services liberalisation and facilitation; mutual recognition agreements/arrangements; regional transport agreements; cross-border procedures; and capacity building programmes. 3. People-to-people connectivity: Education, culture, and tourism.
7.4 Public Security and Safety

The Public Security and Safety are also seen as big issue in ASEAN. There is a specific Forum, namely Senior Officials Meeting on Social Welfare and Development (SOMSWD) within ASEAN to address social risks faced by children, women, the elderly and persons with disabilities. ICT application play key role in those SOMSWD activities.

ASEAN also see ICT as important factor to save Public Security and Safety in the region. Ensuring business continuity is a critical need for cities as numerous recent examples attest. Disasters, whether they are the result of terrorist attacks or natural calamities like earthquakes or tsunamis, have the potential to wreck-havoc on cities, destroying lives, infrastructure and economies. Helping cities anticipate, prepare for, and recover from, disasters is something that ICT application and service can afford to do. Through the ICT application of advanced technologies and solutions, they can offer municipal authorities the ability to minimize the human and economic impact of disasters as well as to facilitate recovery. Disasters, especially, natural disasters, are typically not preventable. Early warning requires gathering data from different sensors to predict incidents such as floods. The ICT systems use various types of seismometers, tsunami sensors, precipitation and water level sensors and surveillance cameras to detect changes in the environment that are preludes to earthquakes and tsunamis.

7.5 ASEAN’s Measures toward Cyber-security

The ASEAN and ARF (ASEAN Regional Forum) Statement on Cooperation in Ensuring Cyber-security (Phnom Penh, 2012) asserted the following measures to intensify regional cooperation on security in the use of information and communication technologies (ICT):

- Promote further consideration of strategies to address threats emerging in this field consistent with international law and its basic principles;
- Promote dialogue on confidence-building, stability, and risk reduction measures to address the implications of ARF participants’ use of ICTs, including exchange of views on the potential use of ICTs in conflict;
- Encourage and enhance cooperation in bringing about culture of cyber-security;
- Develop an ARF work plan on security in the use of ICTs, focused on practical cooperation on confidence building measures, which could set out corresponding goals and a timeframe for their implementation;
- Review a possibility to elaborate common terms and definitions relevant to the sphere of the use of ICTs.

The measures given by ASEAN on human resources in cyber-security are also focusing to resolve the weaknesses of cooperation within the ASEAN region. The creation of a regional hub of cyber-security professionals and experts is among the top priorities in ASEAN. ASEAN aims to develop a workforce with high-level ICT proficiency, member states are trying to develop a pool of cyber-security professionals to effectively respond to regional and international cyber-security challenges. This could be achieved through a range of approaches and programmes including ASEAN cyber-security scholarships. This is similar with those initiatives which proposed under the Mactan Cebu Declaration for the creation of an ASEAN ICT Scholarship programme to attract ICT talent. The education on cyber-security
issues at the earliest possible age as well as incorporation in school curricula is quite important. The further development of “ASEAN Cyber-kids Camp” and initiatives to encourage and attract talent to choose ICT as a career are also effective solutions.
8 Comparative Analysis of EU and ASEAN Cyber-security Priorities

8.1 The Principle and Outcomes of Comparative Matrix

The following matrix has been extracted from many information sources provided by CONNECT2SEA partners. There are 28 matches found in the matrix, which fit at least one of ASEAN countries and fit EU Horizon 2020 ICT Work programme 2014-2015. The matches found are grouped into 3 most important groups, based on the framework of Cyber-security activities defined by ITI-VNU (Information Technology Institute – Vietnam National University). According to ITI-VNU, a framework is necessary and useful for further discussions in streamlining the efforts. Most cyber-security activities can be classified into the following five categories:

- a. Social awareness promotion and information sharing on cyber-security
- b. Standards, reference models and architecture framework of cyber-security
- c. Open platforms for cyber-security
- d. Common actions and knowledge exchanges between EU and ASEAN
- e. New solutions to the urgent issues

Among them, the first 3 groups are the most important. The “Social awareness promotion and information sharing on cyber-security” is the first and most important step to promote social awareness and to share information of cyber-security between individuals, organizations, countries and regions, since the cyber-crimes tend to be repeated and can be prevented only by common efforts. However, unlike other applications the users cannot see the transparent benefits of the cyber-security measures. Sometimes, cyber-security measures need times to be adopted into user’s habits. The cyber-security risks and threats are too sophisticated to be recognized by the users without a basic understanding of their nature. Social awareness promotion and information sharing on Cyber-security should start with events, guidelines documents and later can be implemented as on-line services, training courses and handbooks.

Secondly, the “Cyber-security standards, reference models and architecture framework”, especially the standards are important for the industrial product manufacturers. The reference models are useful for the system integration service providers. The architecture framework is the guideline for the organizations that need the system for their operations. The policy makers play an important role in standardization and in recommending the reference models and architecture framework for the community. International collaboration is very important in these activities, because international standards must be adopted to open the domestic markets for the manufacturers and the experience must be exchanged and reused.

Thirdly, the “Open platforms for cyber-security” is also important. There must be platforms for joint cyber-security actions between the countries. Platforms must be open to make the risks, threats and solutions public, and then to mobilize international resources to address
these challenges. These open platforms should include networks of national and regional CERTs.

In order to design the matrix to find the common activities, this report first clarified in details all 144 activities in EU Horizon 2020 (ICT Work programme 2014-2015) mapped to their previous items in the Horizon 2020 topic (please refer to the appendix at end of this report). These 144 activities are related to cyber-security in some aspects.

Secondly, those 144 activities in EU Horizon 2020 are put in one column and there are other 5 columns for 5 countries (Indonesia, Malaysia, Philippines, Thailand, Vietnam), which sent their report in order to match with activities in EU Horizon 2020 current priorities.

Finally, this report found 28 matches of 144 activities in EU Horizon 2020 fit to at least one of the activities that exist in these 5 countries. Overall, there are 7 matches that satisfy the priorities of all 5 countries and are also priorities in EU Horizon 2020.

The findings of total 28 fields or activities that are good candidate areas for cooperation between EU and SEA countries are:

1. Establishing Centres of Excellence
2. Open, smart and co-operative CPS (cyber-physical systems)
3. Smart systems driven by industrial requirements
4. Establish reference architectures and platforms for customised low-power heterogeneous computing systems
5. Contributions to standards: IETF, IRTF may be targeted
6. Reducing the IT expenditure of the public sector
7. Increasing user perceptions of quality of service, of experience and security
8. Analysis of risks and vulnerabilities in IT system for security managers
9. Improving awareness of new threats, vulnerabilities and risks
10. Security-by-design for end-to-end security
11. Distributed cryptography including functional cryptography
12. Activities supporting the Cryptography Community
13. Ensure a durable integration involving academia, industry, law enforcement and defence agencies
14. Technology watch, joint research agendas and foresight studies
15. Solving training needs and skill shortage of academia and industry
16. Dissemination and outreach, strengthening the link with institutional stakeholders
17. Critical infrastructures and services
18. Joint research combining advanced Clouds and Big Data on Security
19. Innovative Smart ICT solutions for end-users (citizens, workers including home and mobile ones) in private or working environments
20. Ensure security and assistance by online collaboration to support SMEs
21. Cyber-security issues arisen in mobile e-government applications by SMEs
22. Security in communication networks and solutions for real-time information exchange
23. Security management schemes for Smart Grid that consists of millions of devices
24. Risk management frameworks encompassing methods to assess and mitigate the risks in real time
25. Identify new risks and vulnerabilities of ICT systems in critical infrastructures, including the communication networks, stem...
26. Strategies and methodologies for assessing criticalities of services and detecting anomalies due to ICT incidents
27. Address the specific needs and security information of the end-user, private or public organisations
28. Identifying the key factors for promoting a secure and innovative ecosystem through fostering the creation of secure technologies in line with European values

Among those 28 matches above, there are 7 fields that have parity across the EU and all 5 SEA countries included in this report:

1. Establishing Centres of Excellence, Institutes or Organizations to gather and disseminate cyber-security resources
2. Raising awareness and introducing new threats, vulnerabilities and risks
3. Promoting Research and Development in Cyber-security as Joint Researches
4. Developing Human Resources and solve training needs and skill shortage of academia and industry
5. Formulating and improving policies and regulations on information security
6. Protecting national critical infrastructure and network regarding cyber-security
7. Providing assistance to ensure security for SMEs

8.2 The Table of Comparative Matrix
<table>
<thead>
<tr>
<th>EU No</th>
<th>Details in Horizon 2020 (2014-2015 ICT Work programme)</th>
<th>Indonesia</th>
<th>Malaysia</th>
<th>Philippines</th>
<th>Thailand</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Social awareness promotion and information sharing on cyber-security</td>
<td>Institute Technology of Bandung (ITB) has established a Cyber-security Center in collaboration with Korean International Cooperation Agency, to support the R&amp;D activities</td>
<td>THRUST 1: Effective Governance. Centralise coordination of national cyber-security initiatives. ITU-IMPACT (International Multilateral Partnership Against Cyber Threat)</td>
<td>General Directions and Goals of NCSP: Public-private sector and international partnerships. South East Asian Excellence Centres- Recognized ASTI specializing in Service Infrastructure and Engineering.</td>
<td>Promote and support research and development, along with upgrading domestic entrepreneurs, in order to develop technology knowledge and capacity in the country.</td>
<td>Center of Excellence of IT Institute of Hanoi National University. National Institute of Software and Digital Content</td>
</tr>
<tr>
<td>2</td>
<td>open, smart and co-operative CPS</td>
<td>Telkom Indonesia, a major Indonesian telecommunication operator has also launched its Cyber-security Operation Control (CSOC) in order to increase security to its infrastructure</td>
<td>Secure, reliable ICT infrastructure and safe online experience. - Coordination Measures and procedures among stakeholders are in place to protect vital ICT infrastructure by 2016</td>
<td>Strategy 1: Universal and secure ICT and broadband infrastructure</td>
<td>Network and Infrastructure Security Protection</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Matrix of matching priorities among ASEAN and Horizon 2020
| **ICT 2 – 2014: Smart System Integration** | 3 | smart systems are driven by industrial requirements | Application of Risk Management in Information Technology Usage by Commercial Banks in Indonesia | Protect the ICT system from unauthorized entry  
National Cyber-security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors, defence & security, transportation, banking & finance, health services, emergency services, energy, information & communications, government, food & agriculture and water | 4.1 Internet opportunities for all people- improved, cost-efficient service delivery, network infrastructure expansion and upgrades  
Secure, reliable ICT infrastructure and online safety  
6.1 Targets: ICT industry and Business Innovation for National Development by 2016 |

| **ICT 4 – 2015: Customised and low power computing** | 4 | Establish reference architectures and platforms for customised low-power heterogeneous computing systems | National Cyber-security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors: defence & security, transportation, banking & finance, health services, emergency services, energy, information & communications, government, food & agriculture and water | Department of Science and Technology-ASTI priorities included embedded systems on low cost computing. | R&D of power saving systems: hardware and software solutions for data centres |

| **ICT 5 – 2014: Smart Networks and novel Internet Architectures** | 5 | Contribution s to standards: IETF, IRTF may be targeted | Co-author for International standard of ISO/IEC 27037 Guidelines of identification, collection, acquisition and preservation of digital evidence. | The priority of the Philippines to establish SMART grids for the e-science community  
Strategy 1: Universal and secure ICT and broadband infrastructure: Stimulate ICT provision, use and consumption in an holistic approach. A digital ecosystem should be created, paying attention to universal design, usage, program and devices | Chapter 5: Technical Standards of Information Security |

<p>| <strong>II</strong> | <strong>Standards, reference models and architecture framework of cyber-security</strong> |</p>
<table>
<thead>
<tr>
<th>Perspectives</th>
<th>Country</th>
<th>Priority</th>
<th>Research Area</th>
<th>Focus Area</th>
<th>Innovation Approach</th>
<th>Challenges</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT 8 – 2015: Boosting public sector productivity and innovation through cloud computing services</td>
<td>6</td>
<td>reduce the IT expenditure of the public sector</td>
<td>THRUST 1: Effective Governance</td>
<td>Promote effective cooperation between public and private sectors</td>
<td>Internet Opportunities for people” Implement security measures (infrastructure, data and cyber-crime) and privacy protection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT 14 – 2014: Advanced 5G Network Infrastructure for the Future Internet</td>
<td>7</td>
<td>increasing user perceived quality of service, of experience and security</td>
<td>Strategy 1: Universal and secure ICT and broadband infrastructure: Encourage investment in the fixed-line and wireless high-speed network in order to expand the ICT/broadband network to become universally accessible for people throughout the country</td>
<td></td>
<td>Modernizing ICT policies, laws and institution for increased quality, and security on data usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT 32 – 2014: Cyber-security, Trustworthy ICT</td>
<td>9</td>
<td>awareness and introducing new threats, vulnerabilities and risks</td>
<td>the awareness and the countermeasures of cyber-security are still very limited</td>
<td>Raising awareness of cyber-security and its implications</td>
<td>Advocacy and public awareness. Identification and elimination of threats. It involves knowing the threats and determination of ways in which they can be effectively neutralized</td>
<td>Awareness and knowledge should be raised about the policy and guidelines for information security targeting the Chief Information Officer (CIO) of public and private sector organizations, especially organizations in charge of critical infrastructure.</td>
<td>Information delivery management</td>
</tr>
<tr>
<td>FP7/ICT/№ 611014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICT 32 – 2014: Cyber-security, Trustworthy ICT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security-by-design for end-to-end security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secure Communication:</strong> To help protect the confidentiality and integrity of information during transmission and storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>THRUST 6: Compliance and Enforcement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Standardise cyber-security systems across all elements of the CNII</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Strengthen the monitoring and enforcement of standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Develop a standard cyber-security risk assessment framework</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICT project evaluation of the product security features against Common Criteria standard using ISO/IEC 15408 and ISO/IEC18045</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Guiding Framework of National Cyber-security Plan: Part 4 Cyber Infrastructure Protection Requirements Promoting Secure Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information Security Management System (ISMS) certification</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 2: Cyber-security Protection - Information System’s Security Levels</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Formalise the coordination and prioritisation of cyber-security research and development activities
- Enlarge and strengthen the cyber-security research community
- Promote the development and commercialisation of intellectual properties, technologies and innovations through focused research and development. Nurture the growth of cyber-security industry |
| Research and Development including but limited to Cryptography, Information Welfare, Intrusion Detection, Hacking, Vulnerability Assessment |
| Chapter 4: Civil Cryptology
- Production of Civil Crypto Products
- The Use of Civil Crypto Products
- The security Protection of Civil Cryptology
- Civil Cryptology Security Management and Monitoring |

---

- Develop, foster and maintain a national culture of security
- Standardise and coordinate cyber-security awareness and education programmes across all elements of the CNII
- Establish an effective mechanism for cyber-security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals |
| Education and Training, Knowledge Management, Research and Development |
| Awareness and knowledge should be raised about the policy and guidelines for information security targeting the Chief Information Officer (CIO) of public and private sector organizations, especially organizations in charge of critical infrastructure. |
| Chapter 4: Civil Cryptology
- Production of Civil Crypto Products
- The Use of Civil Crypto Products
- The security Protection of Civil Cryptology
- Civil Cryptology Security Management and Monitoring |

III Open platforms for cyber-security
| ICT 32 – 2014: Cyber-security, Trustworthy ICT | 14 | technology watch, joint research agendas and foresight studies | it is considered implicitly as element or characteristic of the ICT research program. |
| ICT 32 – 2014: Cyber-security, Trustworthy ICT | 15 | solve training needs and skill shortage of academia and industry | Major universities of Indonesia, in Jakarta as well as other major city such as Bandung, Jogjakarta, Surabaya, Medan etc. have also various information and cyber-security programs under its ICT department. |
| ICT 32 – 2014: Cyber-security, Trustworthy ICT | 16 | dissemination and outreach, strengthening the link with | few policies and regulation on information security had been set-up 8.3.2 THRUST 2: Legislative &Regulatory Framework - Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber-security threats submission of bills for law creation pertaining to cyber-security. 2) Laws and regulations to control and deter cyber threats 5) Effective law enforcement |


Information Security Law: This law has 8 Chapters and 56 articles.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT 32 – 2014: Cyber-security, Trustworthy ICT</td>
<td>17</td>
<td>Protect national critical infrastructure and improve the security of cyberspace individually and collectively</td>
<td>The 21st century infrastructure protection programmes will need to consider a host of virtual as well as physical threats</td>
<td>Assuring the continuous operation of our critical cyber infrastructures</td>
<td>Improve the quality of the network in preparation for the Next Generation network and intelligent network of the future</td>
<td>Some national cyber-security products of protecting information security in the enterprise LAN and on cloud infrastructures</td>
</tr>
<tr>
<td>EU-Brasil</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EUB 1 – 2015: Cloud Computing, including security aspects</td>
<td>18</td>
<td>Joint research combining advanced Clouds and Big Data on Security</td>
<td>Given the cyberspace crime is mostly cross-country, therefore the government should actively cooperate with foreign parties and focus to protect national interests.</td>
<td>THRUST 8: International Cooperation - Encourage active participation in all relevant international cyber-security bodies, panels and multinational agencies - Promote active participation in all relevant international cyber-security events, conferences and forums - Enhance the strategic position of Malaysia in the field of cyber-security by hosting an annual international cyber-security conference</td>
<td>Public-private sector and international partnerships ICT Industry and Business Innovation for National Development 6.4 Key Actions includes cloud computing</td>
<td>Cyber-security Master Plan to 2020 + National and International Cooperation in Cyber-security + Constructions of Institutions and Standards: National Information Security Agency and CSIRT, Technical Infrastructures</td>
</tr>
<tr>
<td>EU-Japan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU-Japan Research and Development Cooperation in Net Futures</td>
<td>19</td>
<td>Innovative Smart ICT solutions for end-users (citizens, workers including home and mobile ones) in private or working environments</td>
<td>Given the cyberspace crime is mostly cross-country, therefore the government should actively cooperate with foreign parties and focus to protect national interests.</td>
<td>THRUST 8: International Cooperation - Encourage active participation in all relevant international cyber-security bodies, panels and multinational agencies - Promote active participation in all relevant international cyber-security events, conferences and forums Enhance the strategic position of Malaysia in the field of cyber-security by hosting an annual international cyber-security conference Cyber-security Malaysia, as Permanent Secretariat of the OIC-CERT has proposed setting up a Cyber-security Centre of Excellence and Malware Research coordination facility for OIC countries.</td>
<td>Public-private sector and international partnerships</td>
<td></td>
</tr>
<tr>
<td>INNOSUP 6 – 2015: Capitalising the full potential of online-collaboration for SME innovation support</td>
<td>FP7/ICT/No 611014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure security for assistance all online collaboration for innovation for SMEs</td>
<td>Promote effective cooperation between public and private sectors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.2.3 Partnership. Required the cooperation and partnership of various parties to create cyberspace security, given the cyber-security issue is a collective responsibility.</td>
<td>Public and private partnership cooperation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT Industry Development and Business Innovation. Enhancing the capacity of small and micro businesses to leverage ICTs</td>
<td>A digital ecosystem should be created, paying attention to universal design, usage, program and devices. This will promote access of all groups of people and will stimulate the public sector market and consumption by the private sector and Small and Medium Enterprises (SMEs).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure security for assistance all online collaboration for innovation for SMEs</td>
<td>Some national cyber-security products of protecting information security in the enterprise LAN and on cloud infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INSO-9-2015 - Innovative mobile e-government applications by SMEs</th>
<th>Chapter 3: Private Online Information Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-security issues arisen in mobile e-government applications by SMEs</td>
<td>Promote and support research and development, along with upgrading domestic entrepreneurs, in order to develop technology knowledge and capacity in the country</td>
</tr>
<tr>
<td>Philippine e-government master plan mentions one of the thrusts of Philippine Digital Strategy thrust: - Internet for All- Digital Inclusion, Modernize ICT laws, policies, institutions, data privacy, cyber-security, etc.</td>
<td>\</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security in communication network and solutions for real-time information exchange</td>
<td>- Information Security Business Classification</td>
</tr>
<tr>
<td>THRUST 1: Effective Governance . Establish formal and encourage informal information exchanges</td>
<td>- Conditions for Information Security Businesses</td>
</tr>
<tr>
<td>Main Objectives of PDS- ICT Innovations and commercialisation</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Security management schemes for Smart Grid that consists of millions of devices</td>
</tr>
<tr>
<td>Call – Digital Security: Cyber-security, Privacy and Trust</td>
<td></td>
</tr>
<tr>
<td>DS-6-2014: Risk management and assurance models</td>
<td>24</td>
</tr>
</tbody>
</table>
DS-3-2015: The role of ICT in Critical Infrastructure Protection

25 Identify new risks and vulnerabilities of ICT systems in critical infrastructures, including the communication networks, stem...

National Cyber-security Plan
Strategy 4: Institutional build-up

Philippine Digital Strategy: ICT industry and business innovation for national development

26 Strategies and methodologies for assessing criticalities of services and detecting anomalies due to ICT incidents

Protect national critical infrastructure and improve the security of cyberspace individually and collectively

Assuring the continuous operation of our critical cyber infrastructures

Robust systems

Chapter 2: Cyber-security Protection
- Malware detection and processing
- Secure protection of Telecommunication resources
- Information System’s Security Monitoring

DS-4-2015: Information driven Cyber-security Management

27 Address the specific needs and security information of the end-user, private or public

National Cyber-security Plan, Strategy 3: Organization and Mobilization for cyber security

Chapter 2: Cyber-security Protection
- Information classification
- Information delivery management
- Information System’s Security Monitoring
organisation
s

The missions of Information System’s Security Protection
- Responsibilities of Information System’s owners

DS-7-2015: Value-sensitive technological innovation in Cyber-security

28

Identifying the key factors for promoting a secure and innovative ecosystem through fostering the creation of secure technologies in line with European values

THRUST 3: Cyber-security Technology Framework
- Develop a national cyber-security technology framework that specifies cyber-security requirement controls and baselines for CNII elements
- Implement an evaluation/certification programme for cyber-security products and systems

National Cyber-security Plan
Strategy 1: National Assessment
Strategy 3: Organization and Mobilization of Cyber-security

Chapter 2: Cyber-security Protection

<table>
<thead>
<tr>
<th>EU N o</th>
<th>Details in Horizon 2020 (2016-2017 ICT Work programme)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indonesia</td>
</tr>
<tr>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Matrix of matching priorities among ASEAN and Horizon 2020 (2016-2017 Work Programme)
<table>
<thead>
<tr>
<th>Project</th>
<th>Number</th>
<th>Description</th>
<th>Strategy 1: Universal and secure ICT and broadband infrastructure:</th>
<th>Assuring the continuous operation of our critical cyber infrastructures</th>
<th>Improve the quality of the network in preparation for the Next Generation network and intelligent network of the future</th>
<th>Some national cyber-security products of protecting information security in the enterprise LAN and on cloud infrastructures</th>
</tr>
</thead>
<tbody>
<tr>
<td>EINFRA-12-2017: Data and Distributed Computing e-infrastructures for Open Science</td>
<td>1</td>
<td>address the aspects of privacy, cybersecurity and information assurance</td>
<td>Protect national critical infrastructure and improve the security of cyberspace individually and collectively</td>
<td>Assuring the continuous operation of our critical cyber infrastructures</td>
<td>Improve the quality of the network in preparation for the Next Generation network and intelligent network of the future</td>
<td>Some national cyber-security products of protecting information security in the enterprise LAN and on cloud infrastructures</td>
</tr>
</tbody>
</table>
| **ICT-05-2017:** Customised and low energy computing | this call is interested in “security by design” features allowing applications to be resilient to cyber-attacks are encouraged to be part of the proposed technology | Secure Communication: To help protect the confidentiality and integrity of information during transmission and storage  
THRUST 6: Compliance and Enforcement  
- Standardise cyber-security systems across all elements of the CNII  
- Strengthen the monitoring and enforcement of standards  
- Develop a standard cyber-security risk assessment framework  
Cyber Infrastructure Protection Requirements Promoting Secure Environment | Chapter 2: Cyber-security Protection - Information System’s Security Levels |
| ICT-06-2016: Cloud Computing | techniques to deal with trust, security and privacy in decentralised cloud infrastructures and across multiple cloud providers | Given the cyberspace crime is mostly cross-country, therefore the government should actively cooperate with foreign parties and focus to protect national interests.  
THRUST 8: International Cooperation  
- Encourage active participation in all relevant international cyber-security bodies, panels and multinational agencies  
- Promote active participation in all relevant international cyber-security events, conferences and forums  
- Enhance the strategic position of Malaysia in the field of cyber-security by hosting an annual international cyber-security conference  
Public-private sector and international partnerships  
ICT Industry and Business Innovation for National Development 6.4 Key Actions includes cloud computing | | |
<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
<th>Key Actions</th>
<th>Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT-14-2016-2017: Big Data PPP: cross-sectorial and cross-lingual data integration and experimentation</td>
<td>Aiming to eliminate the lack in Europe of secure environment s “where researchers and SMEs can test innovative services and product ideas based on open data and business data”</td>
<td>Public-private sector and international partnerships</td>
<td>ICT Industry and Business Innovation for National Development</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.4 Key Actions includes cloud computing</td>
</tr>
<tr>
<td>ICT-35-2016: Enabling responsible ICT-related research and innovation</td>
<td>Also focused in ongoing ICT-related research and innovation and especially cyber-physical systems, and cybersecurity</td>
<td>It is considered implicitly as element or characteristic of the ICT research program.</td>
<td>Identify &amp; prioritize key technology areas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Research and Development Institutional Build-up, F. Research and Development</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Promote and support research and development, along with upgrading domestic entrepreneurs, in order to develop technology knowledge and capacity in the country.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 national R&amp;D projects funded by Ministry of Science and Technology (MOST) and Ministry of Industry and Trade (MOIT).</td>
</tr>
<tr>
<td>Project</td>
<td>Description</td>
<td>Theme</td>
<td>Support</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>SMEInst-13-2016-2017: Engaging SMEs in security research and development</td>
<td>To engage small and medium enterprises in innovation activities in the domain of security, especially those not traditionally involved in it</td>
<td>SMEs in security research and development</td>
<td>Public and private partnership cooperation</td>
</tr>
<tr>
<td>SMEInst-06-2016-2017: Accelerating market introduction of ICT solutions for Health, Well-Being and Ageing Well</td>
<td>secure eHealth solutions for consumers</td>
<td>Health, Well-Being and Ageing Well</td>
<td>A digital ecosystem should be created, paying attention to universal design, usage, program and devices. This will promote access of all groups of people and will stimulate the public sector market and consumption by the private sector and Small and Medium Enterprises (SMEs).</td>
</tr>
<tr>
<td>SCI-PM-18–2016: Big Data supporting Public Health policies</td>
<td>related to Big Data and the integrated solutions that should include suitable approaches towards securing security and privacy issues</td>
<td>Big Data supporting Public Health policies</td>
<td>Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are: - National Defence and Security - Banking and Finance - Information and Communications - Energy - Transportation - Water - Health Services - Government</td>
</tr>
<tr>
<td>LCE-01-2016-2017: Next generation innovative technologies enabling smart grids, storage and energy system integration with increasing share of renewables: distribution network</td>
<td>the topic also requests that &quot;real-time system awareness; secured communications in the smart grid in particular cyber security and big data analytics&quot; should also be addressed</td>
<td>Co-author for International standard of ISO/IEC 27037 Guidelines of identification, collection, acquisition and preservation of digital evidence.</td>
<td>The priority of the Philippines to establish SMART grids for the e-science community</td>
</tr>
<tr>
<td>MG-6.3-2016: Roadmap, new business models, awareness raising, support and incentives for the roll-out of ITS</td>
<td>proposals should also address &quot;market sizing, customer demand vs. production, project feasibility and financial returns, as well as the awareness and the counter-measures of cyber-security are still very limited</td>
<td>Raising awareness of cyber-security and its implications Cyber-security Malaysia conducts vulnerability assessment &amp; penetration testing (VAPT) services to CNII sector. It also conduct vulnerability assessment services for Control System (SCADA/DCS) to relevant CNII sector.</td>
<td>Advocacy and public awareness. Identification and elimination of threats. It involves knowing the threats and determination of ways in which they can be effectively neutralized</td>
</tr>
<tr>
<td>ART-01-2017: ICT infrastructure to enable the transition towards road transport automation</td>
<td>The topic also requests and advancement of the principles of cyber security for the automated vehicles</td>
<td>Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are: - National Defence and Security - Banking and Finance - Information and Communications - Energy - Transportation - Water - Health Services - Government - Emergency Services - Food and Agriculture</td>
<td>Assuring the continuous operation of our critical cyber infrastructures</td>
</tr>
<tr>
<td>SC5-12-2016: Food systems and water resources for the development of inclusive, sustainable and healthy Euro-Mediterranean societies</td>
<td>a continuation of the WATER related calls of the previous Work Programme</td>
<td>Protect national critical infrastructure and improve the security of cyberspace individually and collectively</td>
<td>Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are: - National Defence and Security - Banking and Finance - Information and Communications - Energy - Transportation - Water - Health Services - Government - Emergency Services Food and Agriculture</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe</td>
<td>CIP</td>
<td>Protect national critical infrastructure and improve the security of cyberspace individually and collectively</td>
<td>Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are: - National Defence and Security - Banking and Finance - Information and Communications - Energy - Transportation - Water - Health Services - Government - Emergency Services Food and Agriculture</td>
</tr>
<tr>
<td>DS-02-2016: Cyber Security for SMEs, local public administration and Individuals</td>
<td>7.2.3 Partnership. Required the cooperation and partnership of various parties to create cyberspace security, given the cyber-security issue is a collective responsibility.</td>
<td>Promote effective cooperation between public and private sectors</td>
<td>Public and private partnership cooperation ICT Industry Development and Business Innovation. Enhancing the capacity of small and micro businesses to leverage ICTs</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>DS-03-2016: Increasing digital security of health related data on a systemic level</td>
<td>eHealth</td>
<td>Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are: - National Defence and Security - Banking and Finance - Information and Communications - Energy - Transportation - Water - Health Services - Government - Emergency Services Food and Agriculture</td>
<td></td>
</tr>
</tbody>
</table>
| DS-04-2016: Economics of Cybersecurity | THRUST 1: Effective Governance  
Promote effective cooperation between public and private sectors | Internet Opportunities for people”  
Implement security measures (infrastructure, data and cyber-crime) and privacy protection. | Chapter 8: Government Administration and Management of Information Security |
|---|---|---|---|
| DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation | Institute Technology of Bandung (ITB) has established a Cyber-security Center in collaboration with Korean International Cooperation Agency, to support the R&D activities | THRUST 1: Effective Governance  
Centralise coordination of national cyber-security initiatives  
ITU-IMPACT (International Multilateral Partnership Against Cyber Threat) | General Directions and Goals of NCSP: Public-private sector and international partnerships  
South East Asian Excellence Centres- Recognized ASTI specializing in Service Infrastructure and Engineering.  
Promote and support research and development, along with upgrading domestic entrepreneurs, in order to develop technology knowledge and capacity in the country.  
Center of Excellence of IT Institute of Hanoi National University, National Institute of Software and Digital Content |
| DS-06-2017: Cryptography | support good practices that can bring cyber-secure primitives and applications | THRUST 5: Research & Development Towards Self-Reliance  
Formalise the coordination and prioritisation of cyber-security research and development activities  
Enlarge and strengthen the cyber-security research community  
Promote the development and commercialisation of intellectual properties, technologies and innovations through focused research and development. Nurture the | Research and Development including but limited to Cryptography, Information Welfare, Intrusion Detection, Hacking, Vulnerability Assessment  
Chapter 4: Civil Cryptology - Production of Civil Crypto Products - The Use of Civil Crypto Products - The security Protection of Civil Cryptology - Civil Cryptology Security Management and Monitoring |
<table>
<thead>
<tr>
<th>FP7/ICT/№ 611014</th>
<th></th>
<th>growth of cyber-security industry</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DS-07-2017:</strong> Addressing Advanced Cyber Security Threats and Threat Actors</td>
<td>The call also supports the EU-Japan ICT dialogue in the area of cybersecurit y</td>
<td>it is considered implicitly as element or characteristic of the ICT research program.</td>
<td></td>
</tr>
<tr>
<td><strong>SwafS-22-2017:</strong> The ethical dimensions of IT technologies: a European perspective focusing on security and human rights aspects</td>
<td>promoting innovation, enabling high quality job creation and ensuring a high level of privacy and cyber security</td>
<td>identify &amp; prioritize key technology areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Research and Development Institutional Build-up, F. Research and Development</td>
<td>Promote and support research and development, along with upgrading domestic entrepreneurs, in order to develop technology knowledge and capacity in the country.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 national R&amp;D projects funded by Ministry of Science and Technology (MOST) and Ministry of Industry and Trade (MOIT).</td>
<td></td>
</tr>
<tr>
<td>IoT-01-2016: Large Scale Pilots</td>
<td>addressing, in particular, issues of trust, attention, security and privacy through pre-defined privacy and security impact assessments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT-02-2016: IoT Horizontal activities</td>
<td>privacy, security, user acceptance, standardisation, creativity, societal and ethical aspects</td>
<td>Co-author for International standard of ISO/IEC 27037 Guidelines of identification, collection, acquisition and preservation of digital evidence.</td>
<td>The priority of the Philippines to establish SMART grids for the e-science community</td>
</tr>
<tr>
<td>IoT-03-2017: R&amp;I on IoT integration and platforms</td>
<td>IoT security and privacy. Approaches must be holistic and include identification and authenticatio n, data protection and prevention against cyber-attacks at the device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and system levels</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9 Recommendations for Possible EU-ASEAN Joint Cooperation

As this report has already mentioned in above items, there are 7 matches which are strongly fitted among all EU and all 5 ASEAN countries. Based on these 7 matches, the report proposes several recommendations for possible EU-ASEAN joint cooperation and divides recommendations into “Participate in large visionary projects” and “Expand the Cyber-security cooperation” as following items.

The report proposes 2 long-term projects for group of “Participate in large visionary projects” and other 5 short-term activities for group of “Expand the Cyber-security cooperation”. The output of long-term projects might be clear and have large impact on the actual ICT application but take long time; meanwhile the long-term projects might be shorter time but make quick results, have direct impact on the cyber-security cooperation between EU and ASEAN.

9.1 Participate in large visionary projects

This report proposes 3 visionary projects to cooperation among ASEAN and EU as below:

   9.1.1 Promote Research and Development on the enterprise infrastructure protection in the evolution toward SDN

   The enterprise infrastructure currently is heavily based on the mature LAN technologies. Since, the network technology is going to evolve to SDN (Software Defined Network). However, most small and medium enterprises and government agencies in SEA are not ready for this process, because there are no guidelines for it and a lot of concerns about the Cyber Security of new platform. Guidelines and reference models based on the experience in EU can avoid the risk, save the implementation cost and provide a huge market for advanced technologies. The components of the projects are


   b. Research and development in selected topics:

      - Performance and Security of Virtualization of Infrastructure

      - Cryptography, CA and solutions for data synchronization between subnetworks with special needs of security protections

      - Traffic monitoring and optimization

      - Attack Pattern recognition

      - Secure Network Management

   c. Consulting services about the technologies of the project
9.1.2 EU-ASEAN Cyber Security Professional Training and Technology Transfer

Human resources is always the top priority for any country and is one of the easy ways to get cooperation among countries and among region, such as EU and ASEAN. In this project, the joint activities to implement the project are to exchange the expert in cyber-security between EU countries and ASEAN countries. In addition, the joint activities to implement can be the workshop or short training courses in order to find the common action to protect the ICT systems of EU and ASEAN.

This project fits 4th item of 7 matches which are fully satisfied the priorities of EU and ASEAN countries in the matrix.

The Project will provide fund to the following activities

a. Professional training courses on the basic and hot topics in cyber security for SEA countries
b. Master courses (Joint degree between EU and SEA institutions) in Cyber Security
c. Research Ph.D. and visiting Professor scholarships in cyber security with but not limited to the following topics:
   - Advanced High Performance and Quantum Cryptography
   - Attack Pattern and Identity Recognition
d. Technical support in Cyber Security: Advices will be provided by a expert network, with the core of the professors, professionals, graduate students and trainees, who have received support from of the project.

The project will have a headquarter office in a SEA countries, but the activities will be done in the SEA countries, where most applicants are there to save funds. Some R&D travel funds will be provided for the visits to EU labs. The researcher and professors in EU will visit SEA countries.

9.1.3 ASEAN Technical support center for secure key enterprise applications and open sources

The cyber security related technical issues are replicated in all the ASEAN countries. Most of them have been addressed with solutions in EU or other ASEAN countries. The key enterprise applications are similar and can be standardized in ASEAN businesses and government agencies. Those applications will face similar cyber security threats. It will save a lot of efforts, if the basic applications with basics protections can be developed (possibly based on the open sources) and shared as open sources. The center will provide assistance mainly to the SME.

The project will fund the security protection solutions for the key enterprise applications, for example

- Secure Document Management and Exchanging systems
- Secure CMS for Enterprise Portal.
- Secure Data Synchronization between Distributed network
- Secure User Management and Certification System

The basic system and security enhancing solution will be given as standardized libraries or open sources for further customizations with technical support from participating institutions.

The center will be organized as an ad hoc distributed online center formed by participating institution. One managing office can be formed and operated by a volunteering partner.

9.2 Recommendations Expand the Cyber-security Cooperation

In the short-term activities, this report also propose groups of cooperated projects, which are fully fitted the 7 matches between EU and ASEAN mentioned above. These proposals help to promote the cooperation among ASEAN and EU. They are described as below:

The recommendations made as the results of the targeted action in cyber security in CONNECT2SEA will be used in different events to the suitable organizations and people. These recommendations are mainly actions, which include projects and non-project activities.

9.2.1 Recommendations to EU and ASEAN bodies

The EU and ASEAN bodies are EC, COST, TEL and similar organizations.

1. Create ASEAN Cyber Security Technical Committee or body (or empower the existing body), linking together legislative and policy issues in cybersecurity (TELSOM), and R&D issues (COST)
   - Consist of academic researchers, independent professionals, vendors and policy makers in cyber security.
   - Discuss R&D, implementation, standardization initiatives and cooperation
   - Discuss the legal issues and give recommendations for the policy makers

2. Encourage and initiate ASEAN Joint projects on
   - Cyber Security Standardization and Architecture Framework
   - Cyber Security Code of Conduct
   - Sharing the attack patterns

3. Assessment of the maturity of activities in Cyber Security in ASEAN

The current status of cyber security in ASEAN countries must be assessed regularly by one or more professional organizations or projects. The results are useful as a reference for achieving consensus, cooperation and project ideas.

Objectives: Frequent assessment for Cyber Security situations in ASEAN countries according to EU norms would useful for finding solutions in terms of:

- Technology capability
- Infrastructure
- Website vulnerabilities
4. Development of Human Resources and Social Awareness

There must be a special EU-SEA cooperation program, which is similar with one with China, Japan, Mexico and Brazil. The initial focuses can be

- Cyber Security

9.2.2 Recommendations to ASEAN and/or EU Member states

The ASEAN and EU countries, who want to promote EU-ASEAN cooperation in cyber security should focus in the following activities in the first steps

1. Human resources development:
   - Exchange technical and implementation experience
   - Professional training, joint degree education and joint R&D.

2. Awareness promotion
   - Sharing experience
   - Database of new threats.
   - Regional technical supports.
   - R&D map in cyber security

9.2.3 Recommendations to the ASEAN RDI organizations

The following R&D topics are priorities:

a. R&D on new threats and urgent issues
b. R&D on long term issues
   - SDN network: The evolution toward new technology platform of Cloud computing lead to the need for R&D activities to protect the new infrastructure which is based on a new technologies.
   - High performance cryptography

9.3 Recommendations for Cyber-security Activities Promotion

9.3.1 Linked-In Community of Practice

The LinkedIn Community of Practice (CoP) “Connect EU-SEA Cyber Security” (CONNECT-EACS) has already been established since May 2015. It has the objective to become an important channel to connect experts in cyber-security both of SEA and EU sides. This professional social networking shows its key roles in combination, matching the people working together. This CoP will continue to operate in the long term by the volunteer partners of CONNECT2SEA like ITI-VNU.
By March 2016, CONNECT-EACS has more than 80 members exchanging ideas about the following issues:

a. *The Policy Issues:* Policy is very important in Cyber Security and needs international cooperation. Policy issues in Cyber-Security must be discovered, formulated and recommended by the interactions between policy makers, researchers and industrial professionals. The CoP will collect ideas and organize the actions leading to effective contributions to the international, regional and national bodies.

b. *Research and Development Cooperation:*
   - *Matching the R&D project ideas:* The members can solicit their project ideas and find partners from many sides between SEA and EU countries to construct real projects and find funds to implement those.
   - *Finding partners:* The members help each other to find partners in SEA and EU for R&D activities.
   - *R&D Map of EU and SEA:* The experts can post their R&D interest on the CoP. Thus in the long term, it will form a R&D Map of EU and SEA in Cyber Security which will be useful for people who want to search for R&D groups in certain specific topics.

c. *Exchange implementation project experience*
   The implementation of the cyber security systems also need international cooperation from the Phase of Proposal, Fund finding, Implementation and Operation
   - Implementation Project ideas.
   - Project finance
   - Implementation experience
   - Operation issues
   - Procurement and commercial products

CONNECT2SEA-EACS also supports the interest groups on security, all of academic, corporate, government, society alumni. The groups have good channel to be accessible to cyber-security members to read, though they must join in order to post messages. The CoP allows users to endorse each other’s skills and knowledge on security.

Currently CONNECT2SEA-EACS is organized as follows

1. Main forum: To discuss the general issues, to post news related to cyber security.
2. Subtopics: For more effective discussion in specific topics, members can discuss the specific topics in smaller groups in the following subgroups
   - EU-SEA Cyber Security Policy Dialog
   - EU-SEA Cyber Security Practical Issues (Implementation Project Experience)
   - EU-SEA R&D Cooperation Opportunities in Cyber Security
9.3.2 ASEAN body (Committee) on Cyber-security

One of important recommendations of this report is a proposal to setup an ASEAN Committee (or body) on Cyber-security covering both policy and research & innovation aspects, or empower the existing body with this function. The cooperation among members will be controlled and synchronized by this body. Its name may be the “ASEAN Network and Information Security Committee”, which can stand short name by SEA-NISC (ASEAN-NISC).

The vision of the Committee is the regional cooperation activities in cyber-security can help the countries in ASEAN to catch up with the world standards and maximize the benefits of the national efforts.

The mission of the Committee is to implement the common efforts in cyber-security standards, recommendations to policy dialogues, guidelines in R&D and sharing experiences in cyber-security infrastructure deployment.

The objectives of the Committee are to setup and implement the activities in order to resolve the issues as below:

- Cyber-security Standard Recommendations
- Cyber-security Reports from member countries and regional overviews
- R&D map, directories and professional forum in cyber-security.
- Comments on National and Regional Cyber-security Policy issues.
- Introduction of New Solutions and Products
- New threat awareness promotions

The function of the Committee is as below:

- Intra and Inter regional cooperation promotion activities
  + Network of professionals in cyber-security.
  + Common platform for Policy makers, academics, businesses and infrastructure builders in cyber-security
  + Cooperation with ENISA and EU.

- Recommendations and Comments on National and Regional Cyber-security policies.
  + Network of national contacts, which will provide regular reports on the updated national policies.
  + Synthesis of the regional policy picture
  + Experience from international cyber-security policies
  + Recommendations to the Policy Dialogues
  + Comments on new and outdated policies

- R&D cooperation activities:
  + Identify the practical needs
  + Integrate R&D results into practical solutions
  + Future technologies which might be relevant for cyber-security.
d. Sharing information and public awareness promotion in cyber-security
   + Sharing implementation experience
   + New threats and new solutions
   + Business matching for cooperation
   + Promotions of knowledge, technology transfer and products
   + Public awareness promotion
   + Publications

e. Shares databases of attack patterns

The organization of the Committee should be consisting of Policy makers; Academics; Businesses; ISP. In addition, the Head of Committee will be assigned by ASEAN Secretary (Headquarter in Jakarta). The Committee Members should also include officials who come from government authority of ASEAN state members.

The actions of the Committee should include the organizing some events, such as CONNECT2SEA Events, Forum. They also make some channel for experience sharing of the National Projects among ASEAN countries. They also help to be the body for Publications of research or experiment on security. The Committee also should work with SCMIT and TELSOM events to find the common activities. The Committee may solicit the ideas to Vietnamese policy makers and ask them to present the idea to ASEAN and make Committee Formation to effectively manage. Other actions should be synchronizing the common activities given by CERT and evaluating of Cyber-security Status in ASEAN annually.

9.3.3 Pilot technical assistance and Cyber Security Architecture Framework

The results of inter and intra-regional cooperation in ASEAN and/or between EU-SEA can be more convincing, if it starts with the technical assistance to those nations or units, which are beginning of development. The experience in the implementation of legal document, key infrastructures and R&D activities is valuable and can help to save a lot of time and money.

Cyber Security Architecture Framework (CSAF) is a blue print to start with. Based on its guidelines, one can plan more detailed actions while keeping the overall construction of Cyber Security infrastructure, legal system and R&D organization interoperable.

CSAF is based on the idea of Enterprise Architecture Framework (EAF), which is popular in ICT implementation and is matured in advanced countries including EU, North America and North Asia. It provides a systematic methodology to plan a sophisticated ICT infrastructure for a nation, government agencies and enterprises. It helps to save cost and guarantees the interoperability.

For developing countries, especially for those who are at beginning of the development, CSAF is very helpful for the future actions. The studies and pilot in such ASEAN countries like Laos, Cambodia, Myanmar,... will be useful input for CSAF.
10 Cyber-security Policy Analysis

Cyber-security is an issue of increasing importance in the modern world, and its solutions can often be difficult to implement on a large scale, nationally or internationally. Having a strong, clear, shared framework is vitally important to keeping cyberspace as secure as possible, in EU, ASEAN or elsewhere.

This is the reasoning behind the EU Cyber-security Maturity Dashboard developed by BSA – Global Software Alliance. The dashboard (report) collects data from 28 EU countries, using a standardized set of criteria. Its primary purpose is to give EU government officials the chance to evaluate their cyber-security policies in comparison with those of other EU countries (but the standardized set of criteria can also be used for ASEAN, perhaps with minor revision). The dashboard is intended to be a living document, updated regularly to show developments in policy as more cyber-security gaps are addressed and filled. The Dashboard’s methodology involved exclusively desk-based research, using publicly available information, with no need for direct interviews. The report can be found in its entirety at http://cybersecurity.bsa.org/.

The dashboard highlights important stumbling blocks to creating a strong policy on cyber-security:

- Manipulating standards. The most effective way to free innovation is to adopt internationally recognized technical standards so that innovative solutions can be accepted across markets.
- Imposing rules on data localization. The cloud model allows data to flow freely, which increases reliability, resilience and opportunities for 24 hour service support.
- A preference for indigenous technology. Foreign competition should be welcomed, as it provides the opportunity to but world-class products and services...

According to the EU cyber-security dashboard report, these are the most important components of a strong legal framework for ensuring cyber-security:

- Being practicable. Policy should be adoptable by the largest possible groups of critical assets and the broadest possible range of critical actors
- Being flexible, to accommodate a wide range of stakeholder needs
- Effective government partnerships with the private sector, as it owns and operates most of the commercial infrastructure services
- Operational entities such as teams for incident response, emergency and operational computer security...

The Dashboard also notes that while cyber-security and cyber resilience are often viewed as funding challenges, they are in fact management ones. The key steps are less related to budgeting than and far more to optimizing legal and policy frameworks, improving collaboration with stakeholders’ communities, effectively sharing information and prioritizing the protection of critical infrastructures.

Earlier, R. Anderson, R. Bohme, R. Clayton and T. Moore (2007) made a report to set out a set of recommendations about security policy. The recommendations mentioned about the
information security issues should be handled at the Member State level and what issues may require harmonization. The report is trusted due to its draw conclusion from researching on both economic principles and empirical data. According to the report, the EU should have 15 focuses on policy regarding the security, they include:

1. EU introduce a comprehensive security-breach notification law.
2. Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime.
3. ENISA collect and publish data about the quantity of spam and other bad traffic.
4. The European Union introduce a statutory scale of damages against ISPs that do not respond promptly to requests for the removal of compromised machines, coupled with a right for users to have disconnected machines reconnected if they assume full liability.
5. The EU develops and enforces standards for network-connected equipment to be secure by default.
6. The EU adopts a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle.
7. The security patches be offered for free, and that patches be kept separate from feature updates.
8. The European Union should harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions.
9. The European Commission prepares a proposal for a Directive establishing coherent regime of proportionate and effective sanctions against abusive online marketers.
10. ENISA should conduct research, coordinated with other affected stakeholders and the European Commission, to study what changes are needed to consumer-protection law as commerce moves online.
11. ENISA should advise the competition authorities whenever diversity has security implications.
12. ENISA sponsor research to better understand the effects of Internet exchange point (IXP) failures. We also recommend they work with telecoms regulators to insist on best practice in IXP peering resilience.
13. The European Commission put immediate pressure on the 15 EU Member States that have yet to ratify the Council of Europe Convention on Cyber-crime.
14. The establishment of an EU-wide body charged with facilitating international cooperation on cyber-crime, using NATO as a model.
15. ENISA champion the interests of the information security sector within the European Commission to ensure that regulations introduced for other purposes do not inadvertently harm security researchers and firms.

From this, European security policies focus not only on regulatory issues, but also on their effects on stakeholders, including telecommunications services, the banking sector, internet
exchange points, and security researchers. The priorities also include clear actions and responsibilities with respect to data collection, statistics, standards and competition mechanisms.

In order to analyze the connection of policy between EU and ASEAN, the CONNECT2SEA team used the same questionnaire (as used in the EU Cybersecurity Maturity Dashboard) for the ASEAN countries, in order to match some common priorities between 2 sides. The result of the dashboard is provided below.

Benchmarking cyber-security framework and policy tool for the ASEAN countries

✓ = yes, 0 = no;  x = process started

### 10.1 The ASEAN Cyber-security Dashboard

#### Table 2: ASEAN Cyber-security Policy Dashboard

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Brunei</th>
<th>Cambodia</th>
<th>Indonesia</th>
<th>Lao PDR</th>
<th>Malaysia</th>
<th>Myanmar</th>
<th>Philippines</th>
<th>Singapore</th>
<th>Thailand</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>LEGAL FOUNDATIONS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Is there a national cyber-security strategy in place?</td>
<td>0</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>X</td>
<td>0</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>What year was the national cyber-security strategy adopted?</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2008</td>
<td>0</td>
<td>2011</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Is there a critical infrastructure protection (CIP) strategy or plan in place?</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>Is there legislation/policy that requires the establishment of a written information security plan?</td>
<td>0</td>
<td>0</td>
<td>✓</td>
<td>0</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

(started)
<table>
<thead>
<tr>
<th></th>
<th>Is there legislation/policy that requires an inventory of “systems” and the classification of data?</th>
<th>√</th>
<th>(esp. for data classification)</th>
<th>√</th>
<th>(National ICT policy of Lao PDR)</th>
<th>X</th>
<th>Classification of data-YES. But inventory of systems-NO.</th>
<th>X</th>
<th>(started)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?</td>
<td>0</td>
<td>√</td>
<td>0</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>7</td>
<td>Is there legislation/policy that requires (at least) an annual cyber-security audit?</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>8</td>
<td>Is there legislation/policy that requires a public report on cyber-security capacity for the government?</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>√</td>
<td>0</td>
<td>√</td>
<td>0</td>
<td>√</td>
</tr>
<tr>
<td>9</td>
<td>Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?</td>
<td>0</td>
<td>√</td>
<td>(MoICT guideline)</td>
<td>0</td>
<td>√</td>
<td>X</td>
<td>None</td>
<td>√</td>
</tr>
<tr>
<td>10</td>
<td>Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?</td>
<td>0</td>
<td>√</td>
<td>(MoICT&amp; national CERT)</td>
<td>0</td>
<td>√</td>
<td>0</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>11</td>
<td>Does legislation/policy include an appropriate definition for “critical infrastructure protection” (CIP)?</td>
<td>0</td>
<td>X (started 2014)</td>
<td>0</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>12</td>
<td>Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?</td>
<td>√</td>
<td>0</td>
<td>0</td>
<td>X (started)</td>
<td>0</td>
<td>No</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

**OPERATIONAL ENTITIES**

|   | Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)? | √ | √ | √ | √ | √ | None, but Philippine Cyber-crime Law R.A. 10175 requires one to be present. | √ | √ | √ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | What year was the computer emergency response team (CERT) established? | 2013 | 2007 | 3 Years | 1997 | 2004 | Not yet | 1998 | 2000 | 2005 |
| 3 | Is there a national competent authority for network and information security (NIS)? | ✓ | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| 4 | Is there an incident reporting platform for collecting cybersecurity incident data? | 0 | ✓ | 0 | ✓ | 0 | None. | ✓ | ✓ | ✓ |
| 5 | Are national cybersecurity exercises conducted? | 0 | ✓ | 0 | ✓ | 0 | Yes | ✓ | ✓ | ✓ |

Is there a national incident management structure (NIMS) for responding to cybersecurity incidents? 0 ✓ ✓ ✓ ✓ LaoCERT ✓ ✓ ✓

**PUBLIC PRIVATE PARTNERSHIPS**

| 1 | Is there a defined public-private partnership (PPP) for cyber-security? | 0 | 0 | 0 | X | X | Yes, first established between 2007-2009. | ✓ | ✓ | X (started) |
| 2 | Is industry organised (i.e. business or industry cyber-security councils)? | 0 | 0 | 0 | X (started) | X | To be started on 2016 | ✓ | No | X (started) |
| 3 | Are new public private partnerships in planning or underway (if so, which focus area)? | 0 | 0 | 0 | X | X | ✓ | ✓ | ✓ |

**SECTOR SPECIFIC CYBER-SECURITY PLANS**

| 1 | Is there a joint public-private sector plan that addresses cybersecurity? | 0 | 0 | 0 | ✓ | X | ✓ | ✓ | ✓ |
| 2 | Have sector specific security priorities been defined? | 0 | 0 | 0 | ✓ | X | ✓ | ✓ | ✓ |
| 3 | Have any sector cybersecurity risk assessments been conducted? | 0 | X (in banking sector) | 0 | ✓ | X | No | ✓ | ✓ | ✓ |

**EDUCATION**
<table>
<thead>
<tr>
<th></th>
<th>Is there an education strategy to enhance cyber-security knowledge and increase cyber-security awareness of the public from a young age?</th>
<th></th>
<th>0 (not yet nationally but initiated partially by higher education/university)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

### 10.2 The Analyses of EU Cyber-security Policy Dashboard

After sending the questionnaires, there are collections of Dashboards from Malaysia, Thailand, Indonesia, Philippines, Cambodia, Laos, Myanmar, Singapore and Vietnam. Based on those responses, in general, the report tells that most of ASEAN countries have the strategy on cyber security which were released around 5-7 years ago, except Laos and Cambodia still not yet, and Myanmar started the process. Among those ASEAN countries, the Cambodia, Laos and Myanmar seem to be less developed legislations and policy in security than other countries. Vietnam has much policy and strategy which leveled as started progress but the effectiveness and actual impact on reality is still a question mark. The case of Indonesia also seems to be lack behind a little comparing with other 4 ASEAN countries. The case of Malaysia seems to be the best countries in terms of cyber-security policy, regulation in ASEAN. It should be noted that Malaysia has been now ranked 3rd in the world in the 2014 Global Cybersecurity Index by ITU, the United Nations specialised agency for information and communication technologies – ICTs, and ranked the first in terms of cybersecurity preparedness in the ASEAN countries according to the same Index.

In the general results, the analyses gives that the legislation/policy for requirements of risk level assessment, the policy on procurement of cyber-security, the standardization based on international accreditation and public private partnership cooperation are still weak among those countries. Thus, EU can help to fulfill these weaknesses in terms of policy and legislations.

The item of requirements for public and private procurement of cyber-security solutions based on international accreditation or certification schemes, without additional local requirements seems to be popular at the higher developed countries. Meanwhile, the less developed countries like Cambodia, Vietnam tend to add several local requirements for cyber-security solutions based on international accreditation or certification schemes.

In cyber-security, the collection of cyber-security incident data is important factor, help to analyze and predict the threats in the future. However, in ASEAN, the countries with an incident reporting platform for collecting cyber-security incident data are still very few, among those 7 reported countries, up to 3 countries (Laos, Cambodia, Philippines) do not have the reporting platform for collecting data about incidents.

---


22 ITU, the United Nations specialised agency for information and communication technologies, is based on public-private partnership, currently has a membership of 193 countries and almost 800 private-sector entities and academic institutions. ITU is headquartered in Geneva, Switzerland, and has twelve regional and area offices around the world.
The operational entities also exist substantially among ASEAN countries. Most of ASEAN countries already have CERT organization. However, the common activities taken by cooperated CERT in ASEAN seems to be weak and need to improve more and more. Anyway, in the TELMIN event this year in 2015, the ASEAN CERT which was already established has plan to take several actions in order to improve the cooperation among CERTs within ASEAN region.

In ASEAN, the involvement of private sector such as joint public private sector plan that addresses cyber-security seems to be low levels in some countries such as Laos, Cambodia, and Indonesia. Vietnam although is less developed country in ASEAN but still work closer with private sector toward cyber-security.

Despite that overall legislations and regulation in cyber-security are mostly existed well in ASEAN. However, regarding the policy, it is surprised that the public private partnerships (PPP) model, which is popular in Europe and most of ASEAN countries, is not really of interest in Indonesia, Laos and Cambodia, even these countries lack of funding and resources for security improvement.

The involvement of entrepreneurships and industry orientation regarding cyber-security seems to be less organized well in the ASEAN state members, except the Malaysia case with better industry and policy close relationship.

The priorities and classified sectors according to the importance and risk of those sectors seem to be less interested in ASEAN countries. The sector cyber-security risk assessments been are also conducted less frequently. The Indonesia case is considering the banking sector as important in their economics. So they are interested to protect the banking sector and also conduct risk assessments on banking sector.

The rarely common issues which are highly interest by all ASEAN countries is education. The dashboard result shows that education in cyber-security was key point and highly interested and all 7 countries (except Laos) have policy to push human resources in this field of cyber-security.

In general, the questionnaires show us the industry and private involvement, the ASEAN cooperation, networking community, standardization, and public private partnership are among weak factors in ASEAN in terms of cyber-security.
11 ASEAN Cyber-security R&D Analysis

11.1 The R&D Cyber-security Dashboard

With the help from SCMIT members, the questionnaire about R&D cyber-security cooperation between Europe and ASEAN countries and between ASEAN countries is filled in.

*The number from 0 to 5 to answer the equivalent question as meanings below:*  
- **Implemented successfully:** 5  
- **Implementing well:** 4  
- **Implementing with difficulties** 3  
- **Planned:** 2  
- **Interested:** 1  
- **Not interested:** 0

<table>
<thead>
<tr>
<th>Table 3: ASEAN Cyber-security R&amp;D Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>I-1</td>
</tr>
<tr>
<td>I-2</td>
</tr>
<tr>
<td>I-3</td>
</tr>
<tr>
<td>I-4</td>
</tr>
<tr>
<td>I-5</td>
</tr>
<tr>
<td>I-6</td>
</tr>
<tr>
<td>I-7</td>
</tr>
<tr>
<td>II</td>
</tr>
<tr>
<td>II-1</td>
</tr>
<tr>
<td>II-2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>22</td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>III</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>25.</td>
</tr>
<tr>
<td>26.</td>
</tr>
<tr>
<td>27.</td>
</tr>
<tr>
<td>28.</td>
</tr>
<tr>
<td>29.</td>
</tr>
<tr>
<td>30.</td>
</tr>
<tr>
<td>31.</td>
</tr>
<tr>
<td>32.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV</th>
<th>Other additional R&amp;D Trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>New application of HPC applied to Big Data and Analytics to identify and clarify the vulnerabilities and threats in the Cloud?</td>
</tr>
<tr>
<td>34.</td>
<td>Quantum Key Distribution by Using Public Key Algorithm (RSA)?</td>
</tr>
<tr>
<td>35.</td>
<td>Application of quantum cryptography in wireless networks?</td>
</tr>
<tr>
<td>36.</td>
<td>The new Cyber threats in Internet of Things and Mobile devices?</td>
</tr>
</tbody>
</table>

### 11.2 Cyber-security R&D Dashboard Analyses

Right now, there are 7 collections of R&D Dashboards from Thailand, Singapore, Indonesia, Malaysia, Laos, Myanmar and Vietnam. The results come from survey can bring the overall view that most of ASEAN countries are still lack behind the R&D priorities of Horizon 2020 for case of cyber-security and other additional advanced R&D techniques.

In order to analyze the results of questionnaire, the report sees the each fill of each country as the point which shows the weight or level of progress and interest of respective R&D topic in that country. Then, the report summed all the points given by all ASEAN country to become the total points of ASEAN country, respective to each ASEAN country. Finally, the report sort all summed point of all ASEAN countries which replied the questionnaires. The
total point shows the highest interests of ASEAN country toward the R&D topic given in the respective questionnaire. The top 12 of R&D topic which have the highest marks (above 20 points) are presented in the Table below.

Table 4: Top 12 issues with highest points in ASEAN

<table>
<thead>
<tr>
<th>Order in Dashboard</th>
<th>Topic question</th>
<th>Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Secure Internet Use and Remote Access for Enterprise LAN and Private Cloud?</td>
<td>24</td>
</tr>
<tr>
<td>1</td>
<td>To identify new threats, vulnerabilities, risks and to implement the campaign to raise public awareness about cyber-security?</td>
<td>23</td>
</tr>
<tr>
<td>3</td>
<td>Cyber-security Architecture Framework, Standards and Guidelines for Enterprise and Government Office Cyber-security Policy</td>
<td>23</td>
</tr>
<tr>
<td>13</td>
<td>Disaster prevention and recovery after disaster</td>
<td>23</td>
</tr>
<tr>
<td>14</td>
<td>Development of new mechanisms, tools and techniques to increase trust, security and transparency of cloud infrastructures and services?</td>
<td>22</td>
</tr>
<tr>
<td>24</td>
<td>Provision of electronic signatures, e-seals, timestamps or certified electronic delivery in Trust eServices?</td>
<td>22</td>
</tr>
<tr>
<td>2</td>
<td>To find new enterprise solutions guaranteeing end-to-end security?</td>
<td>21</td>
</tr>
<tr>
<td>23</td>
<td>Proactive Security Systems able to counteract Denial of Service attacks in Critical Infrastructure?</td>
<td>21</td>
</tr>
<tr>
<td>15</td>
<td>Development of new software tools and methods for large, complex and data-intensive systems with high security?</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>Shared database of threat patterns and analytics of network logs to recognize the attack patterns</td>
<td>20</td>
</tr>
<tr>
<td>18</td>
<td>Cyber-security issues arisen in mobile e-government applications?</td>
<td>20</td>
</tr>
<tr>
<td>36</td>
<td>The new Cyber threats in Internet of Things and Mobile devices?</td>
<td>20</td>
</tr>
</tbody>
</table>

Looking into the Table of top 12 R&D topics above, the report can clarify top 12 R&D issues which are the highest interested by ASEAN countries. To make them more understandable and limit the scope of researches, the report finalizes 12 following topics for research priorities as below:

1. Developing and implementing the technology to secure Internet Use and Remote Access for Enterprise LAN and Cloud Computing, especially toward the Private Cloud
2. The researches and technologies to identify new threats, vulnerabilities, risks and techniques with low cost to implement the campaign to raise public awareness about cyber-security
4. Research the solutions for disaster prevention and effective procedures for recovery after disaster
5. Development of new mechanisms, tools and techniques to increase trust, security and transparency of cloud infrastructures and services
6. Development and provision of electronic signatures, e-seals, timestamps or certified electronic delivery in Trust eServices in ASEAN
7. Technologies and R&D projects in order to find new enterprise solutions guaranteeing end-to-end security, which can be controlled from designation until implementation processes.
8. Advanced researches on proactive Security Systems able to counteract DDoS (Denial of Service) attacks in Critical Infrastructure
9. Development of new software tools and methods for large, complex and data-intensive systems with high security. Research on cyber-security for Big Data and use Big Data to support the security researches
10. Shared database of threat patterns and analytics of network logs to recognize the attack patterns within ASEAN countries
11. Development and implementation of Cyber-security solutions to deal with the issues arisen in mobile e-government applications
12. R&D projects to cope up with the new Cyber threats in Internet of Things (IoT) and Mobile devices.

Among top 12 topics above, the report shows strong interests in security of new advanced R&D trends, such as Cloud Computing, Big Data, Internet of Things, Cryptography, e-Services. Despite of not high points, but by average points given by all ASEAN countries, the cryptography seems to be common technique where many countries have research on cryptography, or at least they are interested in cryptography. However, the advanced quantum cryptography seems still behind the schedule of ASEAN countries. One of the advanced country like Thailand, but it is not interested although the quantum cryptography is interested in Europe, especially in Horizon 2020.

From the survey, it can be seen that the Singapore seems to be the most advanced country in terms of R&D in cyber-security. All most all of topics in questionnaire are marked at high points, much rather than other countries. The Thailand is also advanced country in many topics of cyber-security in the questionnaire.
12 Lessons Learnt from the events organized by CONNECT2SEA project

12.1 Lessons learnt from Hanoi Workshop (December, 2015)

12.1.1 Summary of Hanoi Workshop

CONNECT2SEA project co-organised an international workshop (focus group) in Hanoi, Vietnam on December 3-5, 2015. The workshop has covered both cyber-security policy and R&D issues. With the participation of EU and SEA specialists the discussions have been focused on the information security related topics, and aimed at the following objectives:

- To set up an open discussion on new collaboration avenues in cyber security inside and outside ASEAN (in particular, with the European Union), in areas of common interest including research/technological/market trends, emerging opportunities for collaboration, barriers and ways to overcome them, etc.;
- To exchange good practice (both ASEAN and international) on the topics of common interest including the experience, vision and discuss the cooperation and project ideas;
- To develop recommendations and action proposals to the bodies in charge of cyber security (ICT RDI and Cyber Security Administration).

More than 40 specialists from Italy, Greece, Ireland, South Korea, Thailand, Laos, Malaysia, Philippines and many local experts from Vietnam’s Ministry of Information and Communication, Vietnam’s Software Association, Vietnam CERT, Vietnam’s CA participated in the workshop.

The first presentation in the workshop was on the ASEAN ICT Master Plan 2016 – 2020, which had been approved by all ASEAN ICT Ministers in Danang City of Vietnam just a week before the workshop. The speaker was a manager Ministry of Information and Communication of Vietnam, who was a member of the preparation team of the ASEAN ICT Master Plan 2016 – 2020.

From ASEAN side, there were some informative and fruitful presentations about R&D and policy in ASEAN. Dr. Chalee Vorakulpipat, Head of Cyber-security Lab. of NECTEC, Thailand delivered a speech on Cyber Security Policy, priorities and projects in Thailand. Mr. Ismamuradi, Head of Department Strategy Management, Cybersecurity Malaysia reported about Cyber Security Situation, Policy, strategy and solution given by government in Malaysia, one of the most advanced ASEAN country in cyber security. His presentation focused on what the Malaysian government has done so far against the situation, threats, solution and international cooperation for cyber security. Dr. Daovalath Phommalath, Department of Information Technology, Ministry of Science and Technology, Lao PDR shared about situation, activities and regulation on cyber-security in Lao PDR, one of the countries which are at beginning of ICT development. She also stated that Laos needs international cooperation in cyber security for ICT development.

From EU, there were four speakers, two of them are guest speakers and two members of CONNECT2SEA Consortium. Alessandro Guarino, the guest speaker from Studio AG, Italy, Expert of Technical Committee on Cybersecurity, ETSI – European Telecommunication
Standard Institute talked about Cyber Security in Europe: priorities, challenges and opportunities. The second guest speaker, James Clarke, from Telecommunications, Software & Systems Group (TSSG), Co. Waterford, Ireland, talked about building international cooperation for Cyber Security with a multi-lateral approach. Dr. Sotiris Ioannidis, a member of CONNECT2SEA from FORTH, Greece, talked about Priorities of Policy, Actions on Cybersecurity in Europe and Proposal for EU-ASEAN Cooperation in 2016 – 2020 and he also gave an introduction of European Horizon 2020 Work Programme 2016 - 2017: cybersecurity related research priorities.

Dr. Tran Quy Nam, Ministry of Information and Communications of Vietnam presented a talk about government policy and strategy for ICT in Vietnam including the situation, current status of Vietnamese cyber security and some suggestions for ASEAN – EU Cooperation on Security.

The workshop reserved half day for Dialogues by Roundtable Discussion with Representatives from Vietnam, Korea, European and ASEAN Guests on some topics, such as ASEAN Master Plan 2016 - 2020: Trust on Security, European Cyber Security and Opportunities Cooperation with ASEAN, ASEAN Committee on Cyber Security, LinkedIn Community,...

**12.1.2 Lessons learnt from Hanoi Workshop**

1. Opportunities to exchange the ideas about cooperation with participation both external experts and project team members will lead to useful suggestions, visions and implementation approaches to promote cooperation on cyber security.

2. The discussions help to improve the good results from the CONNECT2SEA Report. In particular the roundtable discussion on the specific question “What are next steps for cyber security collaboration (inside ASEAN and ASEAN-EU) under ICT ASEAN Master Plan 2016 - 2020 and Potential ASEAN – EU Projects proposals under Horizon 2020?” brought new ideas.

3. The participants agreed that human resources and R&D in cryptography are important topics for cooperation in cyber security.

4. The workshop also clearly determined that the actions of EU-ASEAN or ASEAN-Korea, or in each ASEAN country should follow the instruction and direction of ICT ASEAN Master Plan 2016 – 2020 that was recently approved by all ASEAN Ministers and will be the main direction for all ASEAN works in ICT for period of next 5 years.

5. Some suggestions, proposals and applications for Horizon 2020, working programme for 2016-2017 have been made and discussed but further results should be discussed further and can come out in Manila, Philippines. The all participants also agreed to think of how to register some new projects toward ASEAN – EU cooperation in ICT sector.

6. The cyber security has been and will be top important issues in any countries in next many years, from America, Europe to Asia, including ASEAN.

7. Key challenges in cyber security should be discussed frequently to find out the best solution to reduce the cyber threats in cyber space which is increasing rapidly day by day in over the world.
8. It was also agreed that the strong linkages and collaboration between industrial sectors, companies, enterprises to activities on advanced manufacturing and research institute, university must be established to protect the enterprise infrastructure effectively.

9. The pilot projects in cyber security should be implemented to transfer technology and technological knowledge between EU and ASEAN countries. The specific actions are needed which should benefit all partners.

10. The topics which can help all countries should be more specific, useful and feasible. One of the result that all participants know well each other and keep their contact of the CONNECT2SEA project team members as recorded and publish for all partners, including the Korean experts for advice, and to apply for the upcoming CONNECT2SEA call to initiate or to broaden ICT EU-SEA collaborations.

11. The LinkedIn Community of Practice in cyber security should be continued and will play important roles not only for CONNECT2SEA but also become a good networking for all experts in cyber security sector.

12. The topic of ICT human resource cooperation should be one of the key issues to promote on cooperation between EU and ASEAN.

12.2 Lessons Learnt from Manila Cybersecurity Forum (January 2016)

CONNECT2SEA organised the EU-SEA Cybersecurity Forum “International Cooperation for a Safer World” on January 26, 2016 in Manila, the Philippines, during the APAN Meeting (Asia-Pacific Advanced Network). It has more than 70 participants from EU and ASEAN countries. The forum aimed to assemble Asian and European researchers and ICT policy makers to discuss and exchange ideas and experiences on cybersecurity initiatives in their countries.

From the presentations by various experts from EU and SEA, the following lessons can be drawn:

1. The cooperation between the existing and extended partners in Cyber Security must be continued based on the existing and built working relationships. A list of R&D and projects must be established together with funding possibilities from each countries so other partners can participate

2. ITI-VNU and NECTEC continue to support the ASEAN ICT Master Plan team. We will keep the existing connection and try to find resources to do consulting works for the preparation team. The idea of ASEAN Cyber Security Body must be pushed further based on the current ASEAN CERT in the next version of the ASEAN ICT Master Plan.

3. ITI-VNU will continue to support the CoP even after the project. ITI-VNU can provide consulting works for countries like Laos, Cambodia and Myanmar to prepare the ICT master plan and Cyber Security Framework. The initial study is going carried out by CONNECT2SEA but there are some available resources in Vietnam, Korea for future extended works.
4. The key element might be Cyber Security Architecture where you can connect the policy with R&D and CIO. The standardization and reference models from EU can be used.

5. The national project experiences and opportunities can be shared to avoid double work and this is where the ASEAN side need European experts. Experience sharing should be done via some networks of professionals and academic institutions with a regional technical advisory committee.

6. A core “node” in SEA – organization acting on the national level - could act as regional catalyst for collaboration with EU organizations and be a gate (entry point) to other SEA countries. This is the first step toward building of the cybersecurity network in ASEAN. The organization should (1) be motivated to implement the “node” activities, supporting connections with other ASEAN countries, (2) have capacities and resources, and (3) have strong and recognized experience in cybersecurity.

7. The assessment framework for cyber security policy maturity of EU can be used for SEA.

8. A R&D map (directory) must be constructed constantly via a professional network.

9. Professional training and awareness promotion in cybersecurity is important and needs to be done.

10. Experience sharing should be done via some networks of professionals and academic institutions with a regional technical advisory body (committee).

At the Forum, the CONNECT2SEA team has also conducted an interactive session and a survey with the participants. The survey results demonstrate the following:

1. Top 10 threats (each participant can select top three threats) in the following order
   - Malwares
   - Identity threats
   - Privacy invasion
   - Web-banking Fraud/Attacks
   - DDOS
   - Unawareness
   - Cyberware/Cybercrime
   - APT
   - Phishing
   - IoT

2. Top 5 ways of cyber security promotion
   - Education-Training- Awareness
   - Advertisement
   - Research Project funding
   - ICT security policy
   - Incorporate in School-Academic Topics

3. 85% participants think that the cyber security investment in their organization is insufficient.

4. Top 5 cyber security investments the participants want to have
   - Training
   - Infrastructure
   - Core network
   - End point
5. 43% of participants think that the investment in cyber security in their organization is in good traction. 57% of them think otherwise.

6. 71% of participants think that the global cooperation in cyber security is insufficient

7. 73% of participants think that the existing legal framework is insufficient

8. Top 10 topics beside Cyber Security where collaboration between EU-SEA is the most needed are:
   - Big Data
   - Legal Framework
   - Training ICT experts
   - Computing/ICT
   - Disaster Management
   - Transportation
   - Robotics
   - Environment Protection
   - Infrastructure
   - Innovation

The full results of the interactive session organised at the Forum are given in the Annex B.
13 Conclusions

This document emphasizes the need for planned and sustained efforts in support of cyber-security research area. The report listed 144 details of EU Horizon 2020 which relating slightly or directly to cyber-security issues. The report also proposed an analysis the matrix of EU and ASEAN to find out 28 matches between both sides EU and ASEAN regarding cyber-security. Among those 28 matches, the report found 7 fully match EU Horizon 2020 and all 5 ASEAN countries.

Based on these 7 full matches, the report proposed 2 long-term projects involving the R&D and human resources development, namely “Promote Research and Development on Cryptography Technology and Application” and “Human Resources Exchanges on Cyber-security between EU and ASEAN” to promote further the cooperation between ASEAN and EU countries. In addition, the report also proposed other 5 common activities for the short-term cooperation which fit those 7 full matches to make some clear cooperation on cyber-security between EU and ASEAN.

In addition, the report made 2 questionnaires on R&D policy dashboard. The outcomes showed that the ASEAN countries were lack behind far from European countries. The topic about Big Data, Cloud Computing, Internet of Things, Cryptography, e-Services and projects with public private partnerships might be interested in ASEAN, especially in implementation of policy and human resources promotion and improvement.

The report identifies the similar and dissimilar areas where ASEAN and Europe are looking at, the synergies they can exploit playing to the respective strengths. The recommendations listed in the report are possible collaboration areas in the cyber-security area between the ASEAN countries and the EU.
14 References and Sources


### Annex A Table of Activities in EU Horizon 2020 related to Cyber-security

<table>
<thead>
<tr>
<th>EU</th>
<th>No</th>
<th>Details of Activities in Horizon 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future and Emerging Technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FET Open</strong></td>
<td>1</td>
<td>Encourages new high-potential actors &amp; high-tech SMEs</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Collaborative research and innovation actions in high-risk</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Research and innovation toward long-term vision</td>
</tr>
<tr>
<td>European Research Infrastructures, including e-Infrastructures</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EINFRA-5-2015 – Centres of Excellence for computing applications (includes PPP)</strong></td>
<td>4</td>
<td>Establishing some Centres of Excellence</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>High Performance Computing</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Public-Private Partnership (PPP)</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>More scientists and engineers be trained in the use</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Improved access to computing applications and expertise</td>
</tr>
<tr>
<td><strong>EINFRA-6-2014 – Network of HPC Competence Centres for SMEs</strong></td>
<td>9</td>
<td>Facilitate access and take-up by industry and in particular SMEs of HPC services.</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Awareness raising and visibility activities of the benefits of HPC for SMEs</td>
</tr>
<tr>
<td><strong>EINFRA-7-2014 – Provision of core services across e-infrastructures</strong></td>
<td>11</td>
<td>Digital Identifier e-infrastructure for digital objects</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Authentication and authorisation infrastructure (AAI)</td>
</tr>
<tr>
<td>Information and Communication Technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ICT 1 – 2014: Smart Cyber-Physical Systems</strong></td>
<td>13</td>
<td>Interconnected and collaborating including through the Internet of things</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Industrial strengths as well as exploring new markets</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Open, smart and co-operative CPS</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Facilitate users-suppliers partnerships across value chains and regions</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Next generation core ICT platforms with built-in security</td>
</tr>
<tr>
<td><strong>ICT 2 – 2014: Smart System Integration</strong></td>
<td>18</td>
<td>Heterogeneous integration of micro and nanotechnologies</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Smart systems are driven by industrial requirements</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Application specific are driven by users-requirements</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Collaboration for academia, research institutes and SMEs</td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Pre-commercial procurement action</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Surveying and coordinating the consideration of societal issues and users' requirements</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Increase awareness, education and training skills</td>
</tr>
<tr>
<td><strong>ICT 4 – 2015: Customised and low power computing</strong></td>
<td>25</td>
<td>Next generation servers, micro-server and highly parallel embedded computing systems</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>New cross-layer programming approaches</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>Establish reference architectures and platforms for customised low-power heterogeneous computing systems</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Connecting innovators across value chains</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>Higher involvement of SMEs, both on the supply and the demand-side</td>
</tr>
<tr>
<td>ICT 5 – 2014: Smart Networks and novel Internet Architectures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>30 Scientific publications, patents, new PhDs, and new open source software releases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31 Resolving legal issues arise from the interplay between the Internet and society</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32 Contributions to standards: IETF, IRTF may be targeted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33 Closer integration of datacom and telecom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34 Links with related International developments (US NSF Future Internet Architecture and similar programmes in Asia, notably Korea and Japan)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICT 7 – 2014: Advanced Cloud Infrastructures and Services</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>35 Develop infrastructures, methods and tools for high performance, adaptive cloud applications and services</td>
<td></td>
</tr>
<tr>
<td>36 Building strengths in telecoms and mobile infrastructures as well as software applications and services</td>
<td></td>
</tr>
<tr>
<td>37 New computational and data management models</td>
<td></td>
</tr>
<tr>
<td>38 High performance heterogeneous cloud infrastructures</td>
<td></td>
</tr>
<tr>
<td>39 Techniques for the deployment and management of federated and decentralised cloud infrastructures</td>
<td></td>
</tr>
<tr>
<td>40 Dynamic configuration, automated provisioning and orchestration of cloud resources</td>
<td></td>
</tr>
<tr>
<td>41 Facilitate collaboration between public administrations, users and other stakeholders</td>
<td></td>
</tr>
<tr>
<td>42 Mechanisms, tools and techniques to increase trust, security and transparency of cloud infrastructures and services</td>
<td></td>
</tr>
<tr>
<td>43 Allow on-line collaboration across different platforms and different technical environments for geographically dispersed teams</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICT 8 – 2015: Boosting public sector productivity and innovation through cloud computing services</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>44 Reduce the IT expenditure of the public sector</td>
<td></td>
</tr>
<tr>
<td>45 Improving the scope for flexible high-quality new services</td>
<td></td>
</tr>
<tr>
<td>46 Pre-commercial procurement for public sector cloud computing services (PCP)</td>
<td></td>
</tr>
<tr>
<td>47 Public procurement of innovative cloud computing solutions (PPI)</td>
<td></td>
</tr>
<tr>
<td>48 Enabling services to specific applications such as culture, businesses, tourism, education, health care, and cross-border intergovernmental systems</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICT 9 – 2014: Tools and Methods for Software Development</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>49 Software tools and methods for large, complex and data-intensive systems</td>
<td></td>
</tr>
<tr>
<td>50 Software architectures and tools for highly distributed applications</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICT 11 – 2014: FIRE+ (Future Internet Research &amp; Experimentation)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>51 Collaborative projects for the creation, reconfiguration and/or extension of Mobile and Wireless, Cloud, Spectrum, Photonics, Internet of Things (IoT), Distributed Service Platforms, Sensors</td>
<td></td>
</tr>
<tr>
<td>52 Experiments to manage, analyse and extract value from data acquired from sensors, mobile devices and/or online interactions in social and real networks</td>
<td></td>
</tr>
<tr>
<td>53 Develop the concepts of Experimentation-as-a-Service (EaaS) and Virtual Experimentation</td>
<td></td>
</tr>
<tr>
<td>54 Contribution to standardisation and interoperability of experimental facilities</td>
<td></td>
</tr>
<tr>
<td>55 Deployment of products, applications and services on the Future Internet</td>
<td></td>
</tr>
<tr>
<td>56 Online platforms with new services</td>
<td></td>
</tr>
<tr>
<td>57 Highly-visible and innovative web and mobile services and applications</td>
<td></td>
</tr>
<tr>
<td>58 Increasing user perceived quality of service, of experience and security</td>
<td></td>
</tr>
</tbody>
</table>
Future Internet

| 59 | Combination of software defined network implementations |
| 60 | Network security across multiple virtualised or SDN domains |
| 61 | Analysis of risks and vulnerabilities |
| 62 | Definition of threat models |
| 63 | Authentication mechanisms across multiple domains |
| 64 | Intelligence driven security and data analytics |

ICT 16 – 2015: Big data - research

| 65 | Industry-validated, user-defined challenges like predictions, and rigorous processes for monitoring and measurement. |

ICT 18 – 2014: Support the growth of ICT innovative Creative Industries SMEs

| 66 | Increase the market access of creative industries SMEs across borders |

ICT 30 – 2015: Internet of Things and Platforms for Connected Smart Objects

| 67 | Effective and efficient security and privacy mechanisms into devices, architectures, service and network platforms |
| 68 | Platforms for connected devices and objects |
| 69 | Integrated IoT systems and platforms |

ICT 32 – 2014: Cyber-security, Trustworthy ICT

<p>| 70 | Awareness and introducing new threats, vulnerabilities and risks |
| 71 | Find solutions guaranteeing end-to-end security |
| 72 | Solutions withstand progress for the lifespan of the application it supports, regardless of improvements in attacker hardware or computational capabilities |
| 73 | Popularise the found solutions |
| 74 | Automated security policy governance |
| 75 | Security-by-design for end-to-end security |
| 76 | Open and dynamically reconfigurable environments |
| 77 | User or provider has to rely on other providers |
| 78 | Decrease the security risks associated with improper use or misconfiguration |
| 79 | Allowing the user to trust devices and services intuitively |
| 80 | Hardware based real-time cryptography |
| 81 | Fully homomorphic cryptography |
| 82 | Distributed cryptography including functional cryptography |
| 83 | Cryptographic tools for securely binding applications to software, firmware and hardware environments |
| 84 | Post-quantum cryptography for long term security |
| 85 | Quantum key distribution (QKD) systems and networks for long-term security |
| 86 | Networks supporting information theoretic cryptographic primitives |
| 87 | Low cost components for short-distance, low-bit-rate quantum key-distribution |
| 88 | High-bit rate QKD systems that are tolerant to noise and loss |
| 89 | Project with increase in performance, or reduction in energy or power consumption |
| 90 | Taking into account the current trends in ICT like cloud, mobile, IoT, etc. |
| 91 | Provable security against physical attacks |
| 92 | Security certification for devices |
| 93 | Activities supporting the Cryptography Community |</p>
<table>
<thead>
<tr>
<th>Page</th>
<th>Ensure a durable integration involving academia, industry, law enforcement and defence agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>95</td>
<td>Technology watch, joint research agendas and foresight studies</td>
</tr>
<tr>
<td>96</td>
<td>Identify technology gaps</td>
</tr>
<tr>
<td>97</td>
<td>Solve training needs and skill shortage of academia and industry</td>
</tr>
<tr>
<td>98</td>
<td>Cryptographic protocols and algorithms</td>
</tr>
<tr>
<td>99</td>
<td>Dissemination and outreach, strengthening the link with institutional stakeholders</td>
</tr>
<tr>
<td>100</td>
<td>ICT products and services compliant with Europe’s security and privacy regulation</td>
</tr>
<tr>
<td>101</td>
<td>Increase user trust in ICT and online services</td>
</tr>
<tr>
<td>102</td>
<td>Improve users’ ability to detect breaches of security and privacy</td>
</tr>
<tr>
<td>103</td>
<td>Improved protection of the user’s privacy, in compliance with applicable legislation</td>
</tr>
<tr>
<td>104</td>
<td>Critical infrastructures and services</td>
</tr>
<tr>
<td>105</td>
<td>Provides security and privacy as a built-in feature</td>
</tr>
<tr>
<td>106</td>
<td>ICT solutions have compliance with the EU regulation</td>
</tr>
<tr>
<td>107</td>
<td>Simplify the implementation of cryptographic primitives</td>
</tr>
<tr>
<td></td>
<td>EU-Brasil</td>
</tr>
<tr>
<td></td>
<td>EU-Brazil Research and Development Cooperation in Advanced Cyber Infrastructure</td>
</tr>
<tr>
<td></td>
<td>EUB 1 – 2015: Cloud Computing, including security aspects</td>
</tr>
<tr>
<td>108</td>
<td>Joint research combining advanced Clouds and Big Data on Security</td>
</tr>
<tr>
<td>109</td>
<td>Activities address privacy, security and other Quality-of-Service issues in Cloud</td>
</tr>
<tr>
<td></td>
<td>EU-Japan</td>
</tr>
<tr>
<td></td>
<td>EU-Japan Research and Development Cooperation in Net Futures</td>
</tr>
<tr>
<td>110</td>
<td>Experimentation on developing and implementing Internet of Things and Smart ICT in Security issues</td>
</tr>
<tr>
<td>111</td>
<td>Innovative Smart ICT solutions for end-users (citizens, workers including home and mobile ones) in private or working environments</td>
</tr>
<tr>
<td></td>
<td>Nanotechnologies, Advanced Materials, Advanced Manufacturing and Processing, and Biotechnology</td>
</tr>
<tr>
<td></td>
<td>FoF 6 – 2014: Symbiotic human-robot collaborations for safe and dynamic multimodal manufacturing systems</td>
</tr>
<tr>
<td>112</td>
<td>Future human-robot-systems avoid any security attacks</td>
</tr>
<tr>
<td></td>
<td>FoF 8 – 2015: ICT-enabled modelling, simulation, analytics and forecasting technologies</td>
</tr>
<tr>
<td>113</td>
<td>Internet/Cloud world in cyber physical systems (CPS), multi-modal visualisation and interaction technologies</td>
</tr>
<tr>
<td>114</td>
<td>Innovative modelling, simulation, analytics and forecasting tools for manufacturing at large with security ensurance</td>
</tr>
<tr>
<td></td>
<td>FoF 9 – 2015: ICT Innovation for Manufacturing SMEs (I4MS)</td>
</tr>
<tr>
<td>115</td>
<td>Integration of Cyber-Physical-System modules in manufacturing processes and process chains in SMEs</td>
</tr>
<tr>
<td>116</td>
<td>Real-time response (application experiments) with addressing security and privacy issues</td>
</tr>
<tr>
<td></td>
<td>Innovation in SMEs</td>
</tr>
<tr>
<td>FP7/ICT/No 611014</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td><strong>INNOSUP 6 – 2015: Capitalising the full potential of online-collaboration for SME innovation support</strong></td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>Ensure security for assistance all online collaboration for innovation for SMEs</td>
</tr>
<tr>
<td>118</td>
<td>Ensure security for training modules established as web-based self- or collaborative learning modules for SMEs</td>
</tr>
<tr>
<td><strong>INSO-9-2015 - Innovative mobile e-government applications by SMEs</strong></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>Cyber-security issues arisen in mobile e-government applications by SMEs</td>
</tr>
<tr>
<td><strong>Societal Challenges - Secure, Clean and Efficient Energy</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LCE 6 – 2015: Transmission grid and wholesale market</strong></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Activities to increase transmission network flexibility, capacity and operational security (including resilience against disasters) based on Transmission and ICT technologies, including e.g. network synchronisation using European GNSS (global navigation satellite system)</td>
</tr>
<tr>
<td>121</td>
<td>Security in innovative use of ICT for smart grid services to be provided in an open and competitive electricity market</td>
</tr>
<tr>
<td><strong>LCE 7 – 2014: Distribution grid and retail market</strong></td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Security toward advanced ICT for optimising the energy storage systems</td>
</tr>
<tr>
<td>123</td>
<td>Enhance energy balancing, increased grid security and stability or improved grid congestion management via ICT</td>
</tr>
<tr>
<td><strong>LCE 8 – 2014: Local / small-scale storage</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LCE 10 – 2014: Next generation technologies for energy storage</strong></td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>Security in appropriate integration with next generation ICT tools for the control and management of electricity networks</td>
</tr>
<tr>
<td><strong>Smart, Green and Integrated Transport</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MG.7.1-2014. Connectivity and information sharing for intelligent mobility</strong></td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>Measures to improve and maximise the availability of transport data with security and privacy concerns</td>
</tr>
<tr>
<td>126</td>
<td>Security in communication network and solutions for real-time information exchange</td>
</tr>
<tr>
<td><strong>Climate Action, Environment, Resource Efficiency and Raw Materials</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SCS-16-2014: Making Earth Observation and Monitoring Data usable for ecosystem modelling and services</strong></td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>Security in ICT application</td>
</tr>
<tr>
<td>128</td>
<td>Security in provision of open and unrestricted access to interoperable ecosystem Earth Observation data and information</td>
</tr>
<tr>
<td><strong>Secure societies – Protecting freedom and security of Europe and its citizens</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DRS-12-2015: Critical Infrastructure Protection topic 1: Critical Infrastructure “smart grid” protection and resilience under “smart meters” threats</strong></td>
<td></td>
</tr>
<tr>
<td>129</td>
<td>Public Key Infrastructure (PKI) usage in Smart Grid</td>
</tr>
<tr>
<td>130</td>
<td>Security management schemes for Smart Grid that consists of millions of devices</td>
</tr>
<tr>
<td><strong>Call – Digital Security: Cyber-security, Privacy and Trust</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DS-1-2014: Privacy</strong></td>
<td></td>
</tr>
<tr>
<td>131</td>
<td>Data protection and privacy frameworks</td>
</tr>
<tr>
<td><strong>DS-2-2014: Access Control</strong></td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>Creation of commercial services making use of electronic identification and authentication</td>
</tr>
<tr>
<td><strong>DS-6-2014: Risk management and assurance models</strong></td>
<td></td>
</tr>
<tr>
<td>133</td>
<td>public-private platform (Network Information Security Platform)</td>
</tr>
<tr>
<td>134</td>
<td>Risk management framework encompass methods to assess and mitigate the risks in real time</td>
</tr>
<tr>
<td>DS-3-2015: The role of ICT in Critical Infrastructure Protection</td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>Identify new risks and vulnerabilities of ICT systems in critical infrastructures, including the communication networks, stem...</td>
</tr>
<tr>
<td>136</td>
<td>Strategies and methodologies for assessing criticalities of services and detecting anomalies due to ICT incidents</td>
</tr>
<tr>
<td>137</td>
<td>Proactive Security Systems able to counteract Denial of Service attacks</td>
</tr>
<tr>
<td>DS-4-2015: Information driven Cyber-security Management</td>
<td></td>
</tr>
<tr>
<td>138</td>
<td>Address the specific needs and security information of the end-user, private or public organisations</td>
</tr>
<tr>
<td>139</td>
<td>Assistance about information to the private sector (including SMEs) from national or sector-specific Cyber-security Centres or similar organisations</td>
</tr>
<tr>
<td>140</td>
<td>Establish and validate tools and techniques that will facilitate the management of internal and external information sources related to cyber-security management</td>
</tr>
<tr>
<td>DS-5-2015: Trust eServices</td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>Provision of electronic signatures, e-seals, timestamps or certified electronic delivery</td>
</tr>
<tr>
<td>142</td>
<td>Enhancing the trustworthiness of electronic transactions to reduce administrative overhead for citizens, businesses and facilitate higher availability of eGov services</td>
</tr>
<tr>
<td>DS-7-2015: Value-sensitive technological innovation in Cyber-security</td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>Developing ways to determine the relation between the perceived risks and benefits of new technologies</td>
</tr>
<tr>
<td>144</td>
<td>Identifying the key factors for promoting a secure and innovative ecosystem through fostering the creation of secure technologies in line with European values</td>
</tr>
</tbody>
</table>
Annex B  Manila EU-SEA Cybersecurity Forum survey

During the CONNECT2SEA Cybersecurity Forum which was collocated with the APAN41 conference, we organized an interactive session which was focused on 8 question related with Cyber Security and ICT in general. One of the targets of those questions was to identify the vision of the participants for possible collaboration opportunities between EU and ASEAN countries. The questions were prepared by the CONNECT2SEA consortium and will be presented in the next section of the present report. The participants were given colorful post-it notes and asked to write their opinion on them. Then, the notes were posted on poster boards and the CONNECT2SEA representative (moderator) led the discussion commenting and inviting comments on the post-it notes. From the answers we collected from the attendees we compiled some interesting graphs that will be presented within this report.

**Event Title** : Cybersecurity Forum: International Collaboration for a Safer World  
**Event Dates** : 26th of January 2016  
**Event Place** : Ground Floor, Ceremonial Hall, Marriot Hotel Pasay City, Philippines  
**Number of participants** : ~60  
**Countries participated** : Philippines, Vietnam, South Korea, Malaysia, Thailand, France, Germany, Greece, Myanmar, United Kingdom, China, Japan, Taiwan, The Netherlands, Indonesia, Pakistan, Singapore, India.

Question 1

**In your opinion, what are the top 3 threats that will be most relevant in the upcoming years?**  
The question received 46 answers. The participants responded with the top three threats that according to their opinion will be major in the upcoming years.
The results produced 36 different threats that are presented in Figure 3. The workshop attendees believe that malware, identity theft, privacy invasion and banking fraud will be present as major threats in the upcoming years (Figure ).
Questions 2

**Suggest 3 ways to promote Cyber Security in your respective countries?**

The question received 45 answers. The participants were requested to provide ways on how to promote the Cyber Security aspects in their own countries. The results presented 35 possible ways to promote Cyber Security (Figure ). Most of the participants agreed that the “education-training-awareness” is the most effective way to tackle that issue.
Ways of promoting Cyber Security

Education - Training - Awareness
Advertisement
Research Projects Funding
ICT security policies
Incorporate in School-Academic Topics
Building Infrastructure
Fight Against Cyber-Criminals
PKI
Regulation
Funding for SMB
Collaboration Activities
Advances Cyber-Security Implements
Cyber Laws
Money-Human-Time
Facebook-Yahoo-Google
Use of Proper Passwords
Trusted Networks
Industry-Academic-Government Linkages
Regular Dissemination
Appreciation of Leadership
Policy
Tought Email Push
LANuse Guidelines
Architecture
Cryptographic Schema
Forensic Analysis
Intrusion Detection
Country Self-Resilience
Conference
National Cyber-Security Masterplan
Better Software
Government Support
Advocacies
Free Internet Access
Digital Freedom

Figure 5 Ways on how to promote the Cyber Security
Figure 6 The top 10 answers regarding the ways of promoting Cyber Security

Questions 3

*What percentage of your organization budget is invested in Cyber Security? Do you think this is sufficient? Yes or No. (note type of organization)*

The question received 41 answers. Figure presents in details all the answers received in bar chart. The distribution of invested budget, according to the answers received is presented in Figure.
Regarding the question whether the budget invested is sufficient or not (within their organization), 85% of the answers mentioned that the budget is not enough while 15% of the answers mentioned that the budget is sufficient. The respective results can be seen in Figure.
As a last part of that question the participants had to declare their type of organization. 60% of the participants who answered that question belong to a public body (government) while 32% belong to academia (research organizations, universities) and 8% to other types of organizations (Figure ).

**Question 4**

*Where would you invest? Core network, end point, infra, training, etc.*

The question received 47 answers from the audience. Most of them claim that they would probably invest in training, infrastructure and the core network. One participant mentioned that would not invest anywhere and some other in the end point layer (e.g. antivirus).
Figure 11 The areas of investment in order to improve Cyber Security in bar chart

Figure presents the answers received in bars while Figure present the results in pie chart using percentages.

Figure 12 The areas of investment in order to improve Cyber Security in pie chart
Question 5

*Does your investment in Cyber Security have sufficient traction/is it a good investment? If not what should we do?*

The question received 44 answers. The results here were quite close. 57% claimed that their investment has sufficient traction while 43% claimed the opposite (Figure 13)

![Has your investment sufficient traction?](image)

Figure 13: Does your investment have sufficient traction?

Figure from the other side presents which areas organizations should focus in order to further improve their Cyber Security related investment.

![Which area to focus on to improve the cybersecurity related investment?](image)

Figure 14: Which area to focus on to improve the cybersecurity related investment?

120
Question 6

Is there a sufficient global collaboration on countering Cyber Security threats? If no, what are the steps to make it sufficient?

Questions 6 and 7 were focused on the legal aspect regarding the Cyber Security and the existing collaboration. Question 6 regarding the existing collaboration on countering the Cyber Security threats received 41 answers and the majority of the audience responded that there is no such sufficient global collaboration. (Figure).

![Pie chart showing the results of Question 6](image)

**Figure 15 Is the Cyber Security global collaboration sufficient?**

The participants provided the following list of possible actions to be taken for better global collaboration in Cyber Security.

- More Countries
- More Advertisement
- Annual event on every country
- Sharing resources
- Publish cyber security intelligence
- Share best practices
- Mentoring
- Knowledge sharing
- Training
- Global cybersecurity communities
- Information Sharing
- Make governments to understand risks of the threats

Question 7
Is the existing Legal Framework suitable and sufficient to address the changing nature of the Cyber Security landscape?

This question received 42 answers. 73% of the audience think that the existing legal framework is not sufficient to address the issues raised from continuously changing nature of the Cyber Security landscape. Only 7% of the participants claimed that the existing legal framework is enough (Figure).

The audience also commented on this question and responded that the existing legal framework is not enough, it is outdated and there should be further improvement in the law enforcement front.

Question 8

Other than Cyber Security what other ICT areas should SEA-EU collaborate on?
The last question of the interactive session received 35 answers. The audience was requested to identify other ICT areas where EU and ASEAN countries could collaborate. The audience provided a list of 43 different areas as presented in Figure 18.
We have isolated the top 10 of the above mentioned areas and the results are presented in Figure 19. Among other Big Data, Legal Frameworks and training of ICT experts are the areas that have been identified as promising for possible further EU-ASEAN collaboration.

Figure 19  Top 10: Other ICT areas for possible EU-ASEAN collaboration