



# Developing Cybersecurity Capacity

A proof-of-concept implementation guide

Jacopo Bellasio, Richard Flint, Nathan Ryan, Susanne Søndergaard,  
Cristina Gonzalez Monsalve, Arya Sofia Meranto, Anna Knack



For more information on this publication, visit [www.rand.org/t/RR2072](http://www.rand.org/t/RR2072)

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© Copyright 2018 RAND Corporation

RAND® is a registered trademark.

RAND Europe is a not-for-profit organisation whose mission is to help improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

#### Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit [www.rand.org/pubs/permissions](http://www.rand.org/pubs/permissions).

#### Support RAND

Make a tax-deductible charitable contribution at  
[www.rand.org/giving/contribute](http://www.rand.org/giving/contribute)

[www.rand.org](http://www.rand.org)

[www.rand.org/randeurope](http://www.rand.org/randeurope)

## Preface

---

This report constitutes the second output of a project commissioned by the United Kingdom (UK) Foreign and Commonwealth Office (FCO), under which RAND Europe was tasked with developing a proof-of-concept operational toolbox to facilitate the development of national-level cybersecurity capacity. This project was financed through the UK FCO Cyber Security Capacity Building Programme.

The purpose of the toolbox is to support countries in their efforts to develop holistic policy and investment strategies to tackle the complex challenges they face in the cyber domain. In particular, the project seeks to enable a better translation of the results of national cyber maturity reviews and assessments into tangible policy recommendations and investment strategies, allowing policymakers to develop their countries' cybersecurity capacity.

This project comprised two main research and development phases. The first phase of the project entailed a requirements analysis and architecture-design effort. For further details on this phase, please refer to the first study report. The second phase of the project entailed the development of a proof-of-concept toolbox. This report presents the proof-of-concept toolbox.

RAND Europe is an independent not-for-profit policy research organisation that helps to improve policy and decision making through research and analysis. RAND Europe's clients include European governments, institutions, non-governmental organisations and firms with a need for rigorous, independent, multidisciplinary analysis. This report has been peer-reviewed in accordance with RAND's quality-assurance standards.

For more information about this study or this report, please contact:

Giacomo Persi Paoli

Research Leader, Defence, Security and Infrastructure  
RAND Europe  
Westbrook Centre, Milton Road  
Cambridge CB4 1YG  
United Kingdom  
Tel. +44 (1223) 353 329  
[gpersipa@rand.org](mailto:gpersipa@rand.org)



# Table of contents

---

Preface .....	iii
Table of contents.....	v
Figures .....	vii
Tables .....	ix
Boxes .....	xi
Acknowledgements .....	xiii
Abbreviations .....	xv
<b>Introduction.....</b>	<b>1</b>
1.1. The role of cybersecurity in contemporary society .....	1
1.2. About this study.....	2
1.3. How to use this guide.....	4
<b>Dimension 1 – Cybersecurity policy and strategy.....</b>	<b>11</b>
D1.1 – National cybersecurity strategy .....	12
D1.2 – Incident response.....	14
D1.3 – Critical infrastructure protection.....	30
D1.4 – Crisis management .....	43
D1.5 – Cyber defence.....	52
D1.6 – Communications redundancy.....	63
<b>Dimension 2 – Cyber culture and society.....</b>	<b>69</b>
D2.1 – Cybersecurity mindset .....	70
D2.2 – Trust and confidence on the Internet.....	76
D2.3 – User understanding of personal information protection online .....	86
D2.4 – Reporting mechanisms.....	93
D2.5 – Media and social media .....	99
<b>Dimension 3 – Cybersecurity education, training and skills .....</b>	<b>105</b>
D3.1 – Awareness raising.....	106
D3.2 – Framework for cybersecurity education.....	116

D3.3 – Framework for professional training .....	125
<b>Dimension 4 – Legal and regulatory frameworks .....</b>	<b>137</b>
D4.1 – Legal frameworks.....	138
D4.2 – Criminal justice system .....	145
D4.3 – Formal and informal cooperation frameworks to combat cybercrime .....	155
<b>Dimension 5 – Standards, organisations and technologies .....</b>	<b>165</b>
D5.1 – Adherence to standards .....	167
D5.2 – Internet infrastructure resilience.....	178
D5.3 – Software quality .....	187
D5.4 – Technical security controls.....	193
D5.5 – Cryptographic controls .....	197
D5.6 – Cybersecurity marketplace .....	206
D5.7 – Responsible disclosure .....	212
<b>Resources and publications.....</b>	<b>225</b>
D1.Cybersecurity policy and strategy .....	226
D2.Cyber culture and society .....	234
D3.Cyber security education, training and skills.....	239
D4.Legal and regulatory frameworks .....	246
D5.Standards, organisations and technologies .....	251
Full reference list .....	261
Document endnotes .....	285

# Figures

---

Figure I.1: GCSCC CMM structure .....	3
Figure I.2: Toolbox function within a GCSCC CMM-enabled cybersecurity capacity-building cycle.....	4
Figure I.3: Document template for ‘Capacity-building steps’ .....	5
Figure I.4: Document template for ‘Specific guidance’ .....	6
Figure I.5: Document template for ‘Things to watch out for’ .....	6
Figure I.6: Document template for ‘Case study’ .....	6
Figure I.7: Document template for ‘Additional resources’ .....	7
Figure 1.1: Overview of a minimum design for a CSIRT network architecture.....	23
Figure 1.2: Example of an incident response process.....	24
Figure 1.3: An example incident-handling checklist.....	26
Figure 1.4: CIIP represented as the crossover between CIP and cybersecurity.....	31
Figure 1.5: Defining critical information infrastructure .....	37
Figure 1.6: Components of a national-level risk assessment .....	39
Figure 1.7: Example of a risk profile.....	39
Figure 1.8: Example of a risk profile.....	40
Figure 1.9: Exercise and evaluation cycles.....	50
Figure 1.10: Basic framework for a cyber doctrine .....	61
Figure 1.11: Basic crisis communication channels .....	64
Figure 3.1: Examples of different target audiences at varying degrees of granularity .....	109
Figure 3.2: A visual framework of cybersecurity career paths .....	129
Figure 4.1: Information sharing in the international fight against cybercrime .....	156
Figure 5.1: Risk assessment steps for CNI-IT .....	182
Figure 5.2: DevOps showing the intersection of software development, operations and quality assurance.	187
Figure 5.3: Hierarchy of cryptographic controls .....	198



## Tables

---

Table 1.1: Typical operational-technical services offered by a CSIRT .....	20
Table 1.2: UK criticality scale for infrastructure .....	36
Table 1.3: List of CII sectors in Japanese strategic documentation.....	38
Table 1.4: Advantages and disadvantages of action-based and discussion-based exercises .....	46
Table 3.1: Examples of metrics for success.....	113
Table 3.2: Cybersecurity education target audiences and associated educational aims .....	119



## Boxes

---

Box 1.1: Steps for building a national cybersecurity strategy (D1.1) .....	13
Box 1.2: Steps for building incident response capacity (D1.2) .....	14
Box 1.3: Steps for building critical infrastructure protection (D1.3) .....	31
Box 1.4: Steps for building crisis-management capacity (D1.4) .....	43
Box 1.5: Steps for increasing cyber defence consideration (D1.5) .....	52
Box 1.6: Steps for improving communications redundancy (D1.6) .....	65
Box 2.1: Steps for improving the cybersecurity mindset (D2.1) .....	70
Box 2.2: Steps for increasing trust and confidence on the Internet (D2.2) .....	77
Box 2.3: Steps for improving user understanding of personal information protection online (D2.3).....	87
Box 2.4: Steps for improving reporting mechanisms (D2.4) .....	93
Box 2.5: Steps for facilitating the development of a healthy media and social media (D2.5) .....	99
Box 3.1: Steps for improving cybersecurity awareness-raising capacity (D3.1) .....	106
Box 3.2: Steps for developing a national framework for cybersecurity education (D3.2) .....	116
Box 3.3: Steps for improving the framework for professional training in cybersecurity-related areas (D3.3) .....	125
Box 4.1: Steps for developing legal frameworks' capacity to tackle cyber-enabled crimes (D4.1) .....	139
Box 4.2: Steps for developing a criminal justice system's capacity to tackle cyber-enabled crimes (D4.2) .....	146
Box 4.3: Steps for developing or joining formal and informal cooperation mechanisms to combat cybercrime (D4.3) .....	155
Box 5.1: Steps for increasing national adherence to ICT standards (D5.1) .....	167
Box 5.2: Steps for improving Internet infrastructure resilience (D5.2).....	178
Box 5.3: Steps for improving software quality (D5.3) .....	188
Box 5.4: Steps for increasing technical security controls capacity (D5.4).....	193
Box 5.5: Steps for improving cryptographic control capacity (D5.5) .....	198
Box 5.6: Steps for improving cybersecurity marketplace capacity (D5.6) .....	206
Box 5.7: Steps for increasing responsible disclosure capacity (D5.7) .....	212



## Acknowledgements

---

This project could not have been conducted without the funding provided by the UK FCO Cyber Security Capacity Building Programme. At the UK FCO, particular thanks go to Robert Collett and Patrick Mulcahy for their active engagement, constructive feedback and facilitation of contacts throughout the project. Particular thanks also go to the Oxford Global Cyber Security Capacity Centre, and in particular to Professor Paul Cornish and Lara Pace, for their help, support, and constructive feedback provided from the inception to the completion of this project. The authors are also grateful to RAND Europe's Alexandra Hall and Erik Silfversten for their guidance and constructive criticism provided in their quality-assurance roles. Finally, and not least, the authors would like to thank and acknowledge the interviewees and workshop participants who gave the project their time and who provided valuable information and insights for its delivery, including stakeholders and experts from the UK Cabinet Office, the Commonwealth Telecommunications Organisation, the International Telecommunication Union, the Organization of American States, the World Bank and the Potomac Institute for Policy Studies.



## Abbreviations

---

ACORN	Australian Cybercrime Online Reporting Network
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APCERT	Asia Pacific Computer Emergency Response Team
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAE	Centers of Academic Excellence in Cyber Security
CCFP	Certified Cyber Forensics Professional
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CISA	Communications and Information Systems Agency
CiSP	Cyber Security Information Sharing Partnership
CMM	Capacity Maturity Model
CNI	Critical National Infrastructure
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organisation
CTO	Commonwealth Telecommunications Union
CVSS	Common Vulnerability Scoring System
DCPP	Defence Cyber Protection Partnership
DCS	Defence Cyber School
DCU	Digital Crimes Unit

DDoS	Distributed Denial of Service
DefCERT	Defence Computer Emergency Response Team
DHS	Department of Homeland Security
DISS	Netherlands Defence Intelligence and Security Service
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
Dstl	Defence Science and Technology Laboratory
EC-Council	International Council of E-Commerce Consultants
ECIH	EC-Council Certified Incident Handler programme
ECSM	European Cyber Security Month
ENISA	European Network and Information Security Agency
EU	European Union
FCO	Foreign and Commonwealth Office
FINRA	Financial Industry Regulatory Authority
FIRST	Forum of Incident Response and Security Teams
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GASF	GIAC Advanced Smartphone Forensics
GCFE	Global Information Assurance Certification Forensic Examiner
GCHQ	Government Communications Headquarters
GCIH	GIAC Certified Incident Handler
GCSCC	Global Cyber Security Capacity Centre
GDPR	General Data Protection Regulation
GDS	Government Digital Service
GIAC	Global Information Assurance Certification
GIS	Geographic Information System
GNFA	GIAC Network Forensic Analyst
GRID	GIAC Response and Industrial Defense

HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IAPP	International Association of Privacy Professionals
IC3	Internet Crime Complaint Center
IANA	Internet Assigned Number Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control System
ICS2	International Information Systems Security Certification Consortium
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE-SA	Institute of Electrical and Electronics Engineers Standards Association
IETF	Internet Engineering Task Force
IGCI	INTERPOL Global Complex for Innovation
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union (ITU) – Telecommunication Standardization Sector (ITU-T)
ITWAC	Information Technology Workforce Assessment for Cybersecurity
JIMC	Joint Information Management Command
KPI	Key Performance Indicator
LE	Let's Encrypt
MLAT	Mutual Legal Assistance Treaty
MOD	Ministry of Defence
MOOC	Massive Open Online Course
NATO	North Atlantic Treaty Organization
NATO CCDCOE	Cooperative Cyber Defence Centre of Excellence

NCSA	National Cyber Security Alliance
NCSAM	National Cyber Security Awareness Month
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NGO	Non-Governmental Organisation
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NorSIS	Norwegian Centre for Information Security
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
OSM	Online Social Media
PEST	Political, Economic, Socio-cultural and Technological
PGP	Pretty Good Privacy
POC	Point of Contact
PPP	Public-Private Partnership
QA	Quality Assurance
R&D	Research and Development
RCCC	Regional Cybersecurity Centre
RMF	Risk Management Framework
SaaS	Software as a Service
SDG	Sustainable Development Goals
SDO	Standards Developing Organisation
SMART	Specific, Measurable, Achievable, Realistic and Time-bound
SME	Small and Medium Enterprise
SQM	Software Quality Management
SSL	Secure Sockets Layer
SWOT	Strengths, Weaknesses, Opportunities and Threats
TF-CSIRT	Task Force-CSIRT
TLS	Transport Layer Security

UK	United Kingdom
UNCTAD	United Nations Conference on Trade and Development
UN-GGE	United Nations Group of Governmental Experts
US	United States
US-CERT	US Computer Emergency Readiness Team
VEP	Vulnerability Equities Process
VoIP	Voice-Over-IP
WB	World Bank
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access



# Introduction

---

## 1.1. The role of cybersecurity in contemporary society

The role played by information communication technologies (ICTs) and by the networks they generate and underpin has continuously increased throughout recent decades. From an economic perspective, the potential positive impact of the Internet and ICTs on growth and development is now widely recognised.<sup>1</sup> However, the growth and increasing global penetration of ICT, and the cloak of immunity and anonymity that these technologies can provide, have led to a growth in illicit activities across cyberspace – this being the label used to describe the environment formed by physical and non-physical components, characterised by the use of computers and the electro-magnetic spectrum to store, modify and exchange data using computer networks. The development of phenomena such as cyber-enabled crime, espionage and terrorism, and the resulting need to protect ICT-dependent critical national infrastructure, have led more and more countries to adopt and implement a national cybersecurity strategy (NCSS). The adoption of a NCSS is intended to ensure a nationally coherent approach to securing the cyber domain, tackling risks and reducing threats which might otherwise offset the socio-economic gains made through ICTs.

The cyber domain is characterised by complex, transnational interconnections and the functional interdependence of actors and components on a global level. In light of this, a country's ICT-enabled prosperity and wellbeing is becoming more and more dependent on the security and resilience of networks located well beyond its national borders and jurisdiction. Simply put, no one nation can adequately secure its networks and network-dependent infrastructure independently.<sup>2</sup> For this reason, international cooperation and diplomatic efforts aimed at building a shared understanding of cyber issues and spurring common action on these matters have flourished in recent years. Furthermore, a number of institutions and organisations operating in the cybersecurity and international development spheres have put considerable effort into assisting countries with low levels of cybersecurity maturity in the development of their national capacity and resilience.

To help countries ensure that investments in national cybersecurity are as effective, efficient and sustainable as possible, a number of methodological frameworks have been created to help decision making in this sphere. One example of this is the development by different international actors of frameworks and models designed for assessing capacity and identifying areas for targeted capacity-building activities. These tools enable decision makers to perform a review and assessment of national or sectoral cybersecurity capacity, identifying areas for development prior to the allocation of resources.<sup>3</sup> Existing frameworks and models employ different research and analytical approaches for collecting and making

sense of data, as well as for presenting their recommendations to stakeholders seeking to improve their national cybersecurity capacity.

## 1.2. About this study

As part of its Cyber Security Capacity Building Programme, the UK FCO commissioned RAND Europe in May 2016 to develop a proof-of-concept operational toolbox to facilitate the development of national-level cybersecurity capacity. The purpose of this toolbox is to help countries develop holistic policy and investment strategies to tackle the complex challenges they face in the cyber domain. In particular, the toolbox is intended to enable a better translation of the results of national cyber maturity assessments and reviews into tangible policy recommendations and investment strategies, allowing policymakers to develop their countries' cybersecurity capacity.

This project comprised two main research and development phases. The first phase of the project entailed a requirements analysis to inform the structure and content of the toolbox. The requirements analysis work focused on identifying the challenges, opportunities and needs faced by policymakers and implementers operating in cybersecurity capacity development. Data gathered through this exercise informed the efforts to formalise the structure and content of the toolbox. The second phase of the project entails the development of the proof-of-concept toolbox, providing guidance to national-level governmental policymakers and decision makers tasked with leading and coordinating cybersecurity capacity-building efforts across different issues within a country.<sup>4</sup> As different national contexts involve different institutional configurations with respect to responsibility for leading cybersecurity capacity-building activities, the recommendations of the toolbox are geared towards generic senior decision makers and authorities without further specification.

### 1.2.1. *The Global Cyber Security Capacity Centre Capacity Maturity Model*

A model that has emerged and achieved considerable success in the cybersecurity capacity-development field is the Cybersecurity Capacity Maturity Model for Nations (CMM), which was created by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford,<sup>5</sup> and funded by the UK FCO's Cyber Security Capacity Building Programme. This tool has gained traction among practitioners thanks to its deployment in a number of countries and regions by international organisations such as the Organization of American States (OAS), the World Bank (WB), the International Telecommunications Union (ITU) and the Commonwealth Telecommunications Union (CTO).

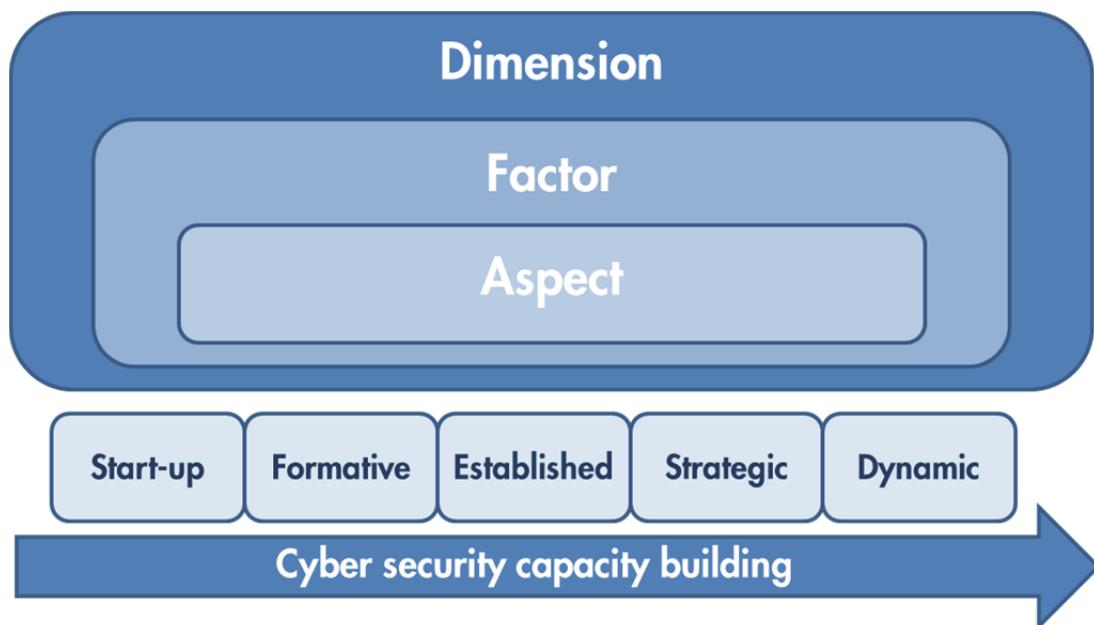
The first version of the GCSCC CMM was published in 2014, and an updated version was released in 2017.<sup>6</sup> According to the GCSCC CMM, a national cyber ecosystem can be considered to comprise five dimensions:

1. D1 – Cybersecurity policy and strategy
2. D2 – Cyber culture and society
3. D3 – Cybersecurity education, training and skills
4. D4 – Legal and regulatory frameworks
5. D5 – Standards, organisations and technologies.

Within each dimension, the CMM identifies various *factors*, which describe what it means to possess cybersecurity capacity. Each factor is characterised by a number of *aspects*, which further detail the different components comprised within a particular niche of cybersecurity capacity.

Each dimension, factor and aspect of the GCSCC CMM is further structured along five stages of maturity. These are used to help countries determine their current level of capacity. From lower to higher, the levels of maturity within the GCSCC CMM are as follows: start-up; formative; established; strategic; dynamic. Figure I.1 provides a visual overview of the structure of the GCSCC CMM.

**Figure I.1: GCSCC CMM structure**



SOURCE: RAND Europe elaboration based on GCSCC (2017)

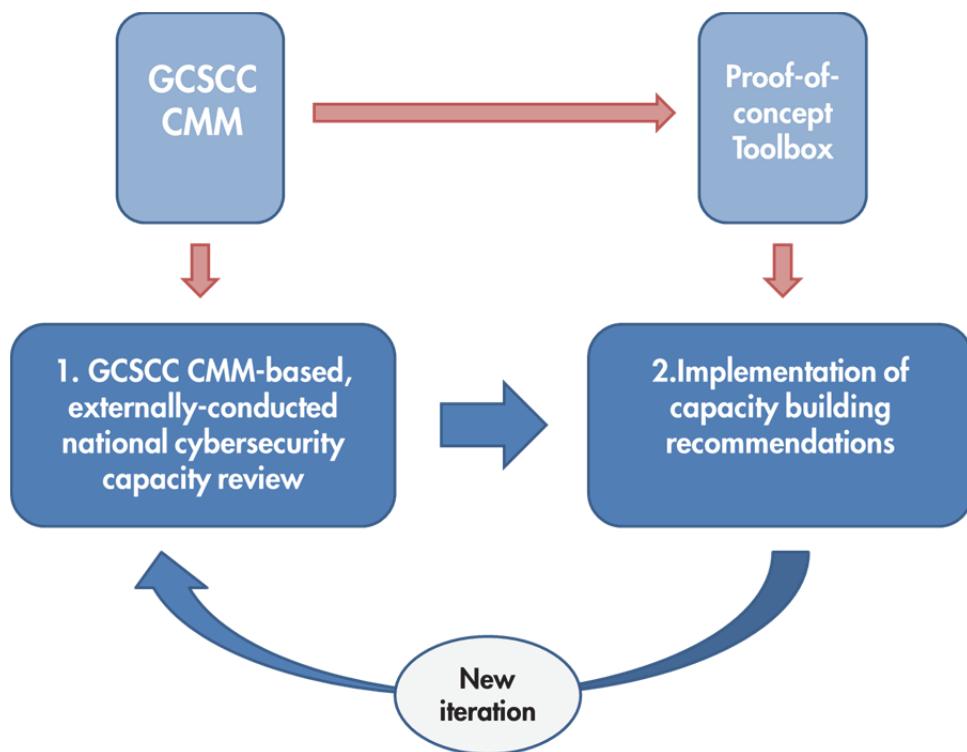
The GCSCC CMM has been used in several countries across the globe in support of expert appraisal of national cybersecurity capacity. In the context of these activities, the GCSCC CMM dimensions and overall structure have been successfully used for mapping issues at stake in a national cyber ecosystem, tracking capacity in a range of different issue areas, and providing recommendations for future developments and investments. However, the tool is not designed to be used by policymakers and implementers as a reference guide to be consulted when devising policies or activities aimed at operationalising recommendations stemming from a review of national cybersecurity capacity.

The present toolbox was designed to provide policymakers and decision makers with such an instrument, facilitating the operationalisation of recommendations generated through a capacity review report completed using the GCSCC CMM. As such, this project uses the GCSCC CMM as its reference framework for structuring its overall understanding of a national cyber ecosystem and of existing guidelines for cybersecurity capacity development.

### 1.3. How to use this guide

This document serves as a cybersecurity capacity-building proof-of-concept toolbox. The proof-of-concept toolbox presents guidelines and recommended approaches as identified through a review of existing literature for cybersecurity capacity building. The document would be best used to act upon the results and the capacity-building recommendations generated following a review of national cybersecurity capacity conducted by external experts employing the GCSCC CMM. Figure I.2 provides a visual overview of the intended purpose of this proof-of-concept toolbox within a broader GCSCC CMM-based cybersecurity capacity-building cycle.

**Figure I.2: Toolbox function within a GCSCC CMM-enabled cybersecurity capacity-building cycle**



The guide can be used as a standalone support document by government officials and cybersecurity practitioners working on developing national cybersecurity capacity. However, previous research indicates that the advice of external cybersecurity experts with experience of facilitating national cybersecurity capacity building should be sought, particularly by countries and stakeholders with limited knowledge and understanding of the issues at stake.<sup>7</sup>

### *1.3.1. Structure of the document*

The chapters of this document build on the approach of the GSCC CMM and are structured around the five dimensions of the model:

- D1 – Cybersecurity policy and strategy
- D2 – Cyber culture and society
- D3 – Cybersecurity education, training and skills
- D4 – Legal and regulatory frameworks
- D5 – Standards, organisations and technologies.

Within the dimension-specific chapters, the document presents a series of capacity-building steps to be followed to develop national capacity for each of the factors set out by the GSCC CMM in that dimension. Steps are presented in a logical, sequential order of implementation. However, the approach taken to discussing capacity-building activities was designed to retain sufficient flexibility to allow readers to browse through different steps independently and according to context-specific considerations, interests and aspirations.

For each capacity-building step, the document provides guidance on implementation, emphasising specific approaches and known challenges to capacity building identified through the existing literature, and presenting relevant real-life examples through case studies. Figures I.3 to I.6 provide an overview of the templates used throughout the document to highlight capacity-building steps, specific implementation guidance, disclaimers about challenges and pitfalls, and case studies.

**Figure I.3: Document template for ‘Capacity-building steps’**



#### **➤ Capacity-building step**

These boxes present factor-specific capacity-building steps.

e.g. ‘Establish a national-level Computer Security Incident Response Team (CSIRT) with responsibility for incident response at the national level.’

Figure I.4: Document template for 'Specific guidance'



#### Specific guidance

These boxes provide specific guidance on how to implement or address a particular aspect of a recommended capacity-building step.

e.g. 'The process of identifying stakeholders to be engaged by a newly established national CSIRT can take the form of a brainstorming session, facilitated through the employment of strategic planning tools such as a Strengths, Weaknesses, Opportunities and Threats (SWOT) or a Political, Economic, Socio-cultural and Technological (PEST) analysis. To ensure an inclusive and representative process, members of different agencies and stakeholder groups should take part in the brainstorming and planning phase of a national CSIRT.'

Figure I.5: Document template for 'Things to watch out for'



#### Things to watch out for

These boxes discuss known risks or pitfalls to watch out for during the implementation of a particular capacity-building step or initiative.

e.g. 'The selection of capabilities and services to be offered by a CSIRT is extremely important, as these define the resources, skills and partnerships required for the CSIRT to fulfil its designated function. The services provided by the CSIRT should be consistent with the formal capability and mandate of the team, and should be defined such that they can realistically be provided using the available resources. The success of a CSIRT is largely measured by the quality of service provided.'

Figure I.6: Document template for 'Case study'



#### Case study

These boxes present short case studies discussing real-life examples of the issues, policies or initiatives discussed under a given capacity-building step.

e.g. 'Task Force (TF)-CSIRT. The TF-CSIRT is an internal taskforce that promotes collaboration between CSIRTS in Europe. The main goals of the TF-CSIRT include: (i) providing a forum for exchanging experiences and knowledge; (ii) establishing pilot services for the European CSIRT community; (iii) promoting common standards and procedures for responding to security incidents; and (iv) assisting the establishment of new CSIRTS and the training of CSIRT staff.'

Following the discussion of recommended capacity-building steps and their accompanying guidance, for each factor the document provides the details of relevant publications and resources that readers wishing to undertake further reading may consult. Figure I.7 provides an overview of the template used for presenting factor-specific resources.

**Figure I.7: Document template for 'Additional resources'**



**Additional resources**

These boxes provide details of relevant publications and resources that readers may consult to further their knowledge and understanding of capacity building within a given cybersecurity issue area.

e.g. Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell & Elizabeth Phillips. 2014. Computer Security Incident Response Teams (CSIRTs): An Overview. Oxford: Global Cyber Security Capacity Centre.

ENISA (European Union Agency for Network and Information Security). 2006. A step-by-step approach on how to set up a CSIRT.

ENISA. 2014. National/governmental CERTs: ENISA's recommendations on baseline capabilities. Heraklion, Greece: ENISA

OAS (Organization of American States). 2015. Best Practices for Establishing a National CSIRT. Heraklion, Greece: ENISA

Lastly, following the dimension-specific chapters, the document presents a list of resources and references that were used to compile this guide and may be consulted during capacity-building activities to further knowledge and understanding of different issue areas.

### *1.3.2. Limitations*

Readers and users of the guide should be aware of the limitations of this document. This guide was compiled between January and May 2017 on the basis of a review and synthesis of publicly available academic and grey literature on cybersecurity capacity building. Literature for review was identified through a snowballing technique (a technique whereby additional studies and resources are identified through studies and resources reviewed) rather than through a systematic review approach, and was limited to publications available in the English language.

The recommendations and approaches presented in the following chapters stem from an analysis of the documents reviewed and referenced in this document's endnotes. While the document constitutes a fair representation of what was identified in the literature as 'state-of-the-art' in cybersecurity capacity building at the time of drafting this guide, cybersecurity remains a dynamic field, characterised by a fast-changing threat landscape and influenced by continuous technological developments. As such, stakeholders and implementers seeking to build national cybersecurity capacity should ensure that their use of this guide is complemented with any updated guidance or expertise relevant at the time of use. Further, due to the emerging nature of cybersecurity, it was not possible to identify any recommended approaches or practices for a number of developing issue areas and aspects that are otherwise comprised and covered in the GSCC CMM, upon which this document is based.

In addition, as different national contexts entail different institutional configurations as regards responsibility for leading cybersecurity capacity-building activities, the recommendations of this toolbox are geared towards generic senior decision makers and authorities without further specification. The toolbox was written with the assumption that adequate political, resource and budgetary support would be available for the implementation of the suggested capacity-building guidelines. The document does not

discuss recommendations for advancing cybersecurity from the perspective of other stakeholders that should be involved in such efforts (e.g. general public).

Finally, this document ambitiously attempts to provide recommendations for capacity-building initiatives across a wide array of cybersecurity-related issue areas. As such, due to the breadth of its approach and the inherent time and resource constraints of the project underpinning its production, a number of relevant issue areas, both emerging and established, are not discussed by this report in the depth and detail they would merit. Examples include laws on cyber-related privacy, freedom of speech, human rights, data protection, child protection, consumer protection, and intellectual property. The resources and tools referenced at the end of each section are meant to provide readers interested in broadening their knowledge of a particular topic discussed in the report with useful indications for their exploration of the matter at hand.

## **Dimension 1**

### **Cybersecurity policy and strategy**



## Dimension 1 – Cybersecurity policy and strategy

---

Dimension 1 of the GCSCC CMM looks at national capacity to devise, implement and review a national cybersecurity strategy and the key strategic, doctrinal and operational documents and activities underpinning it. This dimension also includes national cyber resilience and capacity as regards incident response, crisis management, critical infrastructure protection, communications redundancy, crisis management and cyber defence.

This dimension of the GCSCC CMM comprises six factors. The following sections outline capacity-building steps that national decision makers can implement to build capacity across these issue areas. These factors can be summarised as follows:

### **1. D1.1 – National cybersecurity strategy**

This factor focuses on national capacity to develop, review and update a national cybersecurity strategy that helps to prioritise cybersecurity actions, determine responsibilities, and allocate relevant resources.

### **2. D1.2 – Incident response**

This factor focuses on incident response capacity, particularly the ability to respond to cybersecurity incidents at a national level.

### **3. D1.3 – Critical infrastructure protection**

This factor focuses on the capacity to protect those assets and systems that are essential for maintaining vital social functions, including health, safety, security, economy and social wellbeing.

### **4. D1.4 – Crisis management**

This factor focuses on national capacity to develop, review and update national crisis-management applications, functional protocols and standards.

### **5. D1.5 – Cyber defence**

This factor focuses on national capacity to design and implement a cyber defence strategy while maintaining the benefits and flexibility of an open cyberspace for government, international business and society in general.

### **6. D1.6 – Communications redundancy**

This factor focuses on a government's capacity to identify, map and leverage digital redundancy and redundant communications among national stakeholders.

## D1.1 – National cybersecurity strategy

### Overview

This factor focuses on national capacity to develop, review and update a national cybersecurity strategy to prioritise cybersecurity actions, determine implementation responsibilities and allocate resources required to take action.

A NCSS has the purpose of providing direction and framing for national policies and actions pertaining to cybersecurity over the medium-to-long term. The development of a strategy should begin with an analysis and understanding of the wider context in which it will operate, of the areas that a country wishes to protect or influence through its actions, and of the threats and challenges facing the national cyber ecosystem. If other NCSSs have previously been developed, there is also a need to understand how a new strategy would relate to and build on these. A country's NCSS should be periodically reviewed and updated in light of the results of broad stakeholder consultations and feedback.

Ownership and governance of the future strategy and its associated implementation plans are key elements to consider alongside wider stakeholder engagement in the drafting, delivery, monitoring and evaluation of the strategy. To be effective, it is not sufficient for a strategy merely to exist; it should be implemented, with implementation plans drawn up as part of the drafting process to support the strategy's adoption. To facilitate this, a strategy may be broken down into smaller (e.g. sectoral) sub-strategies, policies and implementation plans. Implementation plans in particular should offer a detailed translation of the strategy into concrete, actionable tasks with well-specified timelines, and clearly identified task leaders and owners. Outlining clear, measurable and time-bound implementation plans for a NCSS can facilitate its subsequent evaluation and the identification of areas for further development during future revisions of the overarching strategy.

It is expected that nations seeking to develop a NCSS will need to go through a number of steps to achieve this. Box 1.1 below provides an overview of the high-level steps required for designing a strategy through an inclusive, multi-stakeholder process.

**Box 1.1: Steps for building a national cybersecurity strategy (D1.1)**

- Give direction to produce a national cybersecurity strategy and create a team to lead on drafting it.
- Nominate the task owner within government for coordinating and prioritising input into the national cybersecurity strategy from all relevant stakeholders.
- Give the strategy-drafting team a mandate to consult across public and private sectors and civic society.
- Allocate a discrete budget for cybersecurity and nominate a central task owner or coordinated taskforce within government responsible for administering it, allocating resources to tasks according to priorities identified in the document, and reassigning budgets dynamically according to the changing risk assessment and conditions.
- Draft a national cybersecurity strategy based on an informed understanding of national cybersecurity risks and the input of all relevant national and international stakeholders.
- Regularly revise and refine the national cybersecurity strategy to account for changing socio-political, threat and technology environments, and to bring the strategy and resource allocation in line with wider national strategic plans.
- Establish mechanisms to assess the quality of contributions of relevant government branches, other stakeholders and international partners to the national cybersecurity strategy and provide feedback as appropriate.
- Establish evaluation mechanisms with clear metrics and measurements to help evaluate the achievement of strategic objectives and inform resource-allocation mechanisms.
- Implement trust-building and confidence-building measures to ensure the continued inclusion and contribution of all stakeholders, including the private sector and international partners.
- Disseminate and receive feedback on the national cybersecurity strategy from relevant stakeholders and wider society through the nominated task owner coordinating the strategy.

For the purposes of avoiding duplication, and in agreement with interested stakeholders, this document does not elaborate further on these steps. An in-depth analysis of the steps required to create or update a national cybersecurity strategy is being undertaken by a partnership comprising the GSOSC, the Commonwealth Secretariat Cybercrime Initiative, the CTO, the European Network and Information Security Agency (ENISA), ITU, the Microsoft Corporation, the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Organization for Economic Co-operation and Development (OECD), the OAS, the Potomac Institute, the United Nations Conference on Trade and Development (UNCTAD), and the World Bank. The output of this partnership will be a resource that stakeholders and policymakers can refer to in order to clarify the purpose, content and drafting procedure for a national cybersecurity strategy. This guide is due to be published by the end of 2017.

## D1.2 – Incident response

### Overview

This factor looks at incident response capacity, focusing on the ability to respond to cybersecurity incidents at a national level. It covers the development and implementation of response processes that allow government to identify national-level cyber incidents and coordinate a response to ensure that damage is contained, the attacker is no longer present, and the functionality and integrity of the network and system are restored.<sup>8</sup>

Cyber-attacks are committed by a wide range of actors with diverse motives, including cybercriminals, insiders, hacktivists, cyber-fighters, cyber-terrorists, state actors, corporations and so-called ‘script kiddies’.<sup>9</sup> A variety of methods<sup>10</sup> are used to target Internet users ranging from government and public authorities to political parties, private companies, non-governmental and non-profit organisations, individual citizens and others.<sup>11</sup> The type and degree of impact from a cyber-attack can vary considerably, and may include a reduction in functionality of networks and computing systems, destruction of records, financial loss, loss of sensitive information, loss of business competitiveness, and disruption to the physical world through, for example, power outages and loss of critical infrastructure.<sup>12</sup>

Incident response at a national level may cover some, if not all, of these areas. This section focuses on the capacity at a national level to understand and detect these cybersecurity threats and incidents, and to respond in a coordinated, systematic and effective manner. It encourages countries to build incident response capacity, not only from a technical standpoint but also through the development of appropriate organisational and communication measures.

Box 1.2 provides an overview of capacity-building steps for increasing national capacity in the area of incident response.

### Box 1.2: Steps for building incident response capacity (D1.2)

- Establish a national-level CSIRT with responsibility for incident response at the national level.
- Recruit, develop and retain members of staff for the national CSIRT tasked with incident response at the national level.
- Set up physical facilities and acquire the technological capabilities necessary for incident response at the national level and for training personnel to perform this task.
- Define, document and operate incident response processes. Periodically review these to ensure their suitability for different incident scenarios.
- Establish a central registry of national-level cybersecurity incidents; set up mechanisms to update the registry regularly, and to issue warnings and alerts on the basis of environmental changes and the evolving threat landscape.
- Establish or join regional and international coordination mechanisms for incident response and information sharing.

### Capacity-building steps



- Establish a national-level CSIRT with responsibility for incident response at the national level.

Responsibility for national-level incident response should be assigned to a clearly identified task owner. This role is usually performed by a national-level CSIRT. A CSIRT is a team of information technology (IT) security experts tasked with handling and responding to security incidents, supporting a constituency and helping its recovery from breaches and incidents. CSIRTs can provide a wide array of services, spanning from reactive incident response to preventative and educational services.

Several guides exist that outline activities required to establish a CSIRT (see reference list at the end of this section). This toolbox does not attempt to replace or augment these documents, but instead highlights some of the key areas of focus, including:

- Defining a **mission** (what does the CSIRT intend to do?);
- Identifying relevant **stakeholders**;
- Defining the CSIRT's position in the wider **institutional framework**;
- Defining a **constituency** (for whom does the CSIRT act?);
- Establishing a CSIRT through **legal frameworks**;
- Defining **capabilities and services** offered by the CSIRT (consistent with the mission);
- Establishing an **organisational structure**, both internally and in relation to other organisations.

#### Mission

It is important to define the overarching mission of a CSIRT from its inception. The mission should be clearly and concisely defined, documented and distributed, and should provide a basic overview of what the team is trying to achieve. It should be possible to confine a mission statement to a maximum of three or four unambiguous sentences. The mission statement should be supported by senior officials to ensure it is recognised across government and the private sector. It is often useful to supplement a mission statement with a secondary statement of purpose, which provides a brief outline of the reasons behind the formation of the CSIRT.<sup>13</sup>



A clear mission statement is important as it helps shape both internal and external perceptions of the CSIRT. Internally, a clear mission statement provides focus for more precise objectives, and allows the capabilities and services offered by the CSIRT to be defined and prioritised in an unambiguous manner. Externally, a clear mission statement enables other cybersecurity stakeholders to understand and recognise the role and importance of the team. This can be important for securing and building the funding, resources and relationships required for the CSIRT to effectively carry out its activities.<sup>14</sup>

## D1.2 – Incident response



A failure to develop and communicate a clear mission statement can result in uncertainties and ambiguities that, in turn, lead to difficulties including inefficient expenditure of effort and resources, particularly during crisis situations.<sup>15</sup>

As a minimum, a CSIRT should provide some form of handling capability in response to cyber incidents, but the mission of a national CSIRT usually includes the following: (i) acting as the national coordinator for incident response; (ii) acting as the contact point for national and international incidents; (iii) functioning as a coordinator of information security advice for private sector actors and institutions from other sectors; and (iv) providing incident response services to government stakeholders and other end-users.

It is worth noting that a national CSIRT coordinating incident response may be assisted by a variety of other CSIRTS, including:

- Critical infrastructure protection (CIP) or critical information infrastructure protection (CIIP) CSIRTS, tasked with the monitoring and protection of critical infrastructure assets;
- Government CSIRTS, tasked with monitoring and responding to incidents in government networks, as well as ensuring that government IT infrastructure and services are adequately secured;
- Military CSIRTS, tasked with protecting the networks and ICT infrastructure of the defence establishment and those required for defence activities;
- Academic CSIRTS, tasked with providing incident response services for academic institutions and communities;
- Small and medium enterprise (SME) sector CSIRTS, tasked with providing incident response services tailoring them to the needs of SMEs;
- Commercial CSIRTS, offering incident response services within an individual company or to paying customers.



The functions and responsibilities to be performed by a national CSIRT with responsibility for coordinating incident response at the national level will vary depending on the landscape of CSIRTS operating within its country. Particularly in more advanced contexts, a national CSIRT may be taken to represent a 'last resort CSIRT',<sup>16</sup> which implies that it may be required to fill gaps in incident response that would normally be provided by sectoral CSIRTS or other bodies. In contexts where limited resources are available, a CSIRT may instead function as a central coordination authority for incident response.

## Stakeholders

When establishing a national-level CSIRT, it is important to identify relevant stakeholders who may both support and benefit from its existence. In the case of a national CSIRT, the community of stakeholders engaging with it typically includes:

- Government and government agencies
- Law enforcement agencies
- Defence establishment
- Academic sector
- Internet service providers (ISPs)
- Financial and other critical sectors
- National and international organisations and working groups.



Members of different agencies and stakeholder groups should take part in planning and setting up a national CSIRT to ensure it is representative of the various interested parties. Relevant stakeholders can be identified by mapping the cyber ecosystem and/or through the use of strategic planning tools such as a SWOT analysis or a PEST analysis.

Stakeholders can be clustered according to their expected role and contribution. This includes the identification of those that should be more closely engaged and able to influence the development and functioning of the national CSIRT, and those that should be kept informed. During the early stages of establishing a national CSIRT, stakeholders may be engaged through working groups, which independently seek to refine the mission and wider vision of the team. Early engagement also helps build relationships and buy-in from individuals and organisations who may directly support the activities of the CSIRT in the future.

## Institutional framework

The national CSIRT team should be well integrated within existing government structures and adequately resourced. The CSIRT's position and communication channels within the broader governmental organisational structure should be clearly defined. Furthermore, the national CSIRT should have access to adequate financial, human and infrastructure resources.<sup>17</sup> The institutional placement and resourcing of the national CSIRT should reflect the ambition and responsibilities outlined in its mission statement.<sup>18</sup>



A project team may be tasked with producing an initial institutional framework for the CSIRT. In addition to being able to produce an appropriate framework, members of this team should have access to senior levels of government to enable them to help shape cybersecurity policy and funding at the national level. Ideally, the project team should be multidisciplinary, comprising experts from cybersecurity incident response, public policy in technology and telecommunications, national-level defence and security, public law and legal frameworks.<sup>19</sup>

## D1.2 – Incident response

### Legal framework

A CSIRT cannot function effectively without a rigorous legal framework. This should verify that the CSIRT conforms to existing laws and provide a legal basis for the activities to be undertaken by the team. A faulty legal framework risks leaving the CSIRT vulnerable to lawsuits or complications when responding to cyber-attacks.<sup>20</sup>

### Constituency

When establishing a CSIRT, it is important to identify the constituency that the team is intended to serve (i.e. the client of the CSIRT). The identification of a client or target constituency should be made clear within the mission statement of the CSIRT.<sup>21</sup> When determining a CSIRT's constituency, the role of any existing CSIRT teams in public and private sector organisations should also be considered, along with whether any differentiation in service should be offered to different constituents (i.e. whether certain services should be provided only to a restricted number of stakeholder actors and groups).<sup>22</sup> The degree of the CSIRT's authority vis-à-vis its constituency should also be determined at this stage. This may be based on different levels of authority, such as:<sup>23</sup>

- **Full authority**, whereby the CSIRT is able to unilaterally carry out necessary actions on behalf of its constituency;
- **Shared authority**, whereby the CSIRT is able to intervene through a joint decision with its constituency;
- **Indirect authority**, whereby the CSIRT is able to influence its constituency through indirect pressure, such as through regulation or trust relationships;
- **Null authority**, whereby the CSIRT is unable to decide whether or not a decision is taken, although advice, information and experience can still be offered.

### Capabilities and services

In addition to the overarching mission, the capabilities and role of a national CSIRT should also be defined.



Engaging with key stakeholders early in the process of establishing a CSIRT can help identify core services and any other services a CSIRT should endeavour to provide.

These capabilities can be broken down into four categories as follows:<sup>24</sup>

- **Formal capability** refers to the official mandate of the CSIRT. CSIRTs may play an important role in developing and implementing national cybersecurity strategies, although there are differences between countries in terms of the scope of mandates given to CSIRTs. The mandate of a CSIRT typically includes, among other things: a clear definition of its roles and responsibilities in national policy and legal frameworks; an authority to act and react to cybersecurity incidents; a clear definition of the CSIRT's relationships with other

cybersecurity stakeholders; a stability of mandate with space for growth in maturity and effectiveness; and a continuity of resources and funding.

- **Operational-technical capability** refers to the technical services that the CSIRT provides to both external and internal organisations.<sup>25</sup> The CSIRT may provide proactive, reactive and/or other security management services to external organisations. CSIRTS may also provide internal services to their overarching organisations (e.g. a national government in the case of national CSIRTS), such as awareness-raising or cybersecurity training activities that target internal staff as well as external stakeholders and audiences. The core operational-technical capability of a national CSIRT includes incident handling and management, and designation as the national point of contact. Further discussion of the external operational-technical capabilities typically offered by CSIRTS is provided in the information box below.
- **Operational-organisational capability** refers to the resources, infrastructure and continuity of service delivery provided by the CSIRT. This includes human resources (such as staffing level, skill level, etc.), technical resources (software and hardware), budget allocation, training provision and the ability to maintain 24/7 operations.
- **Co-operational capability** refers to both vertical and horizontal cooperation among stakeholders. There are a wide variety of stakeholders involved in incident response at a national level, including government and other public bodies, hardware and software providers, operators, service providers and end-users. Cyberspace is borderless and there is often an international aspect to cyber incidents that requires cooperation with other national CSIRTS and cybersecurity organisations. Building and maintaining trust and communication with all relevant stakeholders is important for incident response.



The **operational-technical capabilities** of a CSIRT can be broken down into a number of sub-categories, including:

**Reactive services** provided by the CSIRT in response to an incident. The CSIRT may respond to requests for assistance, reports of an incident, detection of an external incident, or detection of an incident within its own CSIRT systems.

**Proactive services** aimed at improving security infrastructure and processes before an incident occurs or is detected. The primary goal of proactive services is to prevent and reduce the impact of cybersecurity incidents.

**Security management services** that aim to improve the cybersecurity of external organisations.

Examples of these services are outlined in Table 1.1 below.

## D1.2 – Incident response

Table 1.1: Typical operational-technical services offered by a CSIRT

Reactive services	Proactive services	Security management services
Alerts and warnings	Technology watch announcements	Risk analysis
Incident handling <i>Incident analysis</i> <i>Incident response on site</i> <i>Incident response support</i> <i>Incident response coordination</i>	Security audits or assessments	Business continuity and disaster recovery planning
Vulnerability handling <i>Vulnerability analysis</i> <i>Vulnerability response</i> <i>Vulnerability response coordination</i>	Configuration and maintenance of security tools, applications and infrastructures  Development of security tools  Intrusion detection services	Security consulting awareness-building education/training
Artefact handling <i>Artefact analysis</i> <i>Artefact response</i> <i>Artefact response coordination</i>	Security-related information dissemination	Product evaluation or certification

SOURCE: ENISA (2016, 11)



The services provided by the CSIRT should be consistent with the formal capability and mandate of the team, and should be defined in such a way that they can realistically be provided using the available resources. The success of a CSIRT is largely measured by the quality of service provided, and it is better to provide a small number of high-quality services than a large number of low-quality services.<sup>26</sup>

The capability and services offered by the CSIRT team are likely to evolve and expand over time, although this is dependent on a number of factors, including size, infrastructure, funding and human resources.<sup>27</sup>

### Organisational structure

It is important to have clear delegation of roles and responsibilities in a CSIRT, although in smaller teams a single individual may undertake multiple roles. The internal organisational structure is somewhat dependent on the mission statement, size and scope of the CSIRT, although a number of functions are relevant to all CSIRT teams. The following elements are recommended as a minimum initial structure:<sup>28</sup>

- **Management:** This includes strategy, budget, operational organisation, liaison and communication with external stakeholders, and media relations.
- **Operations:** This includes incident management and monitoring of threats.
- **IT:** This includes maintenance of the IT infrastructure, and support to operations and research and development (R&D).

- **R&D:** This includes research into developing technology, statistical analysis of threat and incident trends, development of systems and tools, training, and support to operations.
- **Support services:** This includes marketing, legal support, media relations, administration and finance.

Larger CSIRT teams often include additional functions such as specialist incident response teams, a security operations centre, training, specialist information security management, internal audit and labs for malware forensics.<sup>29</sup>



- Recruit, develop and retain members of staff for the national CSIRT tasked with incident response at the national level.

It is important to ensure that a CSIRT is staffed with sufficient numbers of professionals with the right skills to take on its incident response functions. The National Institute of Standards and Technology of the United States (US) Department of Commerce, through the National Initiative for Cybersecurity Education (NICE), developed a comprehensive *Cybersecurity Workforce Framework* to map the knowledge, skills and competences required for different types of cybersecurity professional roles, including those pertaining to CSIRTs and incident response more broadly.<sup>30</sup> In addition to standard management roles and profiles, a CSIRT should employ operational staff with specialised knowledge and experience in cybersecurity incident response, computer forensics, information assurance and systems development. To attain these specialisms, staff should first have a minimum level of knowledge of (i) Internet technology and protocols; (ii) Linux, Unix or Windows systems (depending on the equipment of the constituency); (iii) network infrastructure equipment; (iv) Internet applications; and (v) security threats and risk assessment.

There are several cybersecurity certifications that may help identify suitable candidates to work in a CSIRT. These include:<sup>31</sup>

- **EC-Council Certified Incident Handler (ECIH) programme:**<sup>32</sup> ECIH is two-day training programme provided by the International Council of E-Commerce Consultants (EC-Council) that focuses on incident handling, risk administration, pen testing, forensic investigation, and other principles and techniques for detecting and responding to computer security threats. An examination must be passed at the end of the course in order to receive the certification. The EC-Council is a private cybersecurity technical certification body which operates in 145 countries worldwide, and provides certification to employees in both the public and private sectors.<sup>33</sup>
- **GIAC Certified Incident Handler (GCIH):**<sup>34</sup> The GCIH, provided by Global Information Assurance Certification (GIAC), is a certification of proficiency in detecting, responding to, and resolving computer security incidents. It is not a training course, but rather a four-hour examination that

## D1.2 – Incident response

covers the process of incident handling, detecting malicious applications and network activity, common attack techniques, detecting and analysing vulnerabilities, and implementing continuous process improvement.<sup>35</sup> The certification must be renewed every four years. GIAC is a private certification company that focuses on computer, information and software security, and certifies incident handlers in both government and industry.<sup>36</sup>

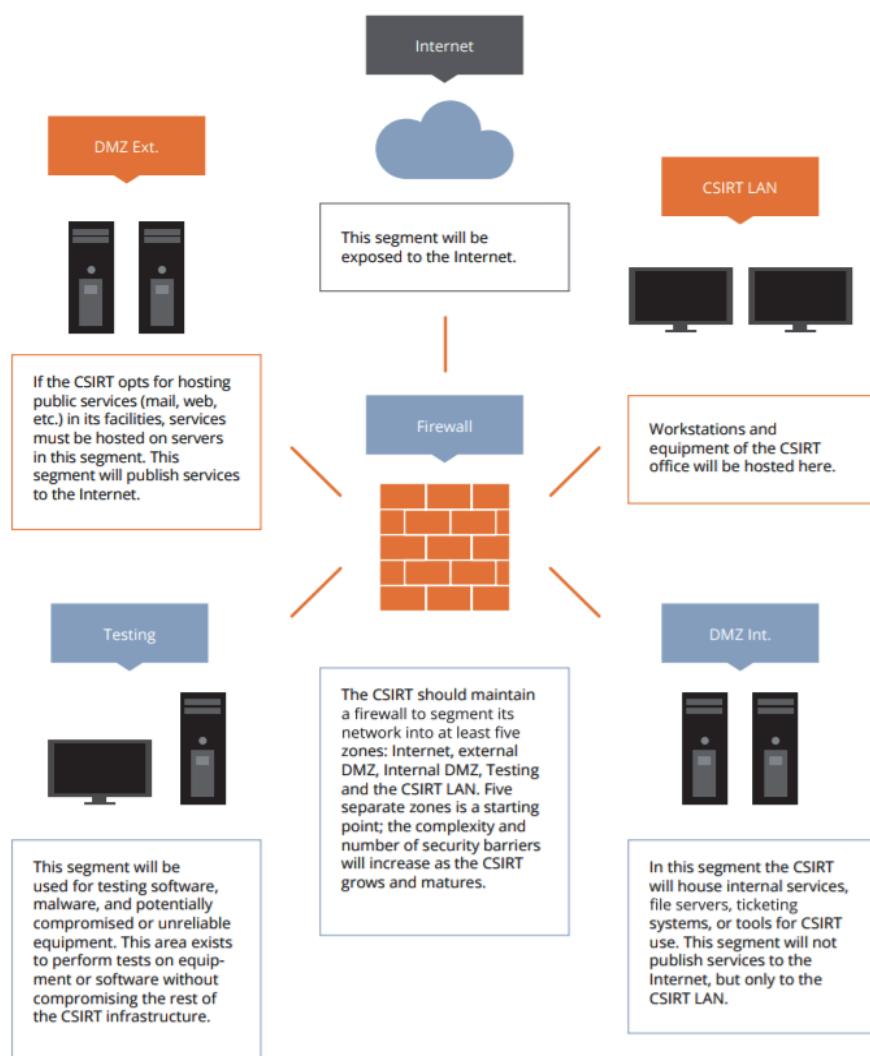
- **GIAC Response and Industrial Defense (GRID):**<sup>37</sup> The GRID certification is also provided by GIAC, and focuses on identifying and protecting critical infrastructure such as public utilities, commercial manufacturing facilities, or other types of Industrial Control System (ICS). In particular, it requires candidates to demonstrate an understanding of Active Defense strategies specific to ICS, as well as an understanding of ICS-specific attacks and how these attacks inform mitigation strategies. To receive the certification candidates must pass a two-hour exam. The certification must be renewed once every four years.<sup>38</sup>
- **Certified Cyber Forensics Professional (CCFP):**<sup>39</sup> The CCFP is a professional certification that focuses on forensics techniques and procedures, standards of practice, and the legal and ethical principles required to ensure that cyber forensic evidence is admissible in court. The certification aims to be applicable across different sectors, including law enforcement, cyber intelligence in defence and security, and the private sector.<sup>40</sup>
- **GIAC computer forensics certifications:**<sup>41</sup> GIAC also offer a range of certifications in cyber forensics, including Global Information Assurance Certification Forensic Examiner (GCFE), GIAC Network Forensic Analyst (GNFA) and GIAC Advanced Smartphone Forensics (GASF).



- Set up physical facilities and acquire the technological capabilities necessary for incident response at the national level and for training personnel to perform this task.

A CSIRT and its employees should be located in dedicated facilities that are secured in the same way in which an organisation would protect a datacentre. CSIRTs should not be located in open cubicle environments, but rather in separate office spaces with restricted access policies in place to prevent unauthorised access to CSIRT resources and information. The CSIRT building or facilities should be protected by 24-hour surveillance. Physical and logical access to servers, communications equipment, logic safety devices and data repositories should be regulated by strict access control.<sup>42</sup> Figure 1.1 presents an overview of a minimum design for a CSIRT's network architecture.

Figure 1.1: Overview of a minimum design for a CSIRT network architecture



SOURCE: OAS (2016a)

In addition to locating the CSIRT within dedicated facilities with adequate equipment, CSIRT staff should be provided with regular training and update courses to ensure that they can effectively perform their functions. In addition to the technical certifications presented above, courses on cybersecurity fundamentals and threats, computer and network forensics, malware analysis and reverse engineering, and other analysis tools and techniques should be provided to the CSIRT's operational staff, either in-house or through external providers.<sup>43</sup>

In addition to training, cyber exercises can be an effective tool to train personnel in handling cyber incidents. This requires assessment of which resources (e.g. personnel, infrastructure and communication capabilities) need to be tested, identification of objectives for the exercise and personnel responsible, and incorporation of exercises within the cybersecurity strategy. The impact of exercises needs to be evaluated and the findings should inform adjustments to future exercises or the cybersecurity strategy as a whole.<sup>44</sup>

## D1.2 – Incident response



- Define, document and operate incident response processes; periodically review these to ensure their suitability for different incident scenarios.

An *incident-handling response process* is a set of defined steps that a CSIRT will follow to effectively counter a cybersecurity incident. It is a process that is defined and developed independent of a specific incident, with the aim of developing a framework that enables a structured, coordinated, methodical and consistent approach to incident response.

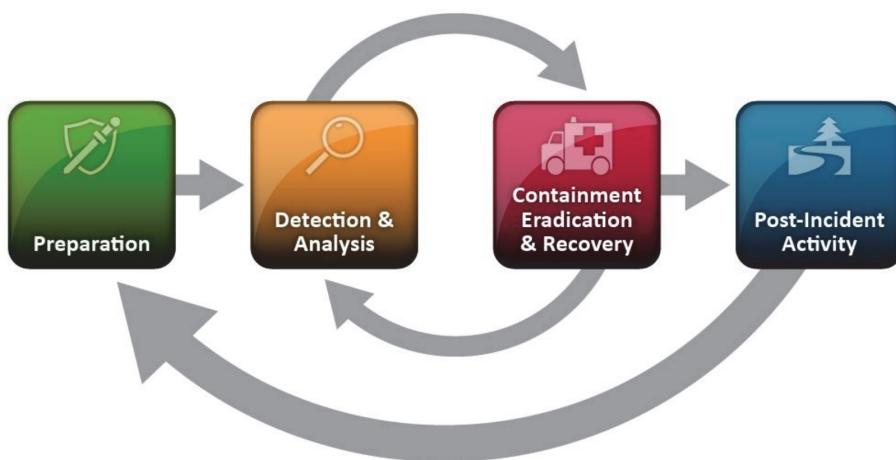
Incident-handling response processes are often developed at a high level, and then refined into more specific processes for particular types of attack. At a strategic level, an overarching incident response process outlines the general steps that should be taken when responding to a cyber incident. These steps should be defined in such a way that they are applicable across different types of attacks, but nonetheless remain tailored to incident-handling response within a particular CSIRT. While an incident-handling response process is most effective when developed within individual CSIRT teams according to local requirements, a number of general frameworks have been developed to support CSIRTs in developing their incident response processes.<sup>45</sup> These frameworks differ slightly in their breakdown and structuring, but broadly cover the same factors.



### NIST Incident Response Life Cycle

The National Institute of Standards and Technology (NIST) structures incident-handling response process into four key stages: i) preparation; ii) detection and analysis; iii) containment, eradication and recovery; and iv) post-incident activity.<sup>46</sup>

Figure 1.2: Example of an incident response process



The following paragraphs expand on each of these stages in turn. **Preparation** refers to the period before an incident occurs. It includes not only the technological and human capacity required to respond to

cyber-attacks, but also the organisational structures and procedures that are required for a clear and well-coordinated response to a cyber-attack. Preparation also includes the process of securing systems and networks in order to prevent attacks, although this often is beyond the remit of a CSIRT.<sup>47</sup>

**Detection and analysis** aims to identify and understand a cyber-attack once it has occurred. At the detection stage, this involves introducing and maintaining appropriate technological detection mechanisms, and establishing organisational procedures that are able to identify data loss and monitor and detect intrusions into both systems and networks. Once an attack has been detected, a subsequent analysis should seek to understand the type, scale and impact of the attack, and include an *endpoint analysis*, *binary analysis* and *enterprise hunting*.<sup>48</sup>

**Containment, eradication and recovery** refers to the period after the initial identification and analysis of a cyber-attack. The first stage – containment – seeks to limit the damage of a cyber-attack by stopping it from spreading to other devices, systems and networks.<sup>49</sup> The attack itself is then removed from the affected systems, for example by blocking the attacker's access to the network, deleting malware and disabling user accounts that have been compromised. The eradication stage should also monitor any response from the attacker, while simultaneously working to identify and remove the vulnerabilities initially exploited during the attack.<sup>50</sup>



While it is important to eradicate an attack as quickly as possible, it is also important to meet the forensic requirements for cyber incident response handling. This includes ensuring a chain of custody that collects and preserves evidence in a manner that is detailed in an action log.<sup>51</sup>

The recovery stage begins after successful containment and eradication of the cyber-attack, and aims to return systems to their normal operating standard. This includes replacing and rebuilding damaged systems and reconnecting them to the network; removing temporary constraints such as permissions, passwords and temporary firewalls; installing appropriate patches; and testing the system to ensure that it is not vulnerable to the same attack.<sup>52</sup>

The final stage in the incident-handling process is **post-incident activity**, which involves collecting and storing information and evidence from the incident, and identifying lessons learned from the response in order to improve future incident-handling processes.<sup>53</sup>



It is important that **digital evidence** is handled in the correct manner and according to national procedural legislation, as this evidence may be used in a criminal court if the attacker is identified and prosecuted.<sup>54</sup>

In order to ensure that each stage is completed during the response to a particular incident, an **incident-handling checklist** may be used to track progress through the incident-handling process. The general incident-handling process is detailed to varying degrees of granularity within the available literature, and a tailored checklist should be developed according to the particular requirements of a CSIRT.<sup>55</sup>

Finally, once a high-level approach to incident handling has been developed, it is often useful to tailor this approach to particular types of cyber-attack. In particular, different types of containment, eradication and

## D1.2 – Incident response

recovery processes are required for different types of cyber-attack, meaning a more tailored approach to incident response may be more useful than a single overarching framework.<sup>56</sup>



It is often difficult to determine the type of cyber-attack during the early stages of an incident response. Tailored processes should therefore use a common approach until the type of cyber-attack is identified, after which more specific forms of analysis, containment, eradication and recovery become relevant.<sup>57</sup>

**Figure 1.3: An example incident-handling checklist**

	Action	Completed
<b>Detection and Analysis</b>		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
<b>Containment, Eradication, and Recovery</b>		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
<b>Post-Incident Activity</b>		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

More specific incident response processes are tailored to particular types of attack, such as DDOS attacks or the detection of malware.



### National and international laws and standards

Incident response processes involve the receipt of incident reports, evaluation of incidents, and actions taken to address incidents. It is therefore important that incident response processes are not only effective, but also comply with national and international laws and standards.<sup>58</sup> For example:

#### International

Basel II Agreement, Council of Europe's Convention on Cybercrime, Council of Europe's Convention on Human Rights, International Accounting Standards.

#### European

Directive on electronic signatures (1993/93/EC), Directives on data protection (1995/46/EC) and privacy in electronic communications (2002/58/EC), Directives on electronic communication networks and services (2002/19/EC – 2002/22/EC), Directives on Company Law (e.g. 8th Company Law Directive).

#### Standards

British Standard BS 7799 (Information Security), International Standards ISO2700x (Information Security Management Systems), German IT-Grundschutzbuch, French EBIOS and other national variations.



- Establish a central registry of national-level cybersecurity incidents and set up mechanisms to update this regularly, as well as to issue warnings and alerts on the basis of environmental changes and the evolving threat landscape.

A national CSIRT should host a server functioning as a registry of national incidents, keeping records and tracking cybersecurity incidents. This registry should record reports of incidents received and communications flowing into and out of the CSIRT related to incident response, and should also be used to check the status of the personnel involved in an incident response.<sup>59</sup>

In addition, a CSIRT should run and periodically review a process for creating security advisory alerts and warnings for its constituency and clients. This process should encompass the following steps:

1. Receive a warning about security vulnerabilities from the CSIRT's partner network or from vendor bulletins and newsletters.
2. Collect information on the vulnerability and evaluate its relevance, classification, associated risk and potential impact.
3. Prepare and distribute a security advisory alert to the CSIRT's constituency presenting the vulnerability's origin, relevance (i.e. to which software or hardware it applies), risk, impact and potential damage, solution and description of details.<sup>60</sup>

## D1.2 – Incident response



- Establish national coordination mechanisms between public and private sectors with national contact points for government and critical industries.

Since cybersecurity is a domain with different public and private actors assuming responsibilities and competencies, it is essential that these actors cooperate closely with one another. National coordination mechanisms with contact points and routine cooperation should be adopted, ranging from information exchange and sharing of good practices to joint actions.<sup>61</sup>



- Establish or join regional and international coordination mechanisms for incident response and information sharing.

An important aspect of a national CSIRT's work pertains to the development of trusted working relations with neighbouring national CSIRTS.<sup>62</sup> Furthermore, a national CSIRT may join a number of regional and international coordination mechanisms for incident response information sharing and coordination. These include:

- **Forum of Incident Response and Security Teams (FIRST):** According to its mission statement, FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident-prevention programmes. Specifically, FIRST: (i) encourages and promotes the development of quality security products, policies and services; (ii) develops and promotes best practices in computer security; and (iii) promotes the creation and expansion of incident response teams and membership from organisations from around the world. FIRST members: (i) develop and share technical information, tools, methodologies, processes and best practices; and (ii) use their combined knowledge, skills and experience to promote a more secure global electronic environment.<sup>63</sup>
- **Task Force-CSIRT:** The TF-CSIRT promotes collaboration between CSIRTS in Europe. The main goals of the TF include: (i) providing a forum for exchanging experiences and knowledge; (ii) establishing pilot services for the European CSIRT community; (iii) promoting common standards and procedures for responding to security incidents; and (iv) assisting the establishment of new CSIRTS and the training of CSIRT staff.<sup>64</sup>
- **Asia Pacific Computer Emergency Response Team (APCERT):** APCERT is a forum established to maintain a trusted contact network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents. APCERT's goals include: (i) enhancing Asia Pacific regional and international cooperation on information security; (ii) jointly developing measures to deal with large-scale or regional network security incidents; (iii) facilitating information sharing and technology exchange, including information security, computer virus and

malicious code among its members; (iv) promoting collaborative R&D on subjects of interest to its members; (v) assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response; and (vi) providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.<sup>65</sup>

- **AfricaCERT:** AfricaCERT describes itself as the African forum of incident response teams. AfricaCERT's objectives include: (i) coordinating cooperation among African CSIRTS; (ii) assisting African countries in establishing CSIRTS; (iii) fostering and supporting education and outreach programmes in ICT security in and among African countries; (iv) strengthening the relationships between CSIRTS in Africa and with other stakeholders around the world; (v) encouraging information sharing in ICT security so that vulnerabilities can be rapidly identified and risks neutralised; (vi) promoting sharing of good practices and experience among its members to develop a comprehensive framework for cybersecurity; (vii) assisting African CSIRTS in improving cyber readiness and enhancing the resilience of ICT infrastructure; and (viii) promoting collaborative technology research, development and innovation in the ICT security field.<sup>66</sup>

#### Additional resources



- Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell & Elizabeth Phillips. 2014. Computer Security Incident Response Teams (CSIRTS): An Overview. Oxford: Global Cyber Security Capacity Centre.
- ENISA. 2006. A step-by-step approach on how to set up a CSIRT. Heraklion, Greece: ENISA
- ENISA. 2014. National/governmental CERTs: ENISA's recommendations on baseline capabilities. Heraklion, Greece: ENISA
- NCSC (National Cyber Security Centrum). 2015. GCCS CSIRT Maturity Quick Scan. As of 1 November 2017: <https://check.ncsc.nl/>
- OAS (Organization of American States). 2015. Best Practices for Establishing a National CSIRT.

## D1.3 – Critical infrastructure protection

### Overview

This factor focuses on the capacity to protect national critical infrastructure. Critical infrastructure (CI), also referred to as critical national infrastructure (CNI), is defined as the assets and systems that are essential for maintaining vital social functions, including health, safety, security, economy and social well-being. The disruption or destruction of CI will necessarily have a significant impact on society.<sup>67</sup> Examples of CI include the energy sector (electricity, oil, gas), transportation networks (road, rail, air, inland waterways and open sea waterways),<sup>68</sup> telecommunications infrastructure, financial systems, waste and drinking water systems, chemical and nuclear industries, emergency services, military and security services, civil administration and governmental services.<sup>69</sup>

ICT is increasingly used to monitor and control CI. These ICT systems are often semi-autonomous, and automatically perform background functions such as monitoring and handling routine tasks, as well as providing a digital platform for users to manage the administration, logistics, monitoring and control of CI systems.<sup>70</sup> In the energy sector, for example, the production, transportation and distribution of natural gas can be monitored and controlled remotely using digital monitoring systems and cyber-physical processes (such as remote operation of pipe valves).<sup>71</sup> Likewise, in the transportation sector, railway signalling and barriers are often automated through an ICT system.<sup>72</sup> These types of control systems are increasingly connected to internal and external networks, such as the Internet, to enable greater efficiency and flexibility. This includes connection with multiple CI operators, remote access for maintenance companies and system interrogators,<sup>73</sup> and, increasingly, connection to end-users through Internet of Things (IoT) devices.<sup>74</sup> There is an increasing interconnection and interdependence between CI computers and networks on a national and international level,<sup>75</sup> and an increasing dependence of CI on hardware and networks over which a government has no direct control as they are privately owned and operated. Examples include cloud services, Internet exchange points, domain name services and satellite communication.<sup>76</sup>

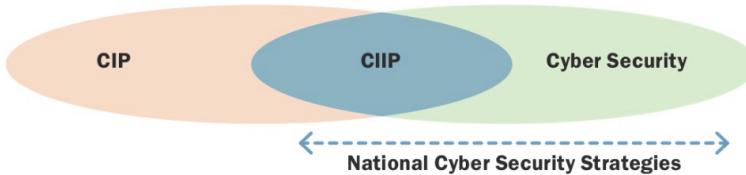
The integration of and reliance on information and communication systems in CI is often referred to as *critical information infrastructure* (CII). CII is broadly defined as the information and (tele)communications infrastructure that is critical to the functioning of CI. More specifically, CII includes both internal information and communication systems used in a particular CI sector or by a provider, and the wider critical information and communication infrastructure, such as the Internet and mobile phone networks.<sup>77</sup>

CI has long faced threats from natural disasters, technical failures, accidental human error and terrorist attacks.<sup>78</sup> However, the transition to ICT-based systems has created new vulnerabilities from cyber-attacks or incidents. By definition, CII is essential in keeping CI operational. If CII is disrupted or destroyed, then CI will also experience disruptions. This, in turn, may have a cascading negative impact on vital societal functions. As Figure 1.4 below illustrates, critical information infrastructure protection can be defined as the crossover between cybersecurity and critical infrastructure protection. CII faces a number of

threats, including hacktivism, cybercrime, cyber espionage and state-sponsored cyber-attacks. It may suffer from a range of vulnerabilities, including software flaws, human error and external interference.<sup>79</sup>

Hacktivism and cybercrime attacks are generally more frequent but less sophisticated and with less severe impacts. They typically include denial-of-service (DoS) attacks, defacing websites, stealing and publishing sensitive information, online fraud and online scams. This can cause both economic damage and disruption to CI, although damage tends to be minor. In contrast, cyber espionage and cyberwar attacks are typically less frequent, but the impact on CI can be severe. In particular, state-sponsored attacks or attacks from significant non-state actors,<sup>80</sup> involving penetration of another state's computers and networks with intent to disrupt or destroy, can lead to significant interruptions to CI with immediate economic damage and interruption to essential societal services. Cyber espionage can lead to the loss of classified information, which typically poses an indirect but significant threat to the security of CI. In other words, cyber espionage itself does not aim to disrupt CII, but the loss of personal, economic, military, political, business and CI information can be used to identify and expose vulnerabilities in CI and CII.<sup>81</sup>

**Figure 1.4: CIIP represented as the crossover between CIP and cybersecurity**



SOURCE: Luijif et al. (2016, 3)

This section discusses a number of steps that can help increase the security of CII, with the ultimate aim of increasing the protection and resilience of CI. Box 1.3 provides an overview of the steps, which are discussed in greater detail in the following pages.

#### **Box 1.3: Steps for building critical infrastructure protection (D1.3)**

- Nominate the task owner within government.
- Identify and engage public and private sector stakeholders.
- Identify cyber-vulnerable critical infrastructure (including vulnerabilities in supply chain) in an audit list to be distributed to relevant governmental stakeholders, prioritising assets identified according to their vulnerability and impact.
- Formulate a protection and risk-management strategy for identified critical infrastructure.
- Outline an action plan for protecting critical national infrastructure assets, indicating which threats are to be managed centrally and which are to be managed locally; embed adequate cybersecurity risk-management processes, technical solutions and harm-mitigation measures in day-to-day administration of critical infrastructure assets.

### D1.3 - Critical infrastructure protection

- Foster trust among stakeholders and create an environment conducive to mutually beneficial collaboration.

#### *Capacity-building steps*



- Nominate the task owner within government.

CIIP is a multi-agency activity with important public stakeholders in government ministries (communications, ICT, economic affairs, security, cabinet office, justice, defence and more), regional public bodies, regulators and other relevant public stakeholders.<sup>82</sup> Moreover, a range of private sector stakeholders are directly involved in CIIP, including CI and CII operators, manufacturers, system integrators, third-party maintenance companies, academics, R&D institutions, and non-governmental organisations (NGOs).<sup>83</sup>

An important factor in coordinating critical national infrastructure protection on a strategic level is the existence of a task owner with key CII expertise, and crucial understanding of CI and CII threats and the interdependencies between these threats within government.<sup>84</sup> There is no universal organisational structure for a task owner for all governments, and different countries have adopted different governance systems. Within European Union (EU) Member States, task owners for CIIP range from National Security Authorities with full supervision of specific activities and stakeholders involved, to decentralised models with distributed responsibilities. This depends on the existing framework at the national level, the budget and resources available and the priorities of the state.<sup>85</sup>



**Estonia** adopted an Emergency Act in 2009 which assigned responsibilities to nine government ministries and public bodies to maintain the continuous operation of vital services. These nine ministries and bodies report to a central national coordinator under the Ministry of Interior.

In 2009, **France** created the Agence Nationale de la Sécurité des Systèmes d'Information (National Agency for the Security of Information Systems – ANSSI), which oversees CIIP and reports to the General Secretariat for Defence and National Security. ANSSI is able to set minimum cybersecurity requirements, enforce the implementation of detection and incident notification systems, manage cybersecurity audits of CI and lead cross-government crisis management.

In the **UK**, CIIP strategy is included in the National Cyber Security Strategy, which is developed by the National Security Council in the Cabinet Office. The Cabinet Office coordinates CIP across the UK government, with the National Cyber Security Centre (under Government Communications Headquarters (GCHQ)) taking the lead on CIIP.<sup>86</sup>

The task owner should coordinate and be accountable for CIIP. This may include: identification of CI and CII, and of relevant CI and CII stakeholders; development of CIP and CIIP strategy; coordination of stakeholders in implementing CIP and CIIP strategy; monitoring and improving CIP and CIIP strategy

and implementation; and facilitating information sharing between relevant public and private sector stakeholders.<sup>87</sup> The potential benefits of assigning a task owner may include minimising the recovery and restoration period and the fostering of a common understanding between various stakeholders.<sup>88</sup> Moreover, the task owner will be able to mediate between agencies with competing priorities.<sup>89</sup> To be well-positioned to provide strategic direction, it is crucial that the CIIP unit is supervised by a leader with strong qualifications in ICT, especially with regard to information assurance, and that the task owner possesses the negotiation skills required to manage the CIIP unit's relations with other stakeholders, including within the private sector.<sup>90</sup>



➤ Identify and engage public and private sector stakeholders.

The task owner should engage on a regular basis with all relevant public stakeholders, and liaise with private sector actors who own and/or control critical infrastructure assets. From the early stages of CIP and CIIP, it is important to adopt a multi-agency approach within government, build public-private partnerships (PPPs) outside of government, and create effective platforms for information sharing between stakeholders.<sup>91</sup> Involving all relevant stakeholders not only provides the task owner with insight into the governance and ownership of different parts of CI and CII, but is also important in building an environment where all stakeholders work together, share information and take appropriate action. The ability and responsibility to mitigate many of the risks to CI and CII lies with a multitude of different public and private sector stakeholders, and a failure to sufficiently engage these stakeholders in the CIIP process may reduce the effectiveness of any CIIP strategy.<sup>92</sup>

It is important to first identify the relevant stakeholders across the public and private sectors. In many countries, a diverse and complex range of stakeholders are involved in CI and CII.



The range of stakeholders to be involved varies between countries, but typically includes:

- CIIP coordinating ministries (e.g. Interior, Justice, Defence, Prime Minister's Office);
- Ministries responsible for ICT (e.g. Communications, Media, ICT);
- Ministries responsible for specific CI (e.g. Economic Affairs, Energy, Health);
- Regulators for identified CI domains;
- Law enforcement and other public agencies;
- CI and CII operators/utilities;
- Policymakers and parliament;
- Manufacturers, system integrators and third-party maintenance companies;
- Cross-sector (branch) organisations;
- CSIRTs;
- National-level cybersecurity organisations;
- Academia and R&D organisations.

### D1.3 - Critical infrastructure protection

Once stakeholders have been identified, the next step is to establish engagement and cooperation between relevant parties. In the public sector, this may be achieved through, for example, regular roundtable meetings that discuss CIIP on a strategic, tactical and operational level. These may include discussions on governance structures, legal mandates, and procedures for operational coordination and cooperation. These roundtable discussions may later be expanded to include private sector stakeholders with the aim of not only delegating tasks effectively between sectors, but also building a collaborative environment that pools resources, shares information and conducts joint decision making.<sup>93</sup>

Roundtable discussions are not the only means of achieving public and private sector engagement, and more options are discussed in the final part of this section.



- Identify cyber-vulnerable critical infrastructure (including vulnerabilities in supply chain) in an audit list to be distributed to relevant governmental stakeholders, prioritising assets identified according to their vulnerability and potential impact.

A number of preliminary steps are required before developing a strategy for CIIP. These include:<sup>94</sup>

- Identification of CI
- Identification of CII
- Risk assessment (including threat assessment, vulnerability assessment and impact analysis).

These three steps do not necessarily need to be carried out in this order, although identification of CI should precede identification of CII.<sup>95</sup> Moreover, substantial documentation exists on each of these three steps. Only a brief overview is provided here, and the documentation listed at the end of this section should be consulted at each of these steps.



Although there are many similarities between different nations, the identification of CI, CII and the associated risk assessment is unique to each country. A bespoke analysis should be carried out by each country. It is often useful to draw on the methodologies and results of others, but this information should be adapted for the local context.<sup>96</sup>

For guidance, countries engaging for the first time in the identification of their CI and CII may wish to refer to:

- **NIST Special Publication 800-37:** NIST developed a *Risk Management Framework* (RMF) to improve information security, strengthen risk management processes and encourage reciprocity among partner organisations. This publication provides guidelines for applying the RMF to information systems and organisations.
- **NIST Special Publication 800-39:** This document is part of NIST's series of information security standards and guidelines. The purpose of this standard is to provide guidance for an integrated, organisation-wide programme for managing information security risk to organisational operations (i.e. mission, functions, image and reputation), organisational assets, individuals, other

organisations and the nation resulting from the operation and use of information systems.<sup>97</sup>

## Identification of CI

A number of different approaches exist for the identification of CI, including a bottom-up approach, a top-down analysis using simple criteria and metrics, and a top-down analysis that develops and employs detailed metrics.<sup>98</sup> These methods are not described in detail here – further information on these is available in resources listed at the end of this section. There are, however, a number of recommendations on good practice that apply across different methods.



The identification of CI is complex, and a number of different approaches exist. There are, however, general **recommendations on good practice** that may help support this analysis.

Using **frameworks and analysis** conducted by other countries can help guide a national CI assessment. For example, definitions of CI sectors and services, along with examples of metrics and indicators, can be found in CI assessments from other countries.<sup>99</sup>

Adopting a **systematic method** for identifying CI can provide structure and rigour to any identification process. The method can help to identify CI in particular sectors, measure the criticality level using a criticality scale, understand dependence and interdependence with other CI, assess cross-cutting criteria and identify international dependencies.<sup>100</sup>



### The UK Cabinet Office CI criticality scale

The UK government developed a criticality scale that provides a framework for measuring the criticality of national infrastructure. It assesses criticality based on the impact of a loss of infrastructure. In other words, if a particular infrastructure sector (such as energy, water or transportation networks) is interrupted, what is a) the impact on delivery of services; b) the economic impact due to the loss of these essential services; and c) the impact on life that results from a loss of these services? ‘Impact’ itself is also broken down into three measurable factors, namely: (i) the degree of disruption; (ii) the extent of disruption (population percentage, geographic distribution); and (iii) the period of disruption. Using this framework, critical national infrastructure is defined as infrastructure with a score above 2.5.<sup>101</sup> Table 1.2 provides an overview of the criticality scale for infrastructure.

**Table 1.2: UK criticality scale for infrastructure**

Category	Description
CAT 5	Infrastructure whose loss would have a catastrophic impact on the UK. These will be assets of unique national importance whose loss would have long-term, national-level effects and may have an impact across a number of sectors. Relatively few are expected to meet the Category 5 criteria.
CAT 4	Infrastructure of the highest importance to CI sectors. The impact of loss of these assets on essential services would be severe and may impact on provision of essential services across the UK or to millions of citizens.
CAT 3	Infrastructure of substantial importance to CI sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people.
CAT 2	Infrastructure whose loss would have a significant impact on the delivery of essential services, leading to loss or disruption of service to tens of thousands of people or affecting whole counties or equivalents.
CAT 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localised basis and affecting thousands of citizens.

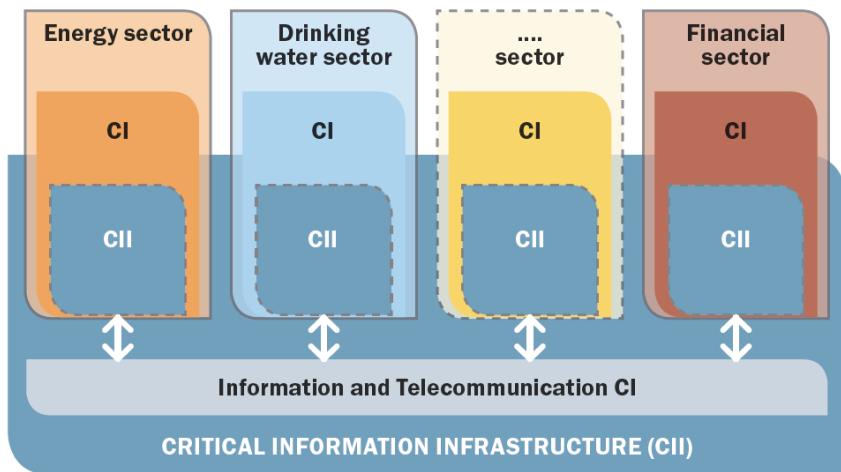
SOURCE: RAND Europe adaptation of UK Cabinet Office (2010, 25)

### Identification of CII

Having identified CI, the next stage is to identify and assess the CII that underpins CI sectors. This includes the identification of:

- Critical information, communication and control systems that support the functioning of each CI sector;
- Critical information and (tele)communication network infrastructure used across CI sectors (such as Internet, mobile phone and satellite networks).<sup>102</sup>

**Figure 1.5: Defining critical information infrastructure**



SOURCE: Luijif et al. (2016, 29)

There is a significant body of literature that discusses different approaches to identifying CII, although a detailed discussion across this domain is not provided in this toolbox. Further references focusing on this are listed at the end of this section. There are, however, a number of general recommendations for approaching CII identification, including:<sup>103</sup>

- Use a structured, systematic approach.
- Identify and engage CII operators from both the public and private sectors.
- Identify dependencies and information supply chains between CI sectors.
- Identify uncontrollable dependencies, such as use of international website-hosting platforms and cloud computing servers, reliance on international Internet exchange points, and use of third-party hardware manufacturers.
- Conduct regular reassessments of CII.
- Research emerging CII technology and shifting dependencies.

The Japanese Basic Policy on CIIP provides a number of examples of CII across different CI sectors, as illustrated in Table 1.3.

## D1.3 - Critical infrastructure protection

**Table 1.3: List of CII sectors in Japanese strategic documentation**

CII sectors	Critical information system examples
Information and communication services	Network systems Operation support systems Organisation/operation systems
Financial services	Accounting systems Financial securities systems International systems External connection systems Financial institution inter-network systems Electronic credit record agency systems Insurance service systems Securities trading systems Exchange systems Money transfer systems Clearance systems, etc.
Aviation services	Flight systems Reservation/boarding systems Maintenance systems Cargo systems Air traffic control systems Meteorological information systems
Railway services	Railway traffic control systems Power supply control systems Seat reservation systems
Electric power supply services	Control systems Operation monitoring systems
Gas supply services	Plant control systems Remote monitoring and control systems
Government and administrative services	Various ministry and local government information systems (handling of e-government and e-municipalities)
Medical services	Medical examination record management systems (electronic patient record systems, remote diagnostic imaging systems, electric medical equipment, etc.)
Water services	Water utility and water supply monitoring systems Water utility control systems, etc.
Logistics services	Collection and delivery management systems Cargo tracking systems Warehouse management systems

SOURCE: Government of Japan (2015)

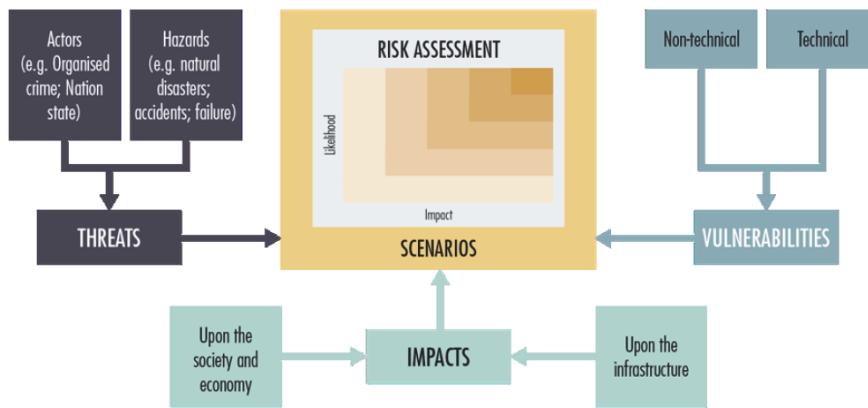
**Risk assessment**

As well as identifying CI and CII, it is also important to conduct a risk assessment of CII.<sup>104</sup> A risk assessment should identify and prioritise the risks facing CII, and communicate this information to the

### D1.3 - Critical infrastructure protection

relevant stakeholders.<sup>105</sup> Risk itself is an abstract concept that combines probability with potential impact, but for the purpose of a risk assessment, it can be broken down into three areas: threats, vulnerability and impact.<sup>106</sup> A risk assessment may include an assessment of each of these three areas.<sup>107</sup>

**Figure 1.6: Components of a national-level risk assessment**

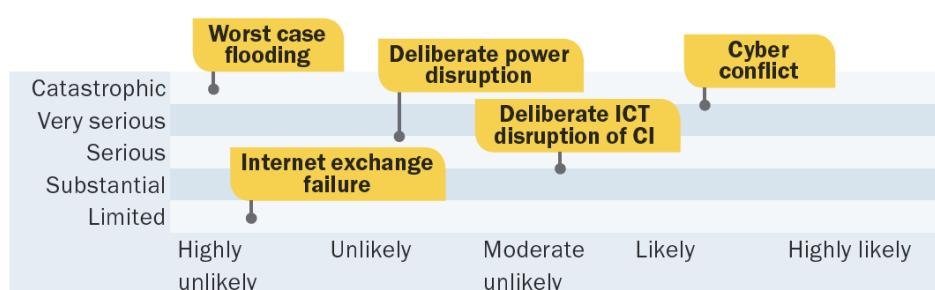


SOURCE: ENISA (2013, 9)

In the case of cybersecurity for critical infrastructure, a threat assessment may seek to identify types of actors, methods of attack, and potential targets of attacks. A vulnerability assessment may look for technical and non-technical weaknesses in the security of CII that may result from, for example, aging information infrastructure, system overload, outdated software, lack of maintenance or increasing interconnection with external networks.<sup>108</sup> Similar to the criticality assessment above, an impact assessment seeks to understand the possible consequences of a cyber-attack on CII, both in terms of type (economic, human) and severity (degree, extent, period).<sup>109</sup>

Several methods exist for conducting a national-level risk assessment. The resources presented at the end of this section should be consulted for obtaining further information about this. Both quantitative and qualitative methods can be applied, using either a centralised government framework or a decentralised model.<sup>110</sup> This can be used to create a risk profile that allows the results of the risk assessment to be prioritised and communicated. Two examples of a risk profile are provided below in Figure 1.7 and Figure 1.8.

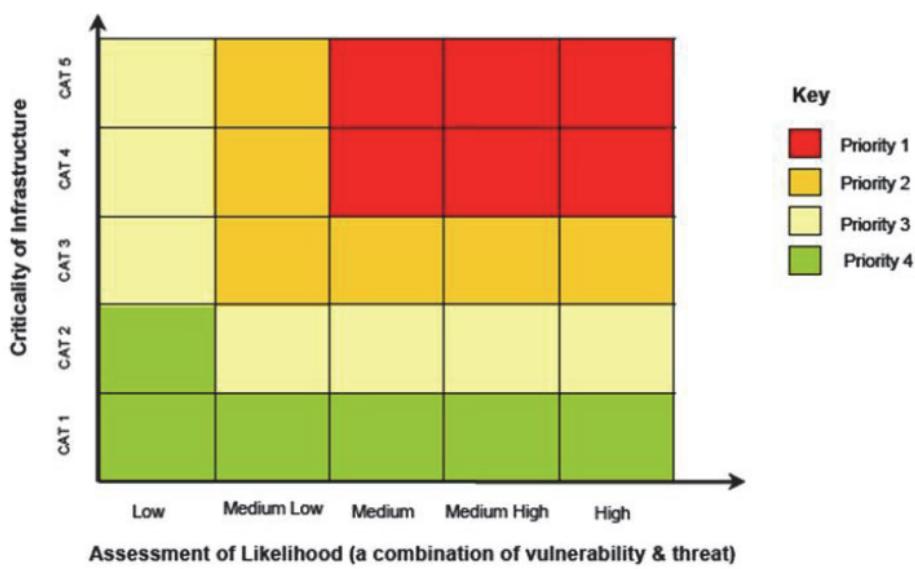
**Figure 1.7: Example of a risk profile**



SOURCE: Luijif et al. (2016, 13)

## D1.3 - Critical infrastructure protection

Figure 1.8: Example of a risk profile



SOURCE: UK Cabinet Office (2010)



- Formulate a protection and risk-management strategy for identified critical infrastructure.

With all the preceding steps completed, the next stage in CIIP is the development of a CIIP strategy.<sup>111</sup> A CIIP strategy may be incorporated into a broader national cybersecurity strategy or exist as a standalone policy document.<sup>112</sup> A protection and risk-management strategy should not only have support from the highest level of government, but also, crucially, commitment from all relevant stakeholders.<sup>113</sup> It should be a result of a coordinated multi-stakeholder process, and of open and transparent procedures.<sup>114</sup>

A CIIP protection strategy may seek to address all four areas of CIIP at a high level, namely: prevention and early warning of possible cyber-attacks; detection of cyber-attacks; reaction to cyber-attacks; and crisis management when CI and CII is disrupted.<sup>115</sup> The strategy should articulate clear intentions and SMART (Specific, Measurable, Achievable, Realistic and Time-bound) policy objectives.<sup>116</sup> A strategy may be configured to address individual risks or it may be harmonised according to a cross-sectoral or multi-risk approach.<sup>117</sup> It should outline the constraints, risk tolerances and assumptions that underlie operational risk decisions,<sup>118</sup> as well as identifying resources and timeframes, and assigning responsibilities as needed.<sup>119</sup> The strategy should also include provision to monitor implementation and effectiveness to allow a continual cycle of improvement that takes the changing risk landscape into account.<sup>120</sup>



- Outline an action plan for protecting critical national infrastructure assets, indicating which threats are to be managed centrally and which are to be managed locally; embed adequate cybersecurity risk-management processes, technical solutions and harm-mitigation measures in day-to-day administration of critical infrastructure assets.

There is an important distinction between a CIIP strategy and a CIIP action plan. Typically, a strategy seeks to communicate high-level objectives that establish an overall direction, whereas an action plan

identifies and delegates short-to-medium-term tasks to be implemented by relevant stakeholders. These may include, for example, the implementation of a risk-management cycle, which involves frequent re-evaluation of risks, followed by the development, implementation and evaluation of new security measures, with the aim of continuously improving and refining the national CIIP.<sup>121</sup>

An action plan may include, but is not restricted to, policies that address the following components:<sup>122</sup>

- Continuous gathering of threat intelligence and analysis to continuously improve the knowledge base for CIIP;
- Promotion of cyber safety principles;
- Enhancement of information sharing and other collaborative mechanisms;
- Incident response capability enhancement;
- Regular testing to detect vulnerabilities in information systems;
- Risk management;
- Cross-sectoral exercises;
- Monitoring of and agile response to environmental changes.

No action plan can be effective in the long term without taking account of the ever-changing risk landscape, and a continuous improvement cycle should be a core component of national action plans.<sup>123</sup> An improvement cycle typically incorporates a review process that evaluates the progress made by action plans, as well as assessing any changes in the threat environment or the legal and regulatory environment,<sup>124</sup> and any subsequent vulnerabilities of CII. Based on the review and the adjustments necessitated by the evolving CII-related risk profile, the national action plan can then be refined on a regular basis in order to maximise its relevance.



- Foster trust among stakeholders and create an environment conducive to mutually beneficial collaboration.

Stakeholder engagement in both the public and private spheres, as well as at both national and international level, is a key condition for the protection of national cybersecurity.<sup>125</sup> Such an environment can be created through the scheduling of regular information exchange meetings.<sup>126</sup>

Building strong networks based on trust is a key condition for activities such as swift and timely exchange of crucial information. This may be achieved most effectively where the individuals involved have similar levels of technical capacity, authority and autonomy, and a shared tolerance for risk.<sup>127</sup>

## D1.3 - Critical infrastructure protection

## Additional resources



- ENISA. 2014. Methodologies for the identification of Critical Information Infrastructure assets and services. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA).
- ENISA. 2015. Critical Information Infrastructures Protection approaches in EU. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA).
- Luijif, Eric, Tom van Schie, Theo van Ruijven & Auke Huijstra. 2016. The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. Rijswijk, Netherlands: TNO.
- Luijif, Eric, Tom van Schie & Theo van Ruijven. 2017. Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. Rijswijk, Netherlands: TNO.
- National Center of Incident readiness and Strategy for Cybersecurity. 2014. The Basic Policy of Critical Information Infrastructure Protection.
- NIST (National Institute of Standards Technology). 2014. Framework for Improving Critical Infrastructure Cybersecurity.
- OECD (Organisation for Economic Co-operation and Development). 2008. OECD Recommendations on the Protection of Critical Information Infrastructures.
- Robles, Rosslyn John, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park & J Lee. 2008. 'Common threats and vulnerabilities of critical infrastructures.' International journal of control and automation 1(1): 17-22.

## D1.4 – Crisis management

### Overview

This factor focuses on the development of national capacity to develop, review and update national crisis-management applications, functional protocols and standards. Some good practices identified are as follows:<sup>128</sup>

- Consider introduction of early warning and horizon-scanning mechanisms at the crisis management planning stages.
- Ensure that legal and regulatory frameworks are optimised to increase the efficiency of crisis management.
- Devise targeted action plans and operational procedures to improve crisis-management activities.
- Build institutional coordination mechanisms and continuously develop standardised information collection, inter-sectoral communication and public affairs handling capabilities.
- Consider the implementation of a crisis-management cell with the necessary autonomy for agile and effective crisis response.

These good practices lay the foundations of crisis management, and may already be present in some national contexts. However, in order to continuously build national resilience and crisis-management capacity, it is beneficial to undergo cycles of high-level, multi-stakeholder exercises assessing the performance of stakeholders involved in the execution of different crisis-management techniques. National-level, sectoral and cross-sectoral exercises can help authorities and other relevant stakeholders to:

- Assess the functioning and resilience of crisis-management applications, functional protocols and standards;
- Identify interdependencies and/or weaknesses;
- Practice working together, share best practices and develop trust across organisations and stakeholder groups;
- Measure improvement (over the course of multiple exercises).

Box 1.4 provides an overview of capacity-building steps for increasing national capacity in this area.

### **Box 1.4: Steps for building crisis-management capacity (D1.4)**

- |  |
|--|
| <ul style="list-style-type: none"> <li>➤ Nominate a task owner responsible for: (i) coordinating work on crisis management; and (ii) liaising with relevant public and private sector stakeholders.</li> <li>➤ Conduct a needs assessment of crisis-management measures and techniques that require assessment.</li> </ul> |
|--|

#### D1.4 - Crisis management

➤ Develop and run a realistic high-level exercise scenario for testing information flows and decision making and continuously inject new information into such a scenario during its running.

➤ Prepare tailored, sector-specific exercise evaluation and lessons learned reports based on SMART evaluation objectives and key performance indicators (KPIs) for relevant national stakeholders and international partners.

#### Capacity-building steps



➤ Nominate a task owner responsible for: (i) coordinating work on crisis management; and (ii) liaising with relevant public and private sector stakeholders.

A task owner with oversight and responsibility for activities pertaining to building crisis-management capacity should be appointed. The task owner will be responsible for facilitating the development of crisis-management capacity by overseeing the lifecycles of high-level exercises. This should entail identifying the measures and mechanisms that need testing, establishing the planning team for the exercise, leading the planning and delivery of the exercises (potentially with external expert support) and providing resources to coordinate and execute this, and ensuring that the exercise is evaluated and that lessons learned and *ad hoc* reports are shared with relevant stakeholders. Often, the organisation that identifies the need for an exercise is also the same organisation tasked with developing and running it, but external specialist support can be useful in extracting maximum value from exercises. Further details about designated task owners, as well as templates and sample materials for planning and conducting exercises, both of which are discussed in the following pages, are among the resources listed at the end this section.



No firm guideline exists as to the type of leading organisation that should have oversight of this type of activities. Examples presented in publicly available literature suggest an authority will often appoint an organisation to lead and moderate the exercise throughout its lifecycle with the help of an *ad hoc* steering committee.



➤ Conduct a needs assessment of crisis-management measures and techniques that require assessment.

At the beginning of the exercise lifecycle, the task owner will need to identify the crisis-management measures and techniques that require testing. Typically, in sectoral and cross-sectoral exercises, a focus on cooperation, coordination and communication mechanisms should be employed.



A number of different measures and techniques could be assessed during an exercise, for example: common situational awareness of participants; elements of business continuity plans; adherence to business continuity plans; speed of response; decision-making process; internal and external collaboration to address a problem; and coordination of resources, logistics and support capabilities.

On the basis of the measures and techniques selected for assessment, relevant stakeholders should be selected to perform key roles. These stakeholders will be involved in activities in this capacity area throughout subsequent steps.



The decision-making process leading to the identification of measures and techniques to be tested should also be informed by consideration of resources available throughout the exercise lifecycle, and of availability and commitment of relevant participants. The effort required to organise, run and evaluate a multi-stakeholder exercise should not be underestimated.<sup>129</sup>



- Develop and run a realistic high-level exercise scenario for testing information flows and decision making, and continuously inject new information into such a scenario during its running.

Having identified measures and techniques to be assessed, the task owner should focus on developing a plausible high-level scenario for use in testing these measures and techniques in an exercise setting. Producing a realistic, challenging and well-planned scenario is critical to ensuring both stakeholder buy-in and the success of the exercise.



A range of high-level scenarios should be considered for development before selecting one and commencing detailed exercise-planning activities. The scenario selected should be the one best suited to the goals and needs identified in the previous step.

Once a high-level scenario has been selected for development, the type, size, geographic scope and participants should be determined.

Several types of exercises may be developed. Each type may be characterised by different formats, benefits, challenges and costs. These types may be broadly clustered under two categories:

- **Discussion-based exercises:** These exercises allow participants to examine and discuss scenarios, test decision-making procedures, and develop or refine response procedures. These exercises may take the form of a seminar, workshop, table-top exercise or game.

## D1.4 - Crisis management

- **Action-based exercises:** These exercises entail the acting out of crisis-management procedures to allow testing of these procedures and the preparedness of relevant staff members to follow them.

**Table 1.4: Advantages and disadvantages of action-based and discussion-based exercises**

	Action-based exercises	Discussion-based exercises
<b>Advantages</b>	<ul style="list-style-type: none"> <li>Allows for validation of complex procedures via real-life events and scenarios</li> <li>Allows for creation of real-life remediation plans for issues/problem areas encountered.</li> </ul>	<ul style="list-style-type: none"> <li>Simpler exercise mechanics allows for engaging broader, non-technical audiences and inclusion of awareness-raising aspects</li> <li>Comparatively limited resource requirements</li> <li>Shorter planning and execution cycle.</li> </ul>
<b>Disadvantages</b>	<ul style="list-style-type: none"> <li>Requires specialist target audience to ensure exercise implementation is successful</li> <li>Longer planning and execution cycle</li> <li>Greater resource.</li> </ul>	<ul style="list-style-type: none"> <li>Injects are hypothetical and pre-coordinated</li> <li>May not generate the tension and stress of real-life incidents.</li> </ul>

SOURCE: Kick (2014)

The size of the exercise will depend largely on the type of exercise to be developed, as well as on the human, technical and financial resources available to planners.



Consider carefully the advantages and disadvantages of exercises of different size. Consider whether the exercise size selected aligns well with the overarching goals and suits any human, technical, financial and time constraints under which organisers may be operating.

The **geographic scope** of the exercise should be determined. Considerations around this aspect may influence the size of the exercise to be implemented. Even with limited resources available, an exercise with a broad geographic scope may be run, for example by reducing the complexity associated with its mechanics or the number of its participants.



Exercises with a broader geographic scope may prove more challenging to implement. However, this often allows the benefits the exercise to be spread across a larger number of organisations/individuals.



The geographic scope of an exercise may be determined by the content of its high-level scenario. Consider that certain events may have cascading effects onto assets in regions and countries other than those considered initially, or may be geographically dispersed by nature.

Lastly, before entering the exercise-development phase, participants should be identified. Which participating organisations to involve in an exercise is largely a function of the measures and techniques that the exercises are designed to assess, as well as the type of exercise that will be implemented.



The exercise should involve representative(s) at the appropriate decision-making level from key stakeholder organisations involved in the measures or techniques to be assessed.

Once the exercise scenario, type, size, geographic scope and participants have been identified, detailed **planning and development** of the exercise should start. The duration of the planning and development phase depends on a number of factors. Operational exercises require planning cycles of at least one calendar year, whereas smaller-scale, discussion-based exercises are likely to require several months of planning.<sup>130</sup>



During the first planning round for a particular exercise type, ensure that extra time is available to the planning team to work out all details, secure participants' commitment and build consensus around the exercise concept.

When developing the exercise scenario, the planning team should start by building on the high-level concept selected at the start of this process. The development team should discuss different iterations of the exercise scenario both internally and with representatives of key stakeholders. The objective should be to ensure that the scenario is as realistic as possible, while being closely aligned with the goals and needs of the organisers. This will reduce the risk of participants challenging the scenario or struggling to absorb it during the exercise.<sup>131</sup> Scenario examples and planning templates are provided in the resources listed at the end of this section.

During the course of the exercise, the scenario will need to be managed and adapted according to the responses and actions of participants. To this end, pre-planned '**injects**' of new information should be prepared and subsequently used by the exercise moderator. Injects should resemble real-life incidents and be presented based on real-life communication (e.g. by presenting incomplete, flawed information and/or using a media-like approach). Most injects should be planned in advance of the exercise being undertaken.<sup>132</sup>

## D1.4 - Crisis management



Not only should the scenario be perceived as realistic by stakeholders and participants, it should also retain sufficient flexibility to evolve and adapt during the course of the exercise according to the actions and decisions taken by participants.



Not all of the injects that have been prepared will necessarily be used during an exercise. The exercise manager should use these on the basis of information received on how participants are engaging and dealing with the pre-planned scenario, as relayed by the exercise monitors. To facilitate this process, a range of injects allowing for different scenario pathways should be prepared.

Once the planning and development of the exercise are complete, the exercise itself should be conducted. The recruitment of participants is the next key phase, and some hurdles in obtaining the desired participants might include the participants' lack of available resources, difficulty in recognising the potential benefits of participation, or concerns about confidentiality.<sup>133</sup> In order to mitigate these challenges, it may be beneficial to invest in raising awareness about the envisaged benefits of the exercise and to ensure that participants are included from the onset of the planning process.<sup>134</sup> Creating incentives (e.g. financial support) and generating trust by ensuring transparency about how information will be utilised may also be helpful. Furthermore, maintaining an inclusive, multi-stakeholder approach can help develop a shared sense of ownership among participating stakeholders.<sup>135</sup> Part of this is the establishment of a media policy by the exercise organisers in order to avoid misconceptions about the exercise.<sup>136</sup>



### Cyber Storm exercises<sup>137</sup>

Cyber Storm is a series of bi-annual, full-scale exercises organised by the United States Department of Homeland Security (DHS). The Cyber Storm series is designed to strengthen cybersecurity preparedness and response capabilities across different levels, enabling participants to exercise policies, processes and procedures for identifying and responding to a multi-sector cyber-attack targeting critical infrastructure.

The 2016 iteration of Cyber Storm (Cyber Storm V) required 18 months of planning and delivery work. Activities were divided into five phases, namely: Scoping, Design and Development, Preparation, Conduct, and Evaluation Phases. Throughout the exercise lifecycle, planners engaged with a range of communities and stakeholders. This led to the exercise having over 1,200 participants, representing a broad spectrum of public and private sector organisations from both within and outside the United States.

The cyber-specific scenario of Cyber Storm V leveraged existing weaknesses in Internet protocols and services to disrupt routing methodologies, the Domain Name System (DNS) and public key infrastructure. Addressing the problems created by the scenario required a coordinated government and private sector response.

According to the organiser, Cyber Storm V was successful in providing participants with an opportunity to examine the evolution of cyber response capabilities and identify current gaps and challenges in responding to a coordinated cyber-enabled attack with global impacts.



- Prepare tailored, sector-specific exercise evaluation and lessons learned reports based on SMART evaluation objectives and KPIs for relevant national stakeholders and international partners.

Evaluations synthesise observations about areas that merit attention for further improvement. They are designed to disseminate lessons learned from conducting the exercise, which could include areas for improvement in organisational structures and processes, mechanisms and various other areas. Evaluations may aim to identify the major impediments to the success of the continuity plan tested, the necessary skills for successful execution, and weak links and vulnerabilities in coordination, decision making and communications. Evaluations may develop recommendations to improve these and other areas.<sup>138</sup>

An evaluation process should comprise the following phases:

1. **Setting evaluation objectives:** Exercises can be a prime method of reinforcing strategic crisis cooperation and management objectives, as long as the objectives are clear, feasible and attainable. SMART objectives for the exercise should be identified by the task lead and stakeholders involved at the very onset of the planning phase. Objectives to be investigated during an evaluation could include, for example: (i) major obstacles to the success of the continuity plans tested; (ii) skills required for successful implementation; and (iii) interdependencies and weak links in the chains of communications tested. The evaluation process and supporting data to be collected should be designed in advance. These might include monitoring report templates and guidelines for completing them, preparing stakeholder questionnaires, and identifying possible debriefing moments for the exercise team at interim stages of the exercise.<sup>139</sup>
2. **After-action review:** The optimal point for conducting an evaluation is directly after the exercise, as this enables organisers to obtain data from the various participants and role-players while the experience is fresh, and also to ensure that results of the evaluation are communicated before the momentum behind the exercise dissipates.<sup>140</sup>

The evaluation should culminate in the preparation of a number of reports, presenting activities completed, lessons learned and recommendations to a range of stakeholders. Given the sensitivity of issues tested during crisis-management exercises, multiple reports targeting different audience groups are likely to be devised. For example, as part of complex exercises, an individual participating stakeholder may receive a unique, confidential report, presenting detailed observations and recommendations for the individual's organisation. Usually, an internal consensus report for distribution among all stakeholders involved should be prepared, presenting general findings and recommendations pertaining to the sector or mechanisms that were tested during the exercise. The adoption of a collaborative and inclusive evaluation

## D1.4 - Crisis management

process that involves participants in the formulation of conclusions and recommendations should be considered. This could give stakeholders greater ownership of the evaluation process, thereby increasing the likelihood of a high level of commitment in responses to recommendations.

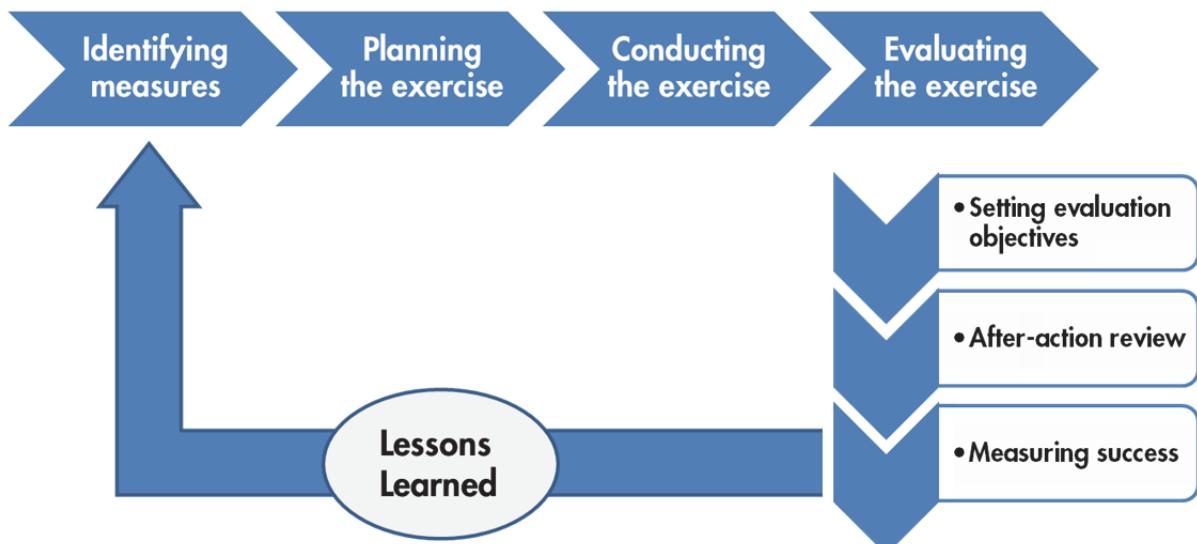
Finally, depending on the size and ambition of the exercise, a report for the general public may be issued, presenting activities undertaken but without discussing any weaknesses, recommendations or findings stemming from the exercise.<sup>141</sup>

3. **Measuring success:** In the concluding phase of the evaluation, the exercise team should focus on assessing whether the exercise broadly achieved the objectives it set out to pursue, and whether this was done in an effective manner by the exercise team. It may be helpful to produce separate templates and documents pertaining to the evaluation of the exercise's management and running to ensure that lessons are collected and acted upon, rather than scattered among those pertaining to the measures being tested.<sup>142</sup>

Finally, evaluation activities should be seen as a link within a broader, continuous cycle of exercises. Evaluations provide opportunities for learning and development, and findings and recommendations stemming from the evaluation should be taken into account during the planning and execution phases of future exercises, with a view to embedding lessons learned and good practices identified.

Figure 1.9 provides an overview of how the evaluation process can be included within the broader exercise cycle.

Figure 1.9: Exercise and evaluation cycles



SOURCE: RAND Europe elaboration of ENISA (2009)

## Additional resources



- European Network and Information Security Agency. 2009. Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks. Heraklion, Greece: European Network and Information Security Agency.
- European Union Agency for Network and Information Security. 2016. Report on cyber crisis cooperation and management: Common practices of EU-level crisis management and applicability to cyber crises. Heraklion, Greece: European Network and Information Security Agency.
- Federal Office of Civil Protection and Disaster Assistance (BBK). 2011. Guideline for Strategic Crisis Management Exercises. Bonn: BBK.
- Kick, Jason. 2014. Cyber Exercise Playbook. Wiesbaden: The MITRE Corporation.

## D1.5 – Cyber defence

### Overview

ICTs are increasingly integrated into all parts of military activities and products, from command and control and intelligence-gathering mechanisms, to logistics systems, high-precision weapons, and positioning and information systems.<sup>143</sup> As ICTs become more embedded in military capabilities, they become more attractive as a target for cyber-attacks.

In response, states need to engage in a comprehensive and integrated effort to develop capabilities and resilience in both the cybersecurity and cyber defence areas. This was acknowledged, for example, by NATO's decision to recognise cyberspace as the fifth military domain along with land, sea, air and space.<sup>144</sup>

The following pages outline a series of capacity-building steps to guide national governments and senior armed forces personnel in the development and implementation of national cyber defence capabilities. These steps are outlined in Box 1.5 below and described in more detail in the pages that follow.

### **Box 1.5: Steps for increasing cyber defence consideration (D1.5)**

- Nominate a central task owner for cyber defence strategy.
- Conduct a risk assessment that includes analysis of the threat landscape and existing vulnerabilities.
- Develop a cyber defence strategy.
- Implement the cyber defence strategy and continuously review and update its implementation approach in light of results achieved and changes in the threat and operational landscapes.
- Establish specialised working groups within the military that are integrated into a more complex cyber defence structure.
- Develop a cyber defence doctrine.
- Evaluate the cyber defence strategy and implement improvements.

### *Capacity-building steps*



- Nominate a central task owner for cyber defence strategy.

The first step in developing effective cyber defence capabilities is the designation of a task owner to lead the development, coordination and implementation of a cyber defence strategy on a national level. Depending on existing organisational structures, this task owner may be within the military or within the national ministry of defence.

During initial stages of development, the task owner should act as the central point of contact and central coordinating body for cybersecurity and cyber defence within the defence sector. It is also likely, even in the absence of an existing centralised coordinating body, that some degree of cyber defence activity will

already exist within different areas of a country's military and defence provision. It is the role of the task owner to understand and map this existing provision, and to incorporate these elements into the development of a coherent national cyber defence strategy.



### Examples of cyber defence task owners

In the UK, the development, integration and coordination of cyber defence capabilities is led by **Joint Forces Command**,<sup>145</sup> which is the organisation within the UK Government's Ministry of Defence (MOD) that provides coordination and support across all defence domains and military forces.<sup>146</sup>

In the Czech Republic, cyber defence is led by the **Communications and Information Systems Agency (CISA)**, which is the organisation within the Support Division of the Czech Armed Forces that is responsible for military communication and information systems.<sup>147</sup>

In the United States, the Department of Defense (DoD) leads on military cyber defence. There is clear distinction between the roles of the DoD and the DHS: the DoD secures military systems, investigates cybercrimes under military jurisdiction, gathers intelligence on foreign cyber threats and protects the .mil Internet domain; while the DHS protects civilian government networks and infrastructure, including the .gov Internet domain.<sup>148</sup>



- Conduct a risk assessment that includes analysis of the threat landscape and existing vulnerabilities.

During the initial development of a national cyber defence strategy, it is important to conduct a **risk assessment** that develops an understanding of both the **threat landscape** and the potential areas of **vulnerability** within the defence architecture.

The **threat landscape** within cyber defence is broad, complex and rapidly changing due to the ease of access to complex information and communication systems by a wide range of state and non-state actors, as well as the rapid pace of technological development.<sup>149</sup> The increasing integration of computer systems within military capabilities, together with increasingly open access to the Internet, has resulted in a greater number and variety of adversaries who are able to attack and compromise the capabilities of national militaries.<sup>150</sup> Conducting an analysis of the threat landscape involves mapping both the range of adversaries who may target a national military (including criminal organisations, foreign intelligence services, foreign state militaries, non-state actors, hacktivists and others)<sup>151</sup> and the range of techniques that may be deployed by these adversaries (including malware, botnets, logic bombs and Advanced Persistent Threats (APTs)).<sup>152</sup>

In addition to an initial threat assessment, it is also important to both map and understand the particular **vulnerabilities** that exist within current and future defence systems. As already noted, the majority of defence capabilities are increasingly reliant on ICT.<sup>153</sup> An initial vulnerability assessment should be conducted to identify the ways in which these systems may be compromised and outline the potential impact of a targeted cyber-attack.

## D1.5 - Cyber defence

By combining an understanding of the threat landscape with an analysis of vulnerabilities, it is possible to produce a single **risk assessment** that identifies and prioritises competing cyber defence demands. This, in turn, can be used as the basis for a more tailored and pragmatic cyber defence strategy that balances practicalities, available resources and risks. Such a strategy would aim to ensure that minimum protection measures are applied where appropriate, and that particular emphasis is placed on those areas of cyber defence that are most threatened, most vulnerable and most important to the effective functioning and deployment of a national military.<sup>154</sup>



- Develop a cyber defence strategy.

Building on the initial risk assessment, the next step is to develop a cyber defence strategy that seeks to actively mitigate the risks identified. This strategy may be produced as a standalone document, or it may form part of a broader national defence strategy.



The **Dutch Ministry of Defence** has developed a standalone national *Cyber Defence Strategy* that is separate from their other national-level defence strategies, such as the *Dutch International Security Strategy*<sup>155</sup> or the *Netherlands' Defence Industry Strategy*.<sup>156</sup> In contrast, the **UK Government** incorporates its cyber defence strategy into a broader *National Security Strategy and Strategic Defence & Security Review*,<sup>157</sup> as opposed to publishing a separate cyber defence strategy.<sup>158</sup>

A useful first step in developing a national cyber defence strategy is to deconstruct the concept of cyber defence into its constituent parts. This breakdown will vary depending on the local context, but many of the high-level categorisations are common across all countries and armed forces.



As an initial point of reference, the cyber defence strategies of other nations may be consulted to provide an overview of the different ways in which a cyber defence strategy can be structured.

One way of breaking down cyber defence is to divide it into three areas:<sup>159</sup>

- Capability
- Organisation
- Coordination.

**Capability** outlines the desired cyber defence capabilities, and details technical and operational requirements. This may include any number of the following areas:

- **Passive cyber defence**, which considers the measures needed to detect cyber-attacks, protect networks and computer systems from attack, monitor internal data traffic to detect compromised systems, and mitigate the impact of a successful cyber-attack;<sup>160</sup>

- **Procurement and supply chain reassurance**, which focuses specifically on ensuring that the supply chain of computer equipment and components is secured in such a way that malicious elements are not introduced either to individual computers or to network systems;<sup>161</sup>



#### UK Defence Cyber Protection Partnership

The UK Defence Cyber Protection Partnership (DCPP) is a government-led initiative that aims to improve the security of technical supply chains without compromising investment in cybersecurity from the private sector. As part of the DCPP, a set of security standards have been developed that are applied when contracting with the MOD, and an online tool has been published that enables users to complete a cyber equipment risk assessment and supplier assurance questionnaire.<sup>162</sup>

- **Incident response**, which primarily focuses on CERTs and their ability to respond to a cyber-attack, but includes all elements involved in preventing and responding to cyber-attacks;
- **Active cyber defence**, which is the proactive deployment of operational cyber assets to actively prevent an attack and ensure the full functioning of defence equipment;<sup>163</sup>
- **Offensive cyber operations**, which refers to the ability to target, attack, disrupt and disable the information and computing systems of an adversary;<sup>164</sup>
- **Cyber intelligence**, which refers to the ability to anticipate threats, collect information on adversaries and conduct cyber counterintelligence analyses that focus on identifying and attributing blame to particular actors following an attack;<sup>165</sup>
- **Cyber deterrence**, which seeks to reduce the probability of being attacked by an adversary by clearly communicating their reduced probability of success, and by increasing the potential cost of an attack by guaranteeing appropriate retaliation;<sup>166</sup>
- **Domestic cyber emergency response**, which refers to the ability of the military to support civilian cybersecurity when required, in particular during large-scale incidents when the civilian response is overwhelmed.<sup>167</sup>



Regardless of external protective measures, an advanced cybersecurity strategy assumes that an adversary will have sufficient capacity to compromise any given network. Perimeter defences should not be fully relied on, and appropriate protection of information and information-exchange mechanisms should be implemented internally within a system. This is in addition to, rather than instead of, any existing perimeter protection that has already been applied.<sup>168</sup>

## D1.5 - Cyber defence



### US cyber intelligence

There are a number of ways to respond to a cyber-attack, but it is difficult to fully respond without knowing who conducted the attack itself. In one instance, the US was able to use digital forensic techniques to attribute commercial cyber espionage activity to China. This enabled the US government to express their concerns to China regarding the use of cyber intelligence, and the potential impact on areas such as intellectual property (IP) and US economic competitiveness.<sup>169</sup>

Secondly, **organisation** refers to the range of measures that can be implemented within existing defence organisations to help deliver the aforementioned cyber defence capabilities. Areas covered by this category include:

- **Professional skills**, which refers to the recruitment, retention and training of sufficiently skilled cybersecurity professionals;<sup>170</sup>



National armed forces and public defence organisations are typically unable to match the salaries available within the private sector. However, there are other ways of attracting cybersecurity professionals into defence roles, such as providing a rewarding career path in an interesting environment, and facilitating personal development and training.<sup>171</sup>



### UK MOD Defence Cyber School

The UK Government established the Defence Cyber School (DCS) in April 2017 as a centre of excellence within the MOD. The aim of the DCS is to deliver cyber defence training and education to the military and wider government, and to provide a platform that helps to facilitate stronger relationships with industry and academia when developing a skilled national cybersecurity workforce. The DCS also provides a testing facility that allows the MOD to test the resilience of UK systems.<sup>172</sup>

- **Facilities**, which refers to the physical infrastructure that is needed to establish and run particular cyber defence tasks, including cyber training centres, cyber research laboratories, cyber testing facilities and cyber ranges;<sup>173</sup>
- **Technical equipment**, which refers to the technical capabilities required to effectively operate in cyberspace, including protecting existing equipment, responding to cyber-attacks, and conducting offensive cyber operations;<sup>174</sup>
- **Internal structure**, which refers to the subdivision and specialisation of cyber defence teams within different areas of the armed forces, and the effective coordination and central direction provided by the overall task owner.

Finally, **coordination** refers to the management of public and private sector actors, their involvement in the defence sphere, and the management of the defence sector's engagement with the civilian domain. Cyber defence and cybersecurity are inherently cross-sectoral and cross-domain. Moreover, militaries, national governments, private sector firms and international actors are all mutually dependent on secure ICT in a number of ways.<sup>175</sup> For example, defence organisations typically rely on public and private sector infrastructure, such as telecommunication systems and the procurement of technical capabilities, in order to effectively conduct their operations. In return, defence organisations can provide both public and private sector actors with valuable services, such as cyber intelligence on foreign actors, and support to civilian emergencies when civilian capacity and capabilities are saturated. The defence, public and private sectors can also benefit from mutual opportunities for learning and development across sectors, and can exploit the pooling of information and resources to strengthen common cyber skills and technical capabilities.

Ensuring effective relationships, partnerships and coordination across the cyber domain is an important aspect of any cyber defence strategy. There is no single method for building these relationships, but the following general approaches may be used to help facilitate effective coordination:

- Encourage **public-private partnerships**<sup>176</sup> and less formal **collaboration** on issues such as joint research programmes, and education and skills development programmes.<sup>177</sup>
- Provide **secure platforms** for communication between different stakeholders.<sup>178</sup>
- Establish clear **separation of roles and responsibilities** across sectors and domains, particularly in possible areas of overlap such as civil cyber intelligence and civil cyber incident response.<sup>179</sup>
- Develop a **central cyber defence hub**, such as a national cyber defence research centre.<sup>180</sup>
- Provide **supporting legislation** that ensures confidence and security when sharing information and intelligence.<sup>181</sup>
- **Engage and cooperate with international allies** and partners as appropriate given the national context.



#### NATO Industry Cyber Partnership

The NATO Industry Cyber Partnership aims to build collaboration within cyber defence between NATO, its member states and industry. The partnership has a number of goals, including: improving the sharing of information and expertise in the cyber domain; facilitating communication networks between industry, enterprise and NATO member states; improving NATO's cyber defence supply chains; and facilitating an increased level of industry involvement in multinational *Smart Defence* projects.<sup>182</sup>

## D1.5 - Cyber defence



- Implement the cyber defence strategy, and continuously review and update its implementation approach in light of results achieved and changes in the threat and operational landscapes.

A cyber defence strategy serves as a framework for implementation of cyber defence activities and will often include long-term objectives, with task owners assigned across different focus areas.



The Dutch National Cyber Security Strategy 2, which considers both cyber defence and cybersecurity more broadly, includes an extended table in Annex 1 that outlines individual tasks, assigns government department responsibilities for implementation, and indicates a required task completion date.<sup>183</sup>

In the cyber domain, however, it is not sufficient to simply develop and review a strategy according to typical strategy-development timelines, which are often in the order of magnitude of approximately five years. Cybersecurity and cyber defence are dynamic environments, and it is important that any implementation is sufficiently agile to keep up with and respond to changes in the cyber domain. This includes the ability to identify emerging threats, develop new capabilities and adapt funding levels, organisational structures and operational processes according to changes in the cyber ecosystem.<sup>184</sup> Even in advanced military structures, it is acknowledged that developing agile cyber defence processes is difficult within a traditional military context, but there are a number of mechanisms that can be implemented to help facilitate and develop more dynamic processes, including:

- Introducing **frequent review cycles** that evaluate current cyber defence provisions and trends, and provide short-term recommendations in between strategic review cycles.



In the US DoD Cyber Strategy, the DoD commits to a comprehensive annual review of its ability to defend against significant cyber-attacks.<sup>185</sup>

- **Supporting research and development** in the cyber defence domain through, for example, publicly funded research institutions, public-private partnerships and collaboration with academia;



### The R-Cloud framework

The R-Cloud framework is a mechanism that provides access to funding for private sector firms ranging from sole traders to SMEs, academic institutions and large defence organisations.<sup>186</sup> It operates in a number of different domains, including cybersecurity and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance).<sup>187</sup> The framework is administered by the Defence Science and Technology Laboratory (Dstl), which is an executive agency of the UK Government, and fully funded by the UK MOD.<sup>188</sup>

- Developing effective **information-sharing** mechanisms and tools across the defence, public, private and academic sectors to facilitate sharing of information on areas such as threat intelligence and vulnerability assessments.<sup>189</sup>



Effective information sharing can be difficult to achieve due to commercial and national security sensitivities. Information-sharing mechanisms should be supported by legislation that provides sufficient protection to all relevant stakeholders, which in turn helps build trust and facilitates increased levels of information sharing.<sup>190</sup>



- Establish specialised working groups within the military that are integrated into a more complex cyber defence structure.

As cyber defence becomes a more established function within military and defence organisations, it is likely that more complex organisational structures will be required to enable closer integration and greater degrees of specialisation. It is important to maintain an overarching task owner, but as the scale of cyber defence capabilities and operations grows, it may become more effective to introduce additional organisational structures or subsidiary teams that deliver more specialised cyber defence capabilities. The central task owner would focus exclusively on coordination, management and strategic development, whereas the subsidiary teams would focus more on operational capacity or specialised supporting roles.

## D1.5 - Cyber defence

**Dutch cyber defence organisational structure**

Since the first Dutch national cybersecurity strategy was published in 2011, the country's national cyber defence organisational structure has increased in complexity in line with growing cyber defence demands and capabilities. In January 2012, an initial military **Task Force Cyber** was established to develop cyber defence capacity within the military, including operational capabilities. In September 2014, this Task Force Cyber was replaced by a joint **Defence Cyber Command**, which was set up as the overarching lead for cyber defence in the Dutch Armed Forces, and covers all four services – army, navy, air force and military police. In parallel, the **Joint Information Management Command (JIMC)** has been operational since 2013, and is responsible for ensuring the resilience of the networks and systems of the defence organisation. Now structured under the JIMC, the **Defence Computer Emergency Response Team (DefCERT)** became fully operational with an expanded capacity in 2012, and is responsible for the security of the main defence networks. The role of the **Netherlands Defence Intelligence and Security Service (DISS)** has also been expanded, and together with its original role of providing intelligence and security information to the Ministry of Defence and the Netherlands Armed Forces, DISS is tasked with gathering information and conducting analysis on computer network defence and exploitation, and developing computer network attack capabilities. The **Joint Sigint Cyber Unit** was established in June 2014 as a support unit under both DISS and the General Intelligence and Security Service, and aims to improve cyber intelligence by pooling cyber expertise and driving technical innovation. Finally, offensive cyber capabilities continue to be administered under the overall responsibility of the **Chief of Defence**.<sup>191</sup>



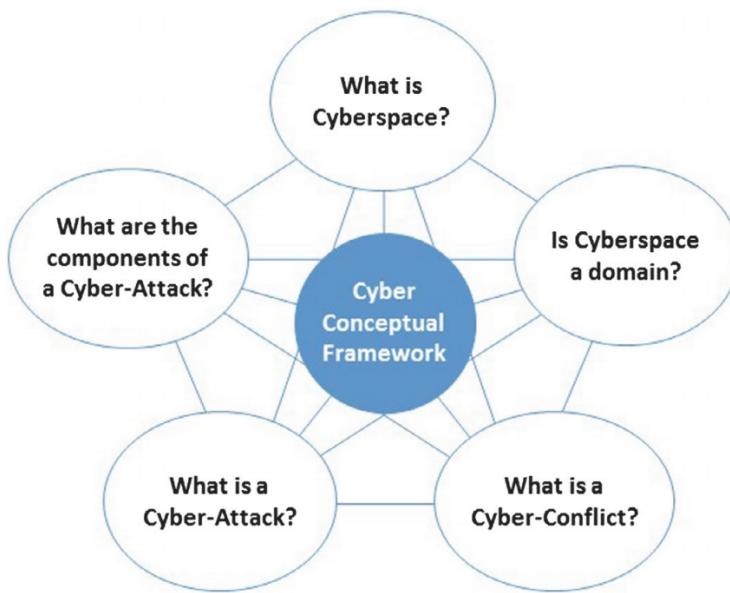
- Develop a cyber defence doctrine.

Cyber defence is increasingly recognised as a military domain on a national and international level, as evidenced by NATO's recognition in 2016 of cyberspace as a domain of operations equivalent to land, sea, air and space.<sup>192</sup> In the traditional military domains, military doctrine has been developed and refined over many years to provide the basic principles upon which tactics are developed and implemented.<sup>193</sup> In cybersecurity, however, these fundamental principles are less developed,<sup>194</sup> which may be due in part to the relative novelty, complexity and speed of change of cyberspace and its application within the defence sphere.

Once developed, a cyber defence doctrine can be used to provide a consistent set principles and rules on which to develop tactics, techniques, procedures and training.<sup>195</sup> However, this doctrine should be developed with cognisance of the local context of a given state, since the conceptualisation of warfare differs according to national capabilities and the manner in which those capabilities are deployed.<sup>196</sup>

A basic framework for a cyber defence doctrine has been developed in the academic literature, and identifies five questions, presented in Figure 1.9 below, that should be considered when developing a cyber defence doctrine.

**Figure 1.10: Basic framework for a cyber doctrine**



SOURCE: Ormrod & Turnbull (2016)



- Evaluate the cyber defence strategy and implement improvements.

The final stage in developing an effective cyber defence capacity is the evaluation and subsequent redevelopment or refinement of the cyber defence strategy. This should build on the general framework for performance audits, which typically consider the initial objectives of a strategy, and compares these to the activities, outputs, outcomes and wider results that have been achieved during the implementation process.<sup>197</sup> In the case of cyber defence strategies, this may include the use of metrics to assess capacity development, proficiency and ability to respond to contingencies,<sup>198</sup> although there are few available studies that provide detailed guidance on specific metrics or other measures of performance.



### EU military cyber defence stocktaking framework

Although not strictly a strategy evaluation, a RAND Europe stocktaking study of EU military cyber defence capabilities provides a useful framework on which to base a cyber defence evaluation. The study separates cyber defence capabilities according to seven lines of development: *Doctrine, Organisation, Training, Personnel, Leadership, Facilities and Interoperability*. It defines five levels of proficiency: *Non-existent Initial, Defined, Balanced and Optimised*. A series of indicators, weightings and assumptions are then defined, and may be used as the basis for establishing tailored metrics for an individual evaluation of a cyber defence strategy.<sup>199</sup>

### Additional resources



- Dutch Ministry of Defence. 2012. The Defence Cyber Strategy. Dutch Ministry of Defence.
- ENISA. 2016. Good Practice Guide Designing and Implementing National Cyber Security Strategies. Athens: ENISA.
- Klimberg, Alexander (Ed). 2012. National Cyber Security Framework Manual. Tallinn: NATO CCD COE Publication.
- UK Government House of Commons Defence Committee. 2012. Defence and Cyber-Security: Sixth Report of Session 2012–13. House of Commons, London: The Stationery Office Limited.
- Ormrod, D. & A. Turnbull. 2016. The cyber conceptual framework for developing military doctrine. *Defence studies*. Vol 16(3) pp. 270-298.
- Osula, Anna-Maria, & Kadri Kaska. 2013. National Cyber Security Strategy Guidelines. Tallinn: NATO CCD COE Publication.
- Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez. 2013. Stocktaking study of military cyber defence capabilities in the European Union (milCybeCAP): Unclassified Summary. Santa Monica, UK: RAND Corporation.
- US Department of Defense. 2015. The DOD Cyber Strategy. Department of Defense.

## D1.6 – Communications redundancy

### Overview

This factor looks at governments' capacity to identify, map and leverage digital and communications redundancy among national stakeholders. In this context, digital and communications redundancy is defined as the national capacity to identify, maintain and develop digital and non-digital backup communication networks for emergency responders.<sup>200</sup>

Emergency responders are the individuals and organisations that prepare for and respond to emergency situations. This typically includes:<sup>201</sup>

- **Day-to-day operations**, such as individual accidents, medical emergencies and low-level criminal activity;
- Supporting large **planned events**, such as sporting fixtures, music concerts, festivals and protests;
- Responding to significant **unplanned events**, such natural disasters, major incidents and terrorist attacks.

While emergency response and crisis management remains a fundamental role of central government, the number of relevant stakeholders outside of central government has increased in recent years due to a trend towards the decentralisation and privatisation of some traditional government services.<sup>202</sup> Public sector emergency services are often organised on both a local and national level, and typically include disaster risk-management agencies, armed forces, and police, health and fire services.<sup>203</sup> In many countries, emergency response has become increasingly decentralised, with crisis management exercised at a sub-national level, and central government providing coordination and support when necessary.<sup>204</sup> Privatisation of critical infrastructure (such as information and communications networks) and emergency response capabilities (such as health care systems) has also increased, as has citizen engagement and self-organisation through NGOs and civil society organisations (CSOs).<sup>205</sup>

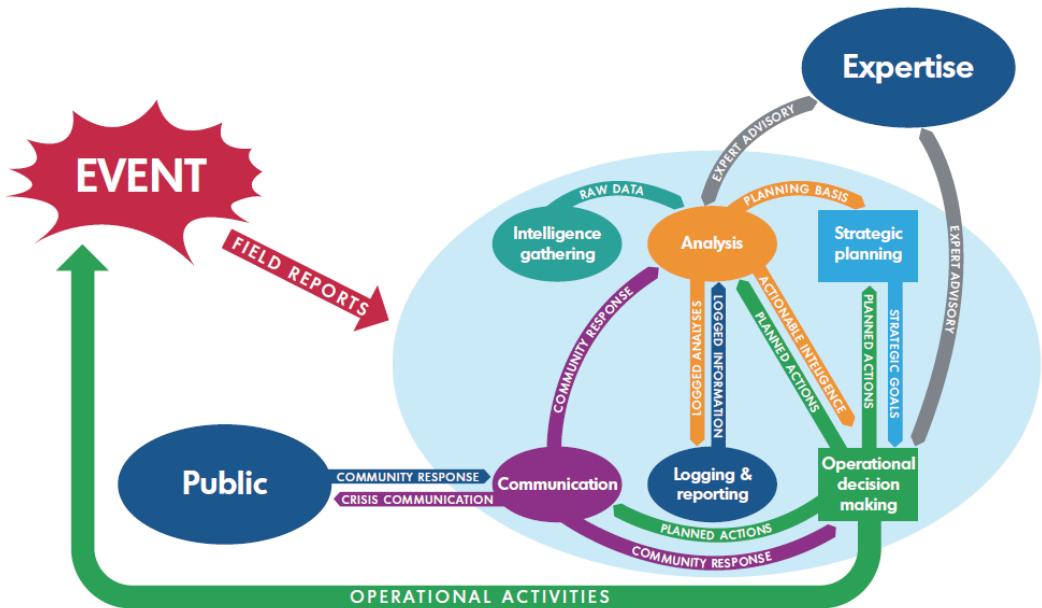
Communication during crisis management is a complex web of bidirectional information flows between the various different stakeholders involved in emergency response. For example, responders on the ground should be able to communicate to coordinate their operational activities. They also need to feed back information into a centralised management structure which may conduct the following: operational decision making, strategic planning, intelligence gathering and analysis, logging and reporting, collation of external advice, and communication with external private and community stakeholders.<sup>206</sup>

Communication within and between each of these functions is vital when providing an effective response to an emergency.<sup>207</sup> If an incident occurs that causes a failure in a digital communications network, it is important that communication channels between emergency responders remain available in order to maintain cooperation, interoperability and functionality.<sup>208</sup> An interruption or failure of the emergency response communication systems can have a significant adverse impact on the emergency response. This can result, for example, from reduced coordination and situational awareness among responders; reduced ability of analysts and decision makers to receive, analyse, discuss and disseminate information; and reduced communication with private organisations, NGOs, CSOs and the wider population to

## D1.6 – Communications redundancy

coordinate response and provide reassurance.<sup>209</sup> This can lead to a slower response time and a less effective response, which may ultimately result in an increased loss of human life, increased number of injuries, greater property or material damage, lower public perception of and confidence in the response, and greater uncertainty among the general public.<sup>210</sup>

**Figure 1.11: Basic crisis communication channels**



SOURCE: ENISA (2014, 20)

There are a number of factors that may cause an interruption or failure of emergency response communication systems, including physical damage to information and communications infrastructure, cyber-attacks, or capacity failures due to a surge in network traffic following an event. These failures are mainly limited to significant unplanned incidents, such as natural disasters or terrorist attacks, as opposed to day-to-day operations or planned events.<sup>211</sup> That said, unexpected interruptions due to technical error, human error or cyber-attack may also occur.<sup>212</sup>

It is therefore important to establish crisis communication backup systems that maintain communication networks during crisis periods. This can be achieved using a number of different measures, including the prioritisation of emergency responders on commercial networks, and the setup of auxiliary communications systems using radio or satellite communication technology, supported by independent power supplies.<sup>213</sup> It is most important to establish effective voice communication (often referred to as ‘Mission Critical Voice’), although data communication (‘Mission Critical Data’) and geographic information systems (GIS) are increasingly important in emergency response.<sup>214</sup>

Box 1.6 provides an overview of capacity-building steps for increasing national capacity in this area, which are discussed in more detail below.

### Box 1.6: Steps for improving communications redundancy (D1.6)

- Identify and map emergency response assets, possibly including details of their location and their designated operators.
- Allocate appropriate resources to hardware integration, technology stress testing, personnel training and crisis-simulation drills.
- Distribute communication across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

#### *Capacity-building steps*

The following section identifies a number of steps that may be taken to improve the provision of emergency response backup communications systems. However, there are few publicly available resources in this area.



- Identify and map emergency response assets, possibly including details of their location and their designated operators.

The coordination of emergency preparedness communications could benefit from having a centralised focal point. This focal point should be tasked with producing, in preparation for a possible crisis, an inventory of existing emergency response assets in various areas, as well as defining the potential base of end-users for these assets at the nationwide level.<sup>215</sup> As part of national strategies and action plans there may also be benefits to incorporating a requirement that obliges applicants to demonstrate how envisaged emergency communications projects are secure, which includes the provision of information on assets, networks and systems to aid the mapping process.<sup>216</sup> The standardised identification and mapping of emergency response assets is helpful for the capability assessment of response-level communications of participating areas on emergency response capabilities and needs,<sup>217</sup> and allows public safety agencies to gain strategic oversight of available emergency communications resources.<sup>218</sup> It can also highlight the concentration of assets in particular areas, particularly in urban settings, underscoring any system vulnerabilities that may become targets for catastrophic events,<sup>219</sup> as well as redundant communications among stakeholders, thereby enhancing the efficiency of resources.<sup>220</sup>



- Allocate appropriate resources to hardware integration, technology stress testing, personnel training and crisis-simulation drills.

It is important to continuously modernise and leverage technologies and hardware integration, as well as to have the ability to rapidly deploy emergency response equipment, services and logistics support.<sup>221</sup> This allows for the maximisation of the speed and efficiency of communications, early warning and alert systems.<sup>222</sup> Technology also needs to be subjected to comprehensive and coordinated testing in order to be

## D1.6 – Communications redundancy

able to quickly determine its benefits, expedite its availability and adoption, and ultimately ensure that it is fit for purpose.<sup>223</sup> The necessary resources for the development of training and exercise programmes should also be allocated to enhance capabilities by increasing responder proficiency, and by simulating an environment that allows for the identification of opportunities for improved stakeholder engagement with private and public sector stakeholders.<sup>224</sup> Exercises are particularly advantageous as tools for learning and gaining experience in contexts where no cyber crisis has occurred.<sup>225</sup> However, it is equally crucial that exercises are conducted at the appropriate level, and although many cyber incidents are handled internally, small-scale exercises may not always adequately prepare nations when highly dynamic crisis situations occur.<sup>226</sup> At the same time, large-scale exercises are resource-intensive and cannot be tailored for different needs.<sup>227</sup> Resources also need to be available for awareness-raising measures and the promotion of joint training among actors at local, federal and national levels through conferences, workshops and other forums.<sup>228</sup> Financial, personnel and knowledge resources on best practices and lessons learned can also be used to improve and share capabilities for emergency communication.<sup>229</sup>



- Distribute communication across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

The allocation of communications responsibilities and planning roles is essential in order to ensure interoperable and regular communications between stakeholders.<sup>230</sup> Continuity of communications is particularly critical due to the time-sensitivity of large-scale disasters. Diffuse communication across emergency response functions at the local, federal, national and potentially international levels allows for: (i) improved responder-to-responder coordination; (ii) easier communication of equipment and personnel needs from responders; and (iii) the expedited delivery of resources.<sup>231</sup> Simultaneously, this allows agencies on multiple levels to promote unified effort.<sup>232</sup> Public-private partnerships between developers, users and service providers can also generate tailored products with unique applications as required to address capability needs.<sup>233</sup> Finally, the US DHS recommends implementing a backup communications solution to ensure redundancy in the system.<sup>234</sup>

### Additional resources



- Cole, Jennifer, & Edward Hawker. 2014. *Emergency Services Communications: Resilience for the Twenty-First Century*. London: Royal United Services Institute.
- Emergency Communications Preparedness Centre. 2016. *Federal Financial Assistance Reference Guide*.
- ENISA. 2014. *Report on Cyber Crisis Cooperation and Management*. 6 November.
- US Department of Homeland Security. 2014. *National Emergency Communications Plan*.

**Dimension 2**  
**Society and culture**



## Dimension 2 – Cyber culture and society

---

Dimension 2 of the GCSCC CMM looks at the wider cultural and societal dimensions of cybersecurity, and the role these play in increasing the security and resilience of cyberspace. The existence of a national cybersecurity culture across stakeholders at the individual, public, private and societal levels is predicated on a common understanding and acceptance of values, attitudes and practices that contribute towards the maturity and resilience of the cyber ecosystem.

This dimension of the GCSCC CMM comprises five factors. The following sections discuss capacity-building steps that national decision makers can implement to build capacity across these issue areas, which are:

### **1. D2.1 – Cybersecurity mindset**

This factor focuses on the values, attitudes and practices of national cybersecurity stakeholders, including government, the private sector, individual users and other actors present in the cyber ecosystem.

### **2. D2.2 – Trust and confidence on the Internet**

This factor focuses on the trust and confidence that the general population has in the use of the Internet in a secure and private manner, including using government e-services and e-commerce platforms.

### **3. D2.3 – User understanding of personal information protection online**

This factor focuses on whether users and stakeholders within the general public, as well as the public and private sectors, recognise and understand the importance and implications of protection of personal information online.

### **4. D2.4 – Reporting mechanisms**

This factor focuses on the presence and use of reporting mechanisms and channels for users to report cyber-enabled crimes, including online frauds, cyber-bullying, child abuse, identity theft, privacy and security breaches, and other incidents.

### **5. D2.5 – Media and social media**

This factor focuses on the role of media and social media, looking at their role in conveying information about cybersecurity and the extent to which cybersecurity is a subject of discussion and debate on these media and platforms.

## D2.1 – Cybersecurity mindset

### Overview

This factor focuses on the values, attitudes and practices of national cybersecurity stakeholders, including government, the private sector, individual users and other actors present in the cyber ecosystem. A mature cybersecurity mindset is signalled by the alignment of values, attitudes and behaviour of actors in the national cyber ecosystem with cybersecurity priorities. This means that there is not only buy-in from various levels of government, but beyond this, there is common recognition of the need for proactive measures to uphold cyber resilience. A cybersecurity mindset means that cybersecurity has been integrated into priority setting, the communication of good practices, strategic planning, and operational procedures and practices across all of society's stakeholders at the individual and organisational levels.

Box 2.1 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 2.1: Steps for improving the cybersecurity mindset (D2.1)

- Nominate a task owner responsible for awareness-raising and information programmes geared towards the development of a cybersecurity mindset.
- Embed cybersecurity considerations into all aspects of public sector decision making and strategic planning.
- Ensure that cybersecurity considerations become ingrained in behavioural practices of public and private sector employees and wider society.
- Periodically assess the degree of correspondence between the cyber conduct of members of the public services and private sector, as well as correspondence with wider society and with good behavioural practices.
- Devise information, training and exercise programmes with clearly defined learning outcomes for different target audiences within the public and private sector and the wider public.
- Evaluate the effectiveness of cybersecurity awareness-raising campaigns and learning interventions. Review learning interventions on the basis of results.

### Capacity-building steps



- Nominate a task owner responsible for awareness-raising and information programmes geared towards the development of a cybersecurity mindset.

A **task owner** with responsibility for coordinating awareness-raising and information programmes should be nominated. As there is no one-size-fits-all method for developing a cybersecurity mindset, this may take the form of a distributed responsibility with a central coordination mechanism, rather than a centralised responsibility. For example, different ministries and governmental bodies and departments may have a leading role in developing a robust cybersecurity mindset within different issue areas and among different target groups. For example, a national CSIRT may be tasked with raising general

cybersecurity awareness, while the Ministry of Education may be tasked with programmes targeting children and students, and the Ministry of Finance may be tasked with programmes concerning online banking and cyber-enabled financial frauds.

Furthermore, since responsibility for ensuring that the Internet is secure is shared among a wide range of stakeholders (governments, businesses, organisations, individuals, etc.), it is important to build **partnerships with all entities with capacity to contribute to different activities**. For example, private sector companies have an interest in developing a robust cybersecurity mindset among their clients and in building consumer confidence in their online services. These companies often have an open channel of direct communication with consumers and may be in a good position to raise awareness and understanding of cybersecurity issues and good cyber hygiene through education and communications campaigns. For example, a campaign seeking to educate people about the safe use of online banking services could involve financial firms providing online services to their clients. While ideally the private sector at large should be involved in such activities, in practice context-specific considerations stemming from national priorities and objectives should inform a prioritisation of which sectors (e.g. technology, financial and telecommunications) should be engaged first.

**Not-for-profit organisations** (e.g. those active in the fields of social entrepreneurship, communications, and skills and resilience development) **and schools** should also be involved in campaigns targeting children, young people and the communities they work with. Not only can they facilitate the delivery of the message among these audiences, but they can also provide insightful input during the planning process. The media (newspapers, radio, television, etc.) and social media companies are also key players in this domain.

Building these partnerships at the **very early stages of the campaign** is critical to fostering discussion about the characteristics and needs of the specific group that the campaign seeks to educate. This will help build a campaign adapted to the target audience.

The task owner will assume the role of campaign leader and **assign tasks among partners**.



It is useful for the lead stakeholder or organisation to develop a **toolkit to be used by all partners** once the campaign is launched. The toolkit should summarise the key messages and include all the necessary material resources, such as logos or even sample communications (press releases, social media posts, etc.). The use of a common toolkit ensures that campaign messaging is uniform, targeted and effective. Common toolkits provide the possibility of creating an engaging campaign identity or branding, and delivering a clear message to the audience.

## D2.1 Cybersecurity mindset

**Global awareness raising campaign: STOP.THINK.CONNECT.**

STOP.THINK.CONNECT. is a global campaign seeking to raise awareness and educate all digital citizens on how to stay safe online. The campaign was launched in October 2010 as part of the US National Cyber Security Awareness Month (NCSAM) and has brought together over 700 organisations inside and outside the US, including governments, international and not-for-profit organisations, and private companies. International partners include organisations and private companies from: Armenia, Australia, Bahrain, Bangladesh, Belgium, Brazil, Bulgaria, Canada, Chile, Denmark, Gambia, Germany, Ghana, Hong Kong, India, Ireland, Israel, Italy, Jamaica, Japan, Latvia, Lithuania, Malaysia, Mexico, New Zealand, Nigeria, Norway, Poland, Portugal, Qatar, Senegal, Serbia, Sierra Leone, Singapore, South Africa, Spain, Sri Lanka, Switzerland, Taiwan, Turkey, UAE, UK, Ukraine, Uruguay and Zimbabwe. The OAS, Panama, Paraguay, Uruguay and Dominica have also signed partnership agreements.

The campaign is led by the US National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). The US Department of Homeland Security coordinates US federal engagement in the campaign.



- Embed cybersecurity considerations in all aspects of public sector decision making and strategic planning.

Cybersecurity considerations should be embedded first of all in strategic policy towards prevention and deterrence. This entails putting controls in place to safeguard systems from human error, and deterrence mechanisms against attacks.<sup>235</sup> There is also a need for clearly formulated policy on detection, utilising effective diagnostic technology to rapidly identify system attacks.<sup>236</sup> Recovery should also be an integral aspect of cybersecurity considerations, with a detailed recovery plan in place aimed at mitigating any damage that has occurred due to an attack, identifying its causes, pinpointing weaknesses in the system and correcting these accordingly.<sup>237</sup> Finally, it is crucial to be able to spread lessons learned and educate stakeholders about security threats, as well as enforcing compliance with rules and regulations.<sup>238</sup>



- Ensure that cybersecurity considerations become ingrained in behavioural practices of public and private sector employees, and those of wider society.

Employees usually constitute the weak link of public and private organisations in relation to cybersecurity.<sup>239</sup> For instance, the Financial Industry Regulatory Authority (FINRA) found that in private sector firms, cybersecurity attacks often gained access due to employee errors such as inadvertently downloading malware or falling victim to a phishing attack.<sup>240</sup> While IT experts and senior management teams tend to show a cybersecurity mindset, this is not necessarily the case among lower levels of management and other employees.<sup>241</sup> In order to create an organisational culture that is conducive to a

cybersecurity mindset, there should be top-down as well as bottom-up buy-in, with leadership visibly engaging with organisations' cybersecurity risk-management policies.<sup>242</sup>

Government should work with private sector actors and stakeholders to facilitate the uptake of good cybersecurity practice by employees. Further information on awareness-raising campaigns, education programmes and professional training is provided in the Dimension 3 chapter of this document.



To ensure that people engage in secure practices, it is advisable to **personalise risks**. Employees in private and public organisations are also consumers and citizens who are concerned about their own privacy. For this reason, explaining to them how non-secure practices could affect them as individuals will make the message more effective. For example, showing an employee in the banking sector that his/her financial information is available online will render an abstract message into a palpable threat for the employee, and may have a greater impact as a result.

There needs to be active engagement with cybersecurity by board members or senior management. Such engagement should be secured by promoting a thorough understanding of cybersecurity issues at the executive level. In particular, cybersecurity should not be seen as challenge only for an organisation's IT team, but rather for the organisation in its entirety,<sup>243</sup> as well as its customers. It is also advisable to define and assign roles and responsibilities to management personnel. This creates explicit authority, responsibility and accountability for key individuals who can act as driving forces behind the establishment and improvement of cybersecurity strategies and operational procedures, as well as the continuation of organisational learning.<sup>244</sup> An individual or individuals in a range of roles should be allocated responsibilities for checking the adequacy of information security measures.<sup>245</sup>



- Periodically assess the level of correspondence between the cyber conduct of members of the public service and private sector, as well as with wider society and good behavioural practices.

A range of codified laws and regulation may already exist, and although these can be useful in improving information security, it is not enough to simply comply with existing laws and regulations. In the context of a quickly evolving cyber threat landscape, there is a need to guard against complacency.<sup>246</sup> One method of proactively seeking improved resilience is to make cyber risk assessments routine practice within public and private sector organisations.<sup>247</sup> Key personnel, meaning those with the strategic oversight and authority to review and validate information security, should play a primary role in periodic assessments.



- Devise information, training and exercise programmes with clearly defined learning outcomes for different target audiences within the public and private sector and the wider public.

A core priority of public and private sector personnel training is to put in place provisions that give leadership, employees and users the foundations for baseline cybersecurity awareness. It should also be

## D2.1 Cybersecurity mindset

ensured that education on cybersecurity is provided on a recurring, if not continuous basis.<sup>248</sup> Cybersecurity awareness-raising campaigns and training programmes should be continuously available within organisations.<sup>249</sup> Training content might include components such as how to recognise risks, phishing, how to handle sensitive and confidential information, password protection, escalation policies and more.<sup>250</sup> In this way, users become enablers of the reinforcement of information security, rather than a potential source of risk.<sup>251</sup>



- Evaluate the effectiveness of cybersecurity awareness-raising campaigns and learning interventions. Review learning interventions on the basis of results.

It is important to measure the success of awareness-raising campaigns and learning interventions, as this will allow the intervention team to **monitor progress towards the established objectives** and, in case of deviations, to implement the necessary changes. Lessons learned can also be taken into account in the design of future interventions.

Measuring behavioural changes is a complex but achievable process, provided that the right evaluation framework is in place. An adequate evaluation framework should do the following:

- Set **intermediate objectives** based on the final goal of the campaign. If the causal link between them is well-evidenced, the intermediate goals should allow the progress of the intervention to be monitored in order to assess whether or not it is on track to achieve the ultimate goal.
- Establish which **outputs, outcomes and impacts** will be measured. Outputs are tangible products of activities (e.g. the launch of an event or a website, the organisation of workshops, courses, contests, etc.) and outcomes are the results of those activities (e.g. participation in the events held, increased awareness in relation to the topic, etc.). The impact of a campaign concerns the causal link between the intervention and the observed result (i.e. the extent to which the creation of a cybersecurity mindset can be attributed to a specific campaign).
- Prioritise which outputs and outcomes will serve as **indicators**.
- Select the **evidence** that will be collected. This should be done according to the size of the campaign as well as the appropriateness and availability of data. Evidence can be qualitative or quantitative. Quantitative data shows the extent to which a change has happened and can be measured with a number (e.g. number of articles written, number of visits to a website, number of attendees at an event, etc.). Qualitative data looks at the change in attitude, opinions or feelings which can be collected through, for example, interviews, focus groups and social network analysis.
- Determine the **sources** from which data will be collected, such as social media, other websites, interviews, media coverage, participation in events, etc.



When measuring visits to a website, it is important to pay attention not only to the number of visits, but also to the number of **unique visitors**. Likewise, the number of **new visitors** will provide useful information to discern whether or not the campaign is reaching the intended target audience. It should be noted that the number of visits does not necessarily indicate whether the campaign has an impact at the behavioural level.

### Additional resources



Dutton, W. 2017. Fostering a cyber security mindset. *Internet Policy Review*. Vol 6(1) pp. 1-14.

Financial Industry Regulatory Authority. 2015. Report on Cybersecurity Practices. As of 17 July: <https://www.finra.org/file/report-cybersecurity-practices>

International Chamber of Commerce (ICC). 2015. ICC Cyber Security Guide for Business. As of 17 July 2017: <https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/>

## D2.2 – Trust and confidence on the Internet

### Overview

This factor considers the trust and confidence of the general population in their ability to use the Internet in a secure and private manner. It focuses on trust and confidence in government e-services and private and public sector e-commerce, but it also includes broader use of the Internet outside of these two categories.

E-commerce refers to the use of computer networks, principally the Internet, for the sale or purchase of goods and services. The transactions can be between governments, companies, households, individuals, or any other public or private organisation.<sup>252</sup> Government e-services refers to the online provision of government information, such as national-level strategies and policy documents, as well as the provision of online government services, such as online tax services and electronic communication methods.<sup>253</sup> It is a subset of e-government, which is the broader implementation of ICT systems that aims to improve not only the provision of public services, but also the administration and management of government departments, as well as the ability to carry out information-intensive research and initiatives.<sup>254</sup> E-government can be divided into three sub-categories of engagement: government-to-citizen (G2C), government-to-business (G2B) and government-to-government (G2G).<sup>255</sup> Government e-services typically refer to the first two areas.<sup>256</sup>

Effective e-commerce and government e-services platforms are both desirable in an effective economy. The provision of government services is more effective when using ICT systems, since information systems are more efficient than traditional methods for disseminating, collating and analysing large volumes of information. This can reduce government costs while offering a higher standard of service and greater transparency, accountability and openness.<sup>257</sup> E-commerce also has a number of advantages over more traditional forms of transactions. For example, it can facilitate greater market access and market reach, it can lower operational and transactional costs, and it can improve market efficiency and create new opportunities that previously did not exist.<sup>258</sup>

Trust is essential for the effective functioning of these online services.<sup>259</sup> Both government e-services and private e-commerce rely on consumers and businesses to entrust them with sensitive information, and in return consumers and businesses trust that this information will be used and stored in a secure manner that respects their privacy.<sup>260</sup> In practical terms, trust and confidence translates to an ability to identify authentic<sup>261</sup> e-commerce and government e-services, and use these services without personal or sensitive information being lost or unfairly exploited.<sup>262</sup> The misuse or loss of personal or sensitive information can be damaging for individuals, organisations and governments, both financially and in terms of operational effectiveness, as people and businesses may be less willing to use online services if they do not believe that their information and activity is private and secure. Trust is a prerequisite for the functioning of these services,<sup>263</sup> and building trust and confidence in the use of the Internet is therefore essential for the full benefits of ICT to be realised. Box 2.2 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 2.2: Steps for increasing trust and confidence on the Internet (D2.2)

- Nominate a task owner and governance structure responsible for overseeing the implementation of government e-services.
- Develop a strategic plan for e-government that includes government e-services.
- Launch and continuously develop government e-services; embed the application of security measures in their design and running to increase public trust in these services.
- Publish periodic reports on government e-service activities, including *ad hoc* disclosure of potential breaches, to increase public trust.
- Gather employee and user feedback on e-services and review management of online content accordingly.
- Stimulate growth of e-commerce through development of infrastructure.
- Regulate the provision of e-commerce services and encourage private sector actors to embed security considerations in the design and running of these services.
- Periodically assess the level of trust and understanding that members of the general public have of online services, including e-government and e-commerce services.
- Devise information programmes and confidence-assurance programmes to promote trust in the use of online service; evaluate the effectiveness of these programmes and review their design and resource allocation accordingly.
- Promote safe Internet use, such as privacy-by-default settings.

#### Capacity-building steps



- Nominate a task owner and governance structure responsible for overseeing the implementation of government e-services.

An obvious prerequisite for trust and confidence in government e-services is the existence of those services. An e-government strategy document should provide the overall direction for the development of e-government in a country, but first a **task owner** is required to (i) work out how this strategy can be designed and implemented; and (ii) manage the implementation process. This **task owner** should be an organisation or body that is responsible for the planning, implementation, operation and evaluation of government ICT services, including e-services, in accordance with the overarching e-government strategy.<sup>264</sup> This includes resource allocation, systems development, training, service provision, and the development of rules, policies and regulations that govern the implementation and operation of the e-government systems.<sup>265</sup>



The designation of a suitable task owner is one way to help ensure that a strategic plan is produced. The task owner is an individual or group that is both responsible and accountable for the development of the strategic plan.

## D2.2 - Trust and confidence on the internet



There is no one-size-fits-all approach to **who** this task owner should be. It may be led by a centralised ICT department, or decentralised across government departments with central oversight provided by a smaller cross-departmental body. Regardless of the implementation model, an element of central planning should be maintained to ensure that resources are used efficiently and that ICT development in each department is supported and integrated.<sup>266</sup>



ICT department leaders are often excluded from high-level discussions and decision-making processes. This results in failure to utilise their understanding and experience. Governments in developed countries are increasingly including ICT managers in executive-level decision making as ICT changes from a support service to the core of government operations and services.<sup>267</sup>



- Develop a strategic plan for e-government that includes government e-services.

However, government e-services cannot be provided without the broader implementation and integration of ICT within government administration, management and operations. The provision of government e-services is typically one element of a broader e-government strategy which also includes the development of ICT infrastructure, expertise, internal information governance, policy compliance and security, among other areas.<sup>268</sup> The development of an e-government strategy that includes government e-services is the first step towards developing those e-services.<sup>269</sup>

The strategy should outline the future vision for e-government across the whole of government and set out a roadmap for achieving this vision.<sup>270</sup> It should define the overall direction of e-government, the overall computing needs of each department, and a timeline for the development and integration of potentially fragmented departmental ICT systems into a coherent, secure system.<sup>271</sup> This vision and roadmap should be sufficiently non-technical to allow managers in each government department to develop a clear, integrated approach to ICT without requiring specialist ICT knowledge.<sup>272</sup>



- Launch and continuously develop government e-services; embed the application of security measures in their design and running to increase public trust in these services.

The implementation of government e-services can be categorised into four dimensions: governance, infrastructure, policy and outreach. The first of these, governance, aims to ensure sufficient oversight of the implementation and management of government ICT systems. This implementation should include ICT infrastructure, policy and outreach. In order to provide government e-services, there should be ICT systems to support electronic platforms, legal frameworks and regulations that govern the secure use of electronic government, and interaction with end-users to encourage and enable them to use the platforms

and provide feedback for further improvements to the system. The extent of these capabilities, frameworks and interactions will depend on context-specific resources and levels of ambition.<sup>273</sup>

There are a number of activities that are typically important for the implementation of e-government strategies. A comprehensive list is not provided here, although additional resources providing a more in-depth discussion of these issues are listed at the end of this section. A number of important elements and recommendations are highlighted below:

- Conduct an assessment of the readiness of government for e-government systems.<sup>274</sup>
- Conduct an assessment of the readiness of the population for e-government systems.<sup>275</sup>
- Use indicators and indices to help review readiness, set goals and track progress.<sup>276</sup>
- Use well-established ICT system development practices.<sup>277</sup>
- Involve and develop technical and managerial ICT expertise to ensure reliable implementation of ICT systems.<sup>278</sup>
- Develop the technical skills and understanding of managers and employees who are not directly involved in ICT.<sup>279</sup>
- Engage and coordinate with all stakeholders throughout the process, including end-users and employees.<sup>280</sup>
- Aim to create a *learning organisation* where employees are able to share and build on knowledge gained from experience.<sup>281</sup>
- Include a focus on security throughout the implementation of an e-government strategy.<sup>282</sup>

Focusing on this last point, the level of security of e-government is an important factor that influences the level of confidence in and uptake of government e-services. As mentioned earlier, there are a number of benefits of using ICT for the provision of government services, but it also introduces additional risks such as increased vulnerability to cyber-attacks, fraud and data leakages.<sup>283</sup> Cybersecurity policies should be implemented to ensure the security and privacy of personal and sensitive information, including digital identification, digital signatures, e-payment methods and data protection laws.<sup>284</sup> Mitigation measures should also be put in place to prevent, detect and deter unwanted cyber activity; limit the damage from cyber-attacks; enable recovery from cyber-attacks; and improve the awareness and compliance of all staff vis-à-vis the risk of cyber-attacks and their importance to cybersecurity.<sup>285</sup> A consideration of cybersecurity measures should be included in all strategic planning documents and implementation of e-government systems.

## D2.2 - Trust and confidence on the internet



Digital identification is one of the key enabling technologies for effective and secure public and private sector e-services.<sup>286</sup> Digital identification is the ability to authenticate individuals when using digital services. It is an essential feature for secure online platforms for bank transactions, public voting, accessing social services, paying utility bills and more. Digital identification systems have been implemented worldwide using a number of different systems, often combining biometric and biographical information stored on a central database. There are, however, a number of legal, institutional, technological and ethical concerns that should be addressed before a comprehensive digital identification system is implemented.<sup>287</sup>



- Publish periodic reports on government e-service activities, including *ad hoc* disclosure of potential breaches, to increase public trust.

The uptake of government e-services may vary across different demographic groups according to factors including education, ICT literacy, provision of ICT infrastructure and cultural preferences.<sup>288</sup> Providing periodic reports on government e-services may increase awareness of the types of services available and the ways in which they can be accessed. These publications may also be used to provide assurances on data protection and security against cybersecurity threats, and may be published in both electronic and paper format.

This may be supplemented by information on security breaches, posted on an *ad hoc* basis in response to cyber incidents. Openly publishing information on cybersecurity incidents serves several purposes: it allows individuals who may be affected to take sufficient precautionary action, it assists other organisations who may be exposed to a similar attack to improve their defences, it encourages international cooperation and interoperability on data protection, and it encourages a culture of transparency which, in turn, can engender greater levels of trust.<sup>289</sup> However, there are important disincentives for both public and private organisations that discourage the open publication of cybersecurity breaches. In particular, organisations can face direct financial loss, reputational damage and loss of trust.<sup>290</sup> A broader discussion of good practices and building capacity in disclosure of vulnerabilities and security breaches is presented in the sections on Dimension 4 and Factor 5.7 of this document.



A comprehensive legal framework can facilitate the disclosure of data security breaches and help promote good practices for effective data protection.<sup>291</sup> In particular, introducing a legal requirement for both governments and organisations to publish information on data breaches can act as a strong incentive, particularly if penalties are assigned for non-disclosure.<sup>292</sup> Further information on these issues is presented in the sections on Dimension 4 and Factor 5.7 of this document.



- Gather employee and user feedback on e-services and review management of online content accordingly.

It is important to involve employees from all levels of government in the development and implementation of e-government strategy, as an *involvement-orientated approach* encourages knowledge sharing and continued cross-government engagement. For example, frontline workers often have close engagement with the ‘customer’, and hence have valuable insight into the customer’s requirements and preferences for their own user interface.<sup>293</sup> Employees should be engaged on a regular basis in both evaluating and suggesting improvements to the existing e-service platform and management. This should be part of an iterative process whereby they are regularly consulted within a broader evaluation and improvement process.

Similarly, it is important to regularly engage end-users, namely citizens and businesses, in order to better understand and address their needs and preferences with regard to areas such as functionality, accessibility, security and transparency.<sup>294</sup> The provision of e-services ultimately aims to improve the experience for end-users when interacting with the government. Engaging with the end-user can help identify problems and means of improving this experience, including: (i) the type of information provided; (ii) the quantity of information provided; (iii) the format in which information is provided (e.g. text, images, video, app, website, etc.); (iv) the platforms used to communicate with the government; and (v) the level of integration and consistency across different e-services. Of course, some of this information will already be obvious to the government, but communication with the end-user enables a more informed prioritisation and distribution of resources to areas of high concern for the end-user.



- Stimulate growth of e-commerce through development of infrastructure.

There are three pre-requisites for e-commerce: Internet access, electronic payment systems, and delivery systems (both physical and virtual).<sup>295</sup> There are a range of options in each of these areas which, in turn, influence the scope for e-commerce. Internet access, for example, is typically provided by broadband and mobile 3G or 4G technology. Some forms of e-commerce can operate effectively using mobile technology. A number of different payment systems also exist, including account-based payment systems (credit cards, debit cards, ‘e-wallets’ such as PayPal, etc.), electronic currency systems (e.g. digital crypto currencies), or systems that rely on additional offline methods (credit purchase systems, bank payment slips, cash on delivery, etc.).<sup>296</sup> In particular, a reliance on offline payment methods limits the potential growth of e-commerce. Finally, goods and services can be delivered in a number of different ways, including digital delivery (e-books, music, computer software, etc.), physical delivery (postage or courier network), buyer pick-up (typically at a local store) and buyer service use (e.g. airport flights, car rental services, etc.). Slow Internet speeds can restrict the possibility of digital delivery (such as data-intensive TV or film streaming), and poor logistical infrastructure remains a critical problem for e-commerce in many economies worldwide.

## D2.2 - Trust and confidence on the internet

A number of different initiatives can be implemented in each of these areas to stimulate the growth of e-commerce. Examples include improving the speed, distribution and access to the Internet through infrastructure investment; and improving delivery networks through the development of nationalised infrastructure. This can be supplemented by private sector development such as private courier services and close-delivery networks, and the provision of accessible e-payment platforms.



- Regulate the provision of e-commerce services and encourage private sector actors to embed security considerations in the design and operation of these services.

The provision of a legal framework is not considered a pre-requisite for e-commerce, but it is considered essential for its sustainable growth. A sufficient legal framework is required to ensure trust and confidence in secure e-commerce transactions, which in turn encourages commercial and consumer uptake.<sup>297</sup> The literature on ICTs shows that it has a demonstrably positive impact on productivity, as well as being a driving force behind increased international trade. However, growth is conditioned upon, for instance, complementary investment in skills and organisational adjustment.<sup>298</sup> As a result of digital technology, e-commerce services are able to bypass barriers such as geographic distance or political systems.<sup>299</sup> A survey of web-based firms bartering goods and services in the Republic of Korea found that e-commerce cut down transaction costs and expanded markets for online establishments.<sup>300</sup>

The term *legal framework* is used in a broad sense here to include a range of measures for regulating behaviour, including public law measures, private law agreements, standards, codes of practice and non-binding, self-regulatory measures. In e-commerce, these are typically applied to four main areas: e-transactions, consumer protection, privacy and data protection, and cybercrime.<sup>301</sup>



There is no one-size-fits-all legal framework, and a number of countries have implemented different legal structures. Some countries enact specific e-commerce regulations, whereas others build on and adapt existing commercial regulations so that they are applicable to online transactions. In establishing a legal framework, consideration should be given to existing laws, idiosyncrasies of existing legal structures, existing and applicable international legal frameworks, and cross-border harmonisation with neighbouring countries with existing e-commerce legislation.<sup>302</sup>

E-transaction laws are primarily concerned with equating electronic and paper-based payment methods (functional equivalence), ensuring transactions are not restricted to specific technologies (technology neutrality), and ensuring compatibility across borders. The enforcement of e-transaction laws is often lacking in developing countries due to a lack of experience and understanding of e-transactions among judges and law enforcement practitioners. This can create uncertainty and insecurity that discourages uptake of e-commerce platforms due to a lack of trust in the system.<sup>303</sup> Further information on methods

and approaches for developing the cybersecurity capacity and understanding of law enforcement agencies and prosecution services of a country is presented in the Dimension 4 section of this document.

Consumer protection laws are intended to protect the consumer against fraudulent, misleading and unfair online commercial practices, and enable the consumer to take action if they are a victim of this type of activity. Consumer protection laws not only encourage the consumer to use e-commerce services, but also provide clarity to businesses regarding their legal duties and help them build self-regulating regimes.<sup>304</sup> Data protection laws similarly provide assurance to the consumer and clarity to business, and also encourage and require businesses to adopt international best practices and security measures to mitigate against cybersecurity risks.<sup>305</sup> Finally, cybercrime is a broad area that includes online fraud; the sale of counterfeit products including used cars, free trials and tickets; and the hacking of bank accounts. Some of this is covered by consumer protection law, but additional criminal law is required to enable law enforcement agencies and judges to effectively pursue and prosecute perpetrators of online criminal activity.<sup>306</sup> A broader discussion of cybercrime and of instruments and approaches for tackling it can be found in the Dimension 4 section of this document.



Governments often adopt e-commerce legal frameworks too slowly and too late, meaning laws are often obsolete by the time they are introduced. A number of factors can contribute to this, such as insufficient awareness and knowledge among lawmakers and the judiciary, and a lack of capacity of existing institutions to increase their mandate to cover e-commerce activity. Building awareness, knowledge and capacity in relevant government institutions is necessary to ensure timely development and updating of legal frameworks.<sup>307</sup>



- Periodically assess the level of trust and understanding that members of the general public have of online services, including e-government and e-commerce services.

Trust is a guiding principle for enterprises and consumers in terms of overcoming barriers and successfully harnessing the growth potential of e-government and e-commerce. It is paramount that a foundation of trust is built among business, academia, civil society and government stakeholders, which helps to mitigate a range of key privacy and security risks.<sup>308</sup>

A periodic evaluation of the general public's trust in online services and the Internet more broadly can be used to understand trends at a societal level as regards the use of government e-services. Governmental research departments, as well as academic and research institutions, would be well placed to undertake such investigations through surveys or other forms of stakeholder engagement and consultation.<sup>309</sup>

## D2.2 - Trust and confidence on the internet



- Devise information programmes and confidence-assurance programmes to promote trust in the use of online services. Evaluate the effectiveness of these programmes and review their design and resource allocation accordingly.

Information and confidence-assurance programmes can be geared towards creating a culture of security-consciousness, with a particular focus on raising awareness among casual users.<sup>310</sup> Similarly, training programmes could also potentially be sponsored by industry actors through public-private partnerships to raise the general public's trust and confidence in online products and services.<sup>311</sup> Further information on how these programmes and initiatives can be designed and employed is provided in the Dimension 3 section of this document.

Confidence-assurance initiatives might also be employed to assure consumers that standardised protocols are applied to online products.<sup>312</sup> These may take the form of initiatives such as the Cyber Essentials programme discussed below.

**UK Cyber Essentials<sup>313</sup>**

Cyber Essentials is a UK government-backed and industry-supported certification scheme to help private sector and civil society organisations develop adequate protection against the most common cybersecurity threats. Companies and organisations that are successfully certified may advertise this through badges and certificates, which may positively affect users' trust and confidence in online services provided.<sup>314</sup>



- Promote safe Internet use, such as privacy-by-default settings.

Government stakeholders should aim to enable the general population to better control the online use of their personal information and better identify cyber risks such as insecure or fake e-commerce platforms. This could be done through a combination of education and awareness-raising initiatives on the one hand, and legislative and regulatory efforts on the other. Further details on these two types of initiatives are presented in the Dimension 3 and Dimension 4 sections of this document, respectively.

Furthermore, legislative and regulatory efforts could be made to encourage the development privacy-enhancing methods of accessing online services, such as ways of validating identities in a secure manner, digital credential systems and privacy-by-default settings.<sup>315</sup> Further details on these are provided in section D2.3 on user understanding of personal information protection online.

## Additional resources



- Gant, Jon P., ed. 2008. Electronic government for developing countries. Geneva: ITU.
- OECD. 2013. The OECD Privacy Framework. Paris: OECD
- UNCTAD. 2015. Information Economy Report. New York: United Nations
- UNCTAD. 2016. Data protection regulations and international data flows: Implications for trade and development. As of 17 July 2018: [http://unctad.org/en/PublicationsLibrary/dtistict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtistict2016d1_en.pdf)

## D2.3 – User understanding of personal information protection online

### Overview

This factor focuses on whether users and stakeholders within the general public, as well as public and private sectors, recognise and understand the importance and implications of protection of personal information online. The digitisation of the public and private sectors, through developments such as *e-government* and *e-commerce*, means that an increasing volume of personal data is collected, used, stored and transferred in electronic form for administrative, operational and analytical purposes. There have been significant increases in the number and variety of actors that use personal data; the ways in which data is collected and volume of personal data stored; the power of processing and analysis techniques; and the frequency and complexity of interactions between citizens, businesses and government that require personal data.<sup>316</sup>

Significant economic and social benefits can be derived from more extensive, innovative and complex uses of digital personal data.<sup>317</sup> However, the transition to and expansion of online personal data systems elevates the risks posed to privacy. There are a number of ways in which the privacy of personal information can be violated, including data being obtained without consent; data being used in ways not anticipated or authorised at time of collection, including the use of data analysis techniques and distribution of personal data; and data being accidentally or unlawfully lost, damaged, destroyed, altered, accessed, copied or distributed, either by the original authorised owner or by unauthorised third-party actors.<sup>318</sup>

There are a number of basic principles that underpin any national-level approach to online personal information protection, namely:<sup>319</sup>

- **Limitation of collection:** Personal data should be collected using lawful and fair means, ideally with the knowledge and consent of the individual.
- **Data quality:** Personal data should be accurate, up-to-date and complete, with the constraint that it is relevant to the specified purpose.
- **Specification of purpose:** Data should be collected according to a specified purpose which is communicated no later than the time of collection.
- **Limitation of use:** Personal data should not be used, disclosed or distributed beyond the initial specified purpose, except with the consent of the individual and within legal constraints.
- **Security safeguards:** Personal data should be protected using reasonable security measures that reduce the risk of data privacy violations such as unauthorised access, modification, destruction or dissemination.
- **Openness:** It should be possible to establish the existence, type, purpose and owner of any personal data stored.
- **Accountability:** The data controller should be accountable for complying with these principles as well as with local and international regulations and standards.

## D2.3 - User understanding of personal information protection online

- **Individual participation:** Individuals should be able to obtain, rectify, complete, amend or remove any personal data relating to them, and should be able to challenge the denial of this principle.

In addition, online data privacy is inherently international in nature, as personal data is collected, used, stored and transferred around the world through global networks. There is a continued need to improve cooperation and interoperability between governments on data privacy strategy and policy, legal frameworks, law enforcement and other areas.<sup>320</sup> This international aspect has been recognised since at least the publication of the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.<sup>321</sup> A number of initiatives have been set up in recent years to address this aspect, including the European Union's Binding Corporate Rules,<sup>322</sup> the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System,<sup>323</sup> and the OECD's 2007 Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy.<sup>324</sup>

It is important that individual users are able to accurately assess risk to personal privacy and make informed decisions when providing personal information to the public or private sectors. However, it is becoming increasingly difficult for individual users to understand and make decisions regarding the privacy of their personal data.<sup>325</sup> The collection, storage, communication and analysis of personal data is increasingly complex, and individuals are often presented with too little or too much information, both of which make it difficult to assess risk and provide informed consent. The growing level of interaction and transfer of personal information means that it is increasingly hard to allocate responsibility and attribute blame for privacy breaches, and it is also increasingly difficult for organisations to keep track of personal data, given the volume and extent of dissemination across the Internet.<sup>326</sup> Box 2.3 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 2.3: Steps for improving user understanding of personal information protection online (D2.3)

- Periodically assess the level of understanding that users in the public and private sectors, and in society at large, have of the mechanisms for and implications of online handling of personal information.
- Devise information, training and exercise programmes with clearly defined learning outcomes for different target audiences within the public and private sectors and the wider public.
- Stimulate public debate on the issues of personal information protection and the balance between privacy and security.
- Promote the use of privacy-by-default settings and establish mechanisms to ensure that privacy and security are not competing.
- Periodically review protection of personal information in e-services and feed results of reviews into policy revision work.

## D2.3 - User understanding of personal information protection online

*Capacity-building steps*

- Periodically assess the level of understanding that users in the public and private sectors, and in society at large, have of the mechanisms for and implications of online handling of personal information.

It is important to assess and regularly reassess Internet users' baseline understanding of personal information privacy. This allows a government to assess the required scale of awareness-raising and educational initiatives, identify important target groups, and track the effectiveness and impact of any initiatives implemented.

To help organise and structure this assessment, information privacy awareness can be broken down into a number of subcategories. For example, distinctions can be drawn between technology information privacy awareness, regulatory information privacy awareness, and common practices in information privacy awareness.<sup>327</sup>



- Devise information, training and exercise programmes with clearly defined learning outcomes for different target audiences within the public and private sector and the wider public.

A wide range of stakeholders should be involved in the development of information, training and exercise programmes, including educators, government officials, representatives from privacy enforcement authorities, members of self-regulatory bodies and representatives from civil society organisations. Programmes should particularly target vulnerable categories of Internet user, such as children and young people. Programmes should aim to build both awareness and technical skills required to protect the privacy of personal information online. This should include an awareness of risks associated with online personal information, and the potential means by which individuals can make informed decisions.<sup>328</sup> There is no single format for the presentation of these programmes, but both privacy professionals and professional educators should be involved in their development in order to achieve a balance between accessibility and complexity of information.<sup>329</sup> Further information on awareness-raising initiatives and on education and training programmes for cybersecurity is presented under Dimension 3 of this document.



### National Cyber Security Alliance

The National Cyber Security Alliance is a public-private partnership that brings together stakeholders from across the public and private sectors, including representatives from the US DHS and private sector software, hardware, social media and cybersecurity companies. The aim of the Alliance is to provide information and education to the wider public on the safe use of the Internet, including personal information privacy.

The Alliance has developed a number of information and education initiatives to improve awareness and understanding of personal information protection online. In particular, it developed StaySafeOnline.org, an online portal that provides information to Internet users and that includes material for teachers and businesses. The Alliance also led and contributed to a number of awareness-raising campaigns, including *Data Privacy Day*, *National Cyber Security Awareness Month*, and *STOP. THINK. CONNECT.*<sup>330</sup>



- Stimulate public debate on the issues of personal information protection and the balance between privacy and security.

Information, training and exercise programmes such as those discussed in the previous section may help stimulate public debate on personal information protection. Regularly updating and renewing these initiatives can help keep their content relevant, and keep data privacy issues at the forefront of public discourse.



### International Data Privacy Days

Data Privacy Day/Data Protection Day is celebrated in North America and a number of European countries to increase awareness and generate discussion of the privacy of private information. A similar Privacy Awareness Week has been celebrated in the Asia-Pacific Region since 2006. There is interest in establishing a single date for a worldwide awareness day for privacy protection.<sup>331</sup>

### US National Cyber Security Awareness Month (NCSAM)

Every October the US DHS runs an awareness-raising campaign on the importance of cybersecurity. NCSAM is designed to engage and educate public and private sector partners of the DHS through events and initiatives on the importance of cybersecurity, provide them with tools and resources needed to stay safe online, and increase the resilience of the US in the event of a cyber incident.<sup>332</sup>

### European Cyber Security Month (ECSM)

ECSM is the EU's annual awareness campaign that takes place during the month of October across EU Member States. The aim of the ECSM is to raise awareness of cybersecurity threats, promote cybersecurity among citizens and organisations, and provide them with resources to protect themselves online, through education and sharing of good practices.<sup>333</sup>

### D2.3 - User understanding of personal information protection online

One area that is particularly relevant to public debate is the balance between privacy and security. Privacy protection, as described throughout this chapter, is an important consideration for all public and private sector actors who use personal information in electronic formats. However, privacy is not the only important consideration. Security, and more specifically national-level security provided by intelligence agencies and law enforcement organisations, often relies on surveillance, intelligence gathering, information sharing and analysis of personal information in order to effectively identify, prevent and respond to threats to national security. This information is often gathered and used without the knowledge or consent of the individual, and consequently conflicts with many of the personal information privacy principles outlined earlier in this chapter. This information is increasingly available in digital form due to the digitisation of the public and private sectors, the transition into cloud computing systems and the development of advanced data-analysis techniques, particularly those associated with big data.<sup>334</sup>

However, the relationship between privacy and security is more complex than a simple trade-off. Law enforcement and intelligence agencies aim to reduce the threat to society, which includes threats to cybersecurity and online privacy through personal information being illegally accessed, edited, damaged, destroyed, obtained or used by malicious actors. Effective security can increase the protection and privacy of personal information, which in turn can enhance trust and confidence in online systems.<sup>335</sup>

The debate on security and privacy can be difficult because important information is often unavailable or unclear. Intelligence agencies are often reluctant to disclose the type and extent of digital surveillance activities, and it is difficult to link this activity directly to a reduction in threat and increase in security. Nonetheless, continued debate in this area is important to try and establish the scope and boundaries of surveillance and the right to personal data protection and privacy.<sup>336</sup> This debate should be allowed to occur freely across different platforms, and can be facilitated and stimulated by governmental transparency and government-led research initiatives.



- Promote the use of privacy-by-default settings and establish mechanisms to ensure that privacy and security are not competing.

Privacy-by-default refers to the initial privacy settings on newly acquired software or hardware being set by default to their strictest level. For privacy settings below this level of strictness to be in operation, settings would need to be changed by hand.<sup>337</sup> Privacy-by-default settings are important because they ensure that the principles of data protection highlighted earlier in this chapter are observed by manufacturers and providers of goods and services. They prevent the collection, use or sharing of personal information without explicit consent from the customer, which provides protection in particular to individuals who are less aware of data protection and less likely to consciously configure privacy settings.<sup>338</sup>

Governments can encourage privacy-by-default settings in goods and services provided by private sector firms. They can choose to impose privacy regulations that require private firms to supply goods and services with privacy-by-default settings. A financial cost for non-compliance can be introduced to further incentivise compliance.



### EU General Data Protection Regulation

In line with trends observed in previous years, May 2018 will see EU regulations on data privacy protection become increasingly strict as the General Data Protection Regulation (GDPR) 2016/679 will enter its implementation phase.<sup>339</sup> Paragraph 79 of the GDPR states that organisations 'should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default', and that these areas 'should also be taken into consideration in the context of public tenders'. This is then substantiated further in Article 25, which focuses exclusively on protection by design and protection by default.<sup>340</sup>



Private sector companies may object to additional regulation, particularly if the regulations themselves are overly complicated and place an additional burden on businesses. To reduce any impact, government regulation on data protection should be technologically neutral, flexible enough to allow business innovation, clear and unambiguous regarding the minimum acceptable requirements, and ideally harmonised with other regulations on an international level.<sup>341</sup>

Some of the most innovative information-management mechanisms that have evolved in recent years stem from more practical concerns regarding the implementation of data privacy protections.<sup>342</sup> Privacy-by-design can be understood as a concept under which, from the onset, the primary design objective of the product, IT system or business practice rests on the assumption of privacy as a default setting.<sup>343</sup> Manufacturers, operators and users stand to benefit from making use of privacy-friendly design choices as part of a privacy-by-design approach. This encourages confidence building and protects users' interests and control over personal data. For companies and organisations involved, however, this approach requires the involvement of so-called Data Protection Officers across the design, implementation, promotion and adoption of regulatory tools such as codes of conduct. Data Protection Officers' roles and responsibilities may vary according to the regulatory context. For example, in the context of the EU GDPR, Data Protection Officers' responsibilities will include:<sup>344</sup>

- Educating the company and employees on data-processing compliance requirements;
- Training staff involved in data processing;
- Conducting internal audits to ensure compliance and address any issues proactively;
- Serving as the point of contact between the organisation and GDPR Supervisory Authorities;
- Maintaining comprehensive records of all data-processing activities conducted by the organisation;

## D2.3 - User understanding of personal information protection online

- Interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information.



- Periodically review protection of personal information in e-services and feed results of reviews into policy revision work.

It is not just the private sector which should respect personal online privacy. It is important that the government provides sufficient protection for individual personal information that it collects, stores and uses as part of e-government and the provision of government e-services. As stated earlier, the assurance of privacy and security of personal information is essential in ensuring citizen trust and confidence in ICT-based government systems. A regular review of the use and vulnerability of personal information can be used to update government policy, and consequently target resources to where they are needed most. Responsibility for this task could fall within the remit of the task owner for e-government activities. If the results of these reviews are communicated clearly to the public, this can also foster a culture of transparency. The review should aim to cover all areas of personal privacy protection, including legal, technical, operational, organisational and strategic. As always, it should include contributions from all relevant stakeholders. The review process may be part of a larger e-government strategy that includes periodic evaluation and revision, but it may also be completed as a standalone (but regular) task if regular reviews of e-government strategy do not exist.

### Additional resources



Correia, John, & Deborah Compeau. 2017. Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. Proceedings of the 50th Hawaii International Conference on System Sciences.

ITU. 2014. The quest for cyber confidence. Geneva: ITU

OECD. 2007. OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. Paris: OECD

OECD. 2013. The OECD Privacy Framework. Paris: OECD

OECD. 2014. OECD Recommendation on Digital Government Strategies. As of 1 November 2017:

<http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm>

## D2.4 – Reporting mechanisms

### Overview

This factor focuses on the presence and use of reporting mechanisms and channels for users to report cyber-enabled crimes, including online fraud, cyber-bullying, child abuse, identity theft, privacy and security breaches, and other incidents. Reporting mechanisms allow individual citizens and businesses to report cybercrime and cyber-attacks directly to relevant public authorities. They exist in a number of formats, including online web forms, dedicated email addresses, telephone hotlines, post, email client plugins, browser plugins, and direct upload to databases (typically businesses only).<sup>345</sup> These reports are typically centralised and processed before being communicated to the relevant authorities (e.g. national CSIRT, law enforcement).<sup>346</sup>

There are a number of operational and strategic benefits stemming from implementing effective cybersecurity reporting mechanisms. First and foremost, on an operational level, reporting mechanisms provide a centralised tool that facilitates the communication of illicit cyber activity to appropriate public authorities on a national level. This communication may not occur or may occur less frequently if an appropriate reporting mechanism is absent. In the short term, this communication helps public authorities to respond to incidents as required. In the long term, the information gathered allows government to analyse any trends in cyber incidents, and develop future capacity in order to better prevent and respond to these in the future. On a strategic level, a centralised reporting tool can help public authorities, including law enforcement and the judiciary system, to coordinate cybersecurity activity across government. For example, a centralised reporting mechanism can be used to distribute and collate information and analysis across government to avoid multiple agencies conducting the same analysis for the same report or dataset.<sup>347</sup>

A reporting mechanism can also help facilitate closer collaboration between the public and private sectors, and help influence business practices so that employees and managers are more aware of cybersecurity issues.<sup>348</sup> They can also help raise awareness of online laws and regulations, and provide a basis for educational tools in industry and the wider public.<sup>349</sup>

Box 2.4 provides an overview of capacity-building steps for increasing national capacity in the area of reporting mechanisms.

### Box 2.4: Steps for improving reporting mechanisms (D2.4)

- Review national legislation to ensure that emerging illicit online activities are covered by existing criminal legislation.
- Establish reporting channels for illicit online activities and launch coordinated campaigns to raise knowledge and awareness among the general public about these mechanisms and related issues.
- Periodically evaluate the effectiveness of reporting mechanisms and review their functioning, resource allocation and promotion campaigns according to results.

## D2.4 - Reporting mechanisms

### Capacity-building steps



- Review national legislation to ensure that emerging illicit online activities are covered by existing criminal legislation.

The term *cybercrime* can refer to any unlawful activity that involves an electronic element in its preparation or execution.<sup>350</sup> This can include attacks on:<sup>351</sup>

- **Individuals**, including identity theft, personal data theft, fraud and financial theft, e-reputation, online sexual abuse and incitement to racial hatred. This is typically done through malware, spam, phishing and other social engineering techniques.
- **Industry**, including theft of money and theft of data that leads to reputational damage, intellectual property infringements, disruption or denial of service and production. This is often done through botnets, malware, hacking, social engineering and intelligence gathering.
- **National infrastructure**, including attacks on government, law enforcement agencies and CNI, using many of the techniques listed above.
- **National security**, including espionage and terrorism, using many of the techniques listed above.

The type, target and frequency of cyber-attacks are continually changing as new technology is developed and used in different areas of society.<sup>352</sup> It is very difficult for policy and legislation to keep up with the pace of change in this field; there is often a delay in recognising the potential abuse of new technology, and adjusting or drafting new national criminal law takes time.<sup>353</sup>

Reports of illicit cyber activity should translate into a continuous updating of criminal legislation to take account of new types of attack and illicit activities. Legislation is the foundation for the investigation and prosecution of cybercrime.<sup>354</sup> If existing legislation does not adequately account for current trends in illicit activities, reporting mechanisms can still be used to collate information and identify trends in cyber activity, but the reports themselves cannot be used as the basis for criminal investigation. Information on cyber trends can be used by government, businesses and citizens to help protect their systems more effectively and mitigate the effects of any attack.

There are a number of ways to improve the drafting of cybercrime legislation, including:<sup>355</sup>

- **Focus on gaps in existing legislation:** Existing laws often cover many types of illicit online activity. For example, laws covering forgery can often be applied to offline and online forgery. It is important to identify types of cybercrime that are not covered by existing legislation, and focus resources on legal amendments or drafting new legislation.
- **Consult specialist CSIRTS:** This can help identify abuses of new technology that feed into adjustments to national law.
- **Execute the drafting of new legislation with international support and cooperation:** Collaborating with international partners, particularly those with

more advanced cybersecurity capacity and legislation, can help identify rapid developments in technology, reduce duplication of effort, and increase international harmonisation with other legal approaches.



- Establish reporting channels for illicit online activities and launch coordinated campaigns to raise knowledge and awareness among the general public about these mechanisms and related issues.

There is no set formula for setting up a reporting mechanism for the first time. It can be done in a number of ways, using different formats, funding structures, and management and organisational structures.<sup>356</sup> Reporting mechanisms can be provided across a number of different platforms, including telephone and the Internet, and may be implemented to different degrees of specificity, ranging from general cybercrime to particular areas of cybercrime such as fraud or child pornography.<sup>357</sup>



#### Examples of cybercrime reporting platforms

**Internet Signalement** is a web-based platform in France that allows users to report instances of offensive or illicit material online.<sup>358</sup> It was set up in 2009 through funding provided by the Ministry of Interior.<sup>359</sup>

**Action Fraud UK** is a central reporting platform for all fraud and financially motivated Internet crime in the UK. Users are able to access an online reporting page or provide reports through a telephone hotline.<sup>360</sup>

The **Internet Crime Complaint Centre (IC3)** is an online reporting mechanism in the US that enables citizens to report instances of Internet-facilitated criminal activity. The platform was set up by the Federal Bureau of Investigation in 2000, and covers intellectual property rights, computer intrusions (hacking), economic espionage and theft of trade secrets, online extortion, international money laundering, identity theft and other forms of cybercrime.<sup>361</sup>



Reporting mechanisms are not only set up by public sector organisations, but also by private-sector companies, public-private partnerships and not-for-profit organisations.<sup>362</sup> The **Anti-Phishing Working Group** is an example of a not-for-profit organisation that provides a reporting mechanism and high-level analysis of instances of cybercrime.<sup>363</sup>

There are a number of general steps that may be useful when establishing a reporting mechanism, including:<sup>364</sup>

- **Define the major objectives of a reporting mechanism.** Will the reports be for law enforcement investigation, judicial prosecution, threat analysis, or something else? What is the target audience of the proposed mechanism?
- **Remain open for insights.** Reporting mechanisms are sometimes set up with a mandate for a particular threat. This approach, however, can ignore the concerns and preferences of individuals and businesses. Flexibility can help build better and more targeted responses to threats.

## D2.4 - Reporting mechanisms

- **Use the most suitable interface.** This can depend on internal factors such as budget, availability of skills, and organisational structure and leadership. It can also depend on external factors, in particular the preferences of users.
- **Streamline operations and share results.** In particular, it is important to explicitly define how information is collected, analysed and distributed across public agencies and authorities to avoid duplication of effort and improve coordination.

There are also a number of more general considerations that should be taken into account when devising a reporting mechanism, including:<sup>365</sup>

- **Political and senior management support:** This is important for securing funding and personnel, and for promoting the mechanisms across all levels of government.
- **Stakeholder management involvement (e.g. law enforcement, CSIRTs, education stakeholders):** Senior managers from key stakeholders affected by issues to be reported should engage with the reporting mechanism's management in order to identify and help solve problems during both the establishment and operational stages.
- **Implementation by experienced ICT project managers and digital investigators:** Experienced specialists are required during the setup stage to install ICT equipment and define the working structures of the reporting mechanisms. They are required during the operational stage to maintain and improve the platform, and handle any problems or complaints.
- **Support from the judiciary:** Law enforcement is not always best placed to decide which reports should be pursued and prosecuted. This process can be supported with formal involvement from the judiciary, as well as other stakeholders with technical and subject matter expertise relevant to the issue at hand.
- **Participation from Internet users:** Engaging with the end-user can help identify what is required from the reporting mechanisms, in what format, and for what reasons.
- **Capacity to measure return on investment:** See section below.
- **Building awareness of the reporting mechanisms:** Awareness of reporting mechanisms among citizens and businesses is critical to the success of those mechanisms. In short, if people are unaware of the existence and purpose of reporting mechanisms, they are less likely to use the platforms to report relevant cyber incidents.



Implementing initiatives to help **build awareness** of reporting mechanisms is an important driver of success, and efforts to increase awareness of these mechanisms should be incorporated into early stages of planning and implementation, and continued thereafter.

During the launch phase of a reporting mechanism, awareness campaigns can be implemented that involve local media (press articles, TV interviews, posters, etc.), SMS messaging, leaflets and social media campaigns.<sup>366</sup> During the operational phase of a reporting mechanism, a number of other methods can be used, including the publication of regular reports, communication through social media, partnering with ISPs for website referencing, producing regular press reports, publishing periodic public service announcements, and attending national and international cybercrime conferences and meetings.<sup>367</sup>



**Funding** plays a critical role in determining the scope and role of reporting mechanisms. In particular, the level of specificity of the mechanism to particular threats (as opposed to more general cybercrime), the method used to collect and analyse reports, and the size of the population are all influenced by the level of available funding. The main areas of expenditure include hardware and maintenance of websites (if applicable), the implementation and maintenance of databases, and the employment of analysts and law enforcement officers to retrieve and process the information.

There are a number of different funding structures that support reporting mechanisms. Most are supported entirely or primarily by public funding, but there are notable exceptions. For example, Signal Spam in France and the APWG in the US are both privately funded initiatives that receive payment through membership fees in return for providing valuable information to businesses and governments.



### Signal Spam (France)

Signal Spam is a private not-for-profit initiative funded by industry. It provides an Internet-based complaints form and a client email plugin to allow businesses to report instances of spam, phishing and abusive email marketing. Businesses pay a membership fee, and in return receive valuable information on current cyber threats.<sup>368</sup> Reports are also redirected to the most relevant public authorities, including the data protection authority and law enforcement. By 2012, around 2.5 million complaints had been received. The platform has helped law enforcement agencies, industry, businesses and public authorities to collaborate more closely.

## D2.4 - Reporting mechanisms



- Periodically evaluate the effectiveness of reporting mechanisms and review their functioning, resource allocation and promotion campaigns according to results.

Measuring and evaluating performance can be used as a basis for designing and implementing improvements, and can indicate whether the financial investment in the mechanisms corresponds to their perceived impact.<sup>369</sup> An evaluation may consider a multitude of different factors, including frequency of use, ease of use, rate of successful prosecutions (if relevant), value for money, readiness for future developments, and impact on understanding of cyber threats and trends.

### Additional resources



- ITU. 2012. Understanding cybercrime: Phenomena, challenges and legal response. Geneva: ITU.
- ITU. 2012. *HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts*. Geneva: ITU.
- ITU. 2014. The quest for cyber confidence. Geneva: ITU.
- GLACY (Global Action on Cybercrime). 2014. Good practice study: Cybercrime reporting mechanisms. September. As of 17 July 2017: <https://rm.coe.int/168030287c>

## D2.5 – Media and social media

### Overview

This factor looks at the implications of online media and social media on cybersecurity, focusing on the role these media have in conveying information about cybersecurity and the extent to which cybersecurity is a subject of discussion and debate on online media and platforms.

Cybersecurity concerns pertaining to Online Social Media (OSM) and online media overlap with those more broadly related to trust in the Internet and issues of privacy. These may be amplified in the media and OSM environment due to the potential for rapid dissemination of information on these platforms. Online media and OSM are also susceptible to traditional cyber-attacks such as malware and distributed denial-of-service (DDoS) attacks. DDoS attacks can be particularly harmful by temporarily silencing entire platforms and thus silencing open discussion. There are also concerns about ‘over-policing’ or ‘over-surveillance’ that threaten the public’s trust in media and OSM.<sup>370</sup>

Cybersecurity in media and OSM has its own unique challenges to consider and overcome. Areas of concern are issues of privacy, use of personal information, protection of freedoms and the spreading of so-called ‘fake news’ (i.e. false, often sensationalised information, disseminated under the guise of legitimate news reporting).<sup>371</sup>

It is therefore important for policymakers to identify ways in which the use of OSM can be regulated, while ensuring that users’ rights to privacy and freedom of expression are protected. Box 2.5 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 2.5: Steps for facilitating the development of a healthy media and social media (D2.5)

- Ensure that existing laws and regulations do not hinder an open discussion of cybersecurity issues on national media and social media.
- Stimulate public debate on cybersecurity-related issues through state-controlled media and awareness-raising campaigns.

### Capacity-building steps



- Ensure that existing laws and regulations do not hinder an open discussion of cybersecurity issues on national media and social media.

Although OSM and online media technologies raise, among other issues, a large number of information management considerations (e.g. issues of privacy, security, accuracy and archiving for data pertaining to personally identifiable information), no international standards have emerged yet for their regulation. Guiding principles underpinning traditional regulations concerning information can be taken to apply to this context, but beyond this the rapid adoption of OSM and the role played by online media in contemporary society has outpaced the development of regulatory frameworks.<sup>372</sup>

## D2.5 - Media and social media



As the prevalence of OSM use is a relatively recent phenomenon, concerns have been articulated in relation to the lack of explicit laws and regulations covering these platforms. Aligning national laws and regulations with international good practices may help strengthen integrity and prevent the dilution of trust in these platforms.<sup>373</sup>



Creation and amendment of laws and regulations may create overlaps with existing legislation. Although these overlaps should be noted, overlap commonly occurs in criminal law and it is not desirable to deliberately avoid such overlaps.<sup>374</sup>



- Stimulate public debate on cybersecurity-related issues through state-controlled media and awareness-raising campaigns.

Public debate on cybersecurity-related issues on online media and OSM can be stimulated by a range of public and private entities, as well by non-governmental organisations. The use of OSM has become an increasingly popular way for governmental agencies and stakeholders to reach out and engage with the general public. In this context, OSM provide a good platform for organisations to spread awareness about their work and activities.<sup>375</sup>



Use of OSM may also pose risks and challenges. Organisations should seek guidance on good practice and set rules for employees representing the organisation. Understanding potential security threats and mitigating risks of identity theft and malware are examples of considerations for organisations and users while using OSM.<sup>376</sup>

With the advent of targeted online marketing, organisations can reach specific user groups more effectively. Government organisations can take advantage of this by specifically targeting demographic groups that may be most susceptible to cyber-attacks. OSM users with particular interest in cybersecurity can also be targeted with awareness campaigns in the hope that they will spread the campaign to their wider network of connections and a more general audience. Further information on awareness-raising campaigns, their purpose and ways in which they can be established is provided in Section 3.1 of this document.<sup>377</sup>



Awareness campaigns should not be limited to only one medium. Despite the growth in OSM, many people do not have access or are infrequent users, and are therefore more effectively reached through awareness campaigns on television, government webpages, newspapers and other print notifications.



The US DHS is an active user of Twitter. The DHS uses this OSM platform to raise awareness of cybersecurity issues and threats among its followers, as well as to spread public service announcements. As of 2017, the US DHS cybersecurity department has more than 106,000 followers.<sup>378</sup>

### Additional resources



- Bertot, John Carlo, Paul T Jaeger & Derek Hansen. 2012. The impact of policies on government social media usage: Issues, challenges, and recommendations. *Government information quarterly* 29(1): 30-40.
- Goolsby, Rebecca. 2013. On Cybersecurity, Crowdsourcing, and Social Cyber-Attack. 4 March. As of 17 July: <https://www.wilsoncenter.org/publication/cybersecurity-crowdsourcing-and-social-cyber-attack>
- International Telecommunication Union (ITU). 2014. The Quest for Cyber Confidence. Geneva: ITU.



## **Dimension 3**

### **Cybersecurity, education, training and skills**



## Dimension 3 – Cybersecurity education, training and skills

---

Dimension 3 of the GCSCC CMM looks at the national availability of high-quality cybersecurity education, training, and awareness-raising campaigns, and capacity to develop and deliver these. This includes educational and training offerings for various groups of government stakeholders, the private sector and the general population.

This dimension of the GCSCC CMM comprises three factors. The following sections discuss capacity-building steps that national decision makers can implement to build capacity across the following issue areas:

### **1. D3.1 – Awareness raising**

This factor looks at the availability, provision and reception of cybersecurity awareness programmes and initiatives targeting stakeholders in the public, private, academic and civil society sectors, as well as the general public.

### **2. D3.2 – Framework for cybersecurity education**

This factor looks at the availability and provision of cybersecurity education at the primary, secondary and tertiary levels of education.

### **3. D3.3 – Framework for professional training**

This factor focuses on the availability and provision of professional cybersecurity training to build cadres of cybersecurity professionals, including through horizontal and vertical cybersecurity knowledge transfer within organisations, and through continuous skills development.

## D3.1 – Awareness raising

### Overview

This factor focuses on the availability, provision and reception of cybersecurity awareness programmes and initiatives targeting stakeholders in the public, private, academic and civil society sectors, as well as the general public.

At its most basic level, cybersecurity awareness constitutes an understanding that cyberspace is fundamentally insecure, and that malicious actors may seek to damage or exploit hardware, software, behaviours and information at a personal, commercial or state level. Cybersecurity awareness raising, however, seeks to go beyond this basic description of awareness, and build a more nuanced understanding of cybersecurity across stakeholder groups. The rationale behind this is that individuals, organisations and governments should have an informed understanding of the actors and motivations involved, the ways in which various cyber-attacks may occur (including the signs to look out for), the potential impact of cybersecurity breaches, and the ways in which the frequency and severity of cyber-attacks can be reduced.

Awareness of cybersecurity is relevant across all parts of society, and includes individuals acting in a personal, employee and executive capacity. At a personal level, an improved awareness of cybersecurity enables individuals to better protect themselves against threats ranging from malicious software and online theft to the misuse of personal information and breaches of personal privacy. There are similar considerations at an employee level, although in this instance it is the company (as opposed to the individual) that is primarily at risk. At an executive level, individuals typically control greater resources and hold greater influence, and consequently are in a stronger position to elevate the profile of cybersecurity, and to develop and implement cybersecurity strategies to mitigate against threats at an organisational and, in some instances, national level.

Cybersecurity awareness raising should be directed at all audiences and can be achieved through various means, including general awareness campaigns, targeted cybersecurity awareness programmes, and dynamic awareness-raising campaigns that measure impact and effectiveness and adapt accordingly. Box 3.1 and the following section outline a number of steps that can be taken to help increase awareness of cybersecurity at a national level.

### Box 3.1: Steps for improving cybersecurity awareness-raising capacity (D3.1)

- Establish a national programme for cybersecurity awareness to address a wide range of demographics and issues.
- Develop and implement awareness-raising materials and programmes in consultation with relevant stakeholders from different sectors.
- Devise tailored information, training and exercise programmes on cybersecurity with clearly defined learning outcomes for executives in the public, private, academic and civil society sectors.
- Evaluate the effectiveness of cybersecurity awareness-raising campaigns and learning interventions, and review existing initiatives on the basis of results.
- Monitor adherence to cybersecurity behaviour standards and best practices.

- Periodically assess the level of correspondence between good practices and the cyber conduct of members of the public service, private sector and wider society.
- Regulate provision and accreditation of awareness courses in cybersecurity to make these mandatory for executives across nearly all sectors.

### *Capacity-building steps*



- Assign a task owner to develop and implement a national programme for raising cybersecurity awareness.

To increase cybersecurity awareness at a national level, the first stage is to assign a dedicated **task owner** who is responsible for developing a cybersecurity awareness programme. This is typically outlined in a national cybersecurity strategy, with one or more government agencies tasked with cybersecurity awareness raising. The selected agency is often already engaged with national-level cybersecurity in some form. This helps ensure sufficient expertise, profile and legitimacy when providing information and advice. In some instances, independent organisations or public-private partnerships have been established, either instead of or alongside internal government agencies, in order to promote cybersecurity awareness. Since aspirations, needs and organisational structures differ between countries, the designation of a **task owner** should be made on an individual country basis.



In the UK, the **National Cyber Security Centre**, which is part of GCHQ, is tasked with cybersecurity outreach and awareness building, including capability development in industry and academia. This is one of several responsibilities for the centre, which also include responding to cybersecurity incidents and providing security to public and private sector networks.<sup>379</sup>

In Norway, cybersecurity awareness raising is shared across a number of government agencies, including the **Business Security Council**, the **Norwegian Data Protection Authority**, the **Post and Telecommunications Authority** and the **Media Authority**.<sup>380</sup> The Norwegian government also works closely with **The Norwegian Centre for Information Security**, which is an independent organisation that partners with government, businesses and research facilities to promote cybersecurity awareness and guidance.

In Malaysia, **CyberSAFE** is the cybersecurity awareness and outreach programme of the Malaysian government's **Outreach and Corporate Communications Department**. The department sits within CyberSecurity Malaysia, which is the national cybersecurity agency within the Ministry of Science, Technology and Innovation.<sup>381</sup>

In the US, the **Department of Homeland Security** runs the Stop.Think.Connect. campaign, which is a national cybersecurity awareness-raising programme that is implemented in collaboration with representatives from the private sector from the **National Cyber Security Alliance (NCSA)**. The NCSA is a private sector organisation with representatives from across US industry.<sup>382</sup>

### D3.1 – Awareness raising



The development and implementation of cybersecurity awareness programmes requires both financial and human resources. If awareness raising is assigned as a new task for a government agency, additional resources may be required to enable the agency to carry out the task without impacting its work elsewhere.<sup>383</sup>



- Develop and implement awareness-raising materials and programmes in consultation with relevant stakeholders from different sectors.

Once a **task owner** is assigned, the next stage is to design and implement a cybersecurity awareness-raising campaign. The goal of an awareness campaign is not simply to inform a target audience of risks and mitigation strategies within cyberspace, but rather to change their behaviour so that they use ICTs in a more secure manner.<sup>384</sup>

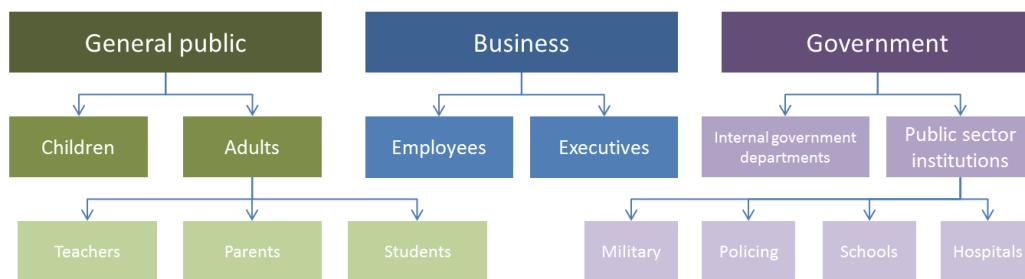
When designing this campaign, a number of factors should be considered, namely:<sup>385</sup>

- Stakeholders
- Goals
- Target audience
- Situational awareness
- Strategy
- Tactics
- Measurements of success.

Expanding on each of these points, it is important to map the relevant **stakeholders** in any awareness-raising campaign at an early stage in the planning process. In any given country, there are a wide range of stakeholders with an interest in improving cybersecurity. These include other governmental agencies, ISPs, software and IT companies, universities, telecommunication companies, financial institutions, educational establishments, and non-governmental organisations. Engaging with stakeholders at an early stage in the planning process ensures that their insights and experience are included throughout the campaign. Stakeholders to be involved should be selected based on their expertise and responsibilities pertaining to a campaign's area of focus. Early stakeholder engagement may also increase the probability of further support and participation in the programme through, for example, the provision of further resources and assistance in information dissemination.<sup>386</sup>

The next stage in developing a cybersecurity awareness campaign is to identify the **goals** of the campaign, which is closely linked to both target **audience** and **situational awareness**. It is important to identify *who* the campaign will target, and then investigate the existing competences, requirements and resources available within this target group. From this information, the aims of the awareness campaign can be established. These may include, for example, reducing the number of cybersecurity incidents, changing attitudes and behaviour towards cybersecurity, or developing a more critical understanding of purchasing new computing equipment. The audience can be defined in a number of different ways, to varying degrees of granularity, as illustrated in Figure 3.1 below.<sup>387</sup>

**Figure 3.1: Examples of different target audiences at varying degrees of granularity**



SOURCE: RAND Europe analysis

The **strategy** and **tactics** of an awareness campaign should then be developed to outline the ways in which the goals of the campaign will be achieved given the situational awareness of the target audience. The strategy should outline the high-level roadmap required to achieve a given goal, whereas the tactics should detail the individual, tangible steps required. This includes the platforms for delivery, the required activities and resources, and the timeframe for completion.<sup>388</sup>



It is important to develop an effective **logo**, **slogan** and **message** for any awareness campaign. An awareness campaign should attract the attention of the target audience, be simple and easy to understand, and be recognisable and memorable in the future. The content of an awareness campaign should avoid technical jargon, and should be phrased in a positive manner, using simple language.<sup>389</sup>

## D3.1 – Awareness raising



A number of different tactics can be used as part of an awareness-building campaign, including:

- Developing a website;
- Designing and distributing educational material (e.g. example presentations, business toolkits);
- Developing strategic partnerships (e.g. with business organisations, community groups, youth groups);
- Organising information events (e.g. public talks, roundtable discussions);
- Engaging with media outlets (e.g. newspapers, news websites, television, radio);
- Developing a presence on social media.

The platform and content should be selected and developed according to the specific target audience. Further information on the relative strengths and weaknesses of different approaches is available in the OAS Cybersecurity Awareness Campaign Toolkit referenced in the resource list at the end of this section.<sup>390</sup>

**Safer Internet Day**

Safer Internet Day is a designated annual day in February that aims to raise awareness and draw attention to emerging online security issues. It was initially set up by the European Commission, but is now observed in over 130 countries worldwide.<sup>391</sup>



In the UK, GCHQ has published toolkits for novices to develop their cybersecurity capabilities across a number of fundamental areas, including: web applications, infrastructure security, mobile devices, Java, PHP, C++, PYTHON, malware analysis, forensic investigations and incident response.<sup>392</sup>

Finally, the **measurements of success** for an awareness campaign should be considered before the campaign is implemented. Implementation should be accompanied by periodic measurements of success and re-evaluation of aims, strategy and tactics. This is discussed in further detail in the subsequent capacity-building step on evaluating the effectiveness of cybersecurity awareness-raising campaigns and learning interventions.



Research suggests that awareness campaigns often fail to improve the behaviour of their target audience. A number of common pitfalls have been identified, including:<sup>393</sup>

- Overly negative messaging
- Excessive demand on effort and skill
- Focus on compliance rather than behavioural change
- Lack of engaging and appropriate material
- Overly complex messaging
- Overly narrow focus that is insufficient for the target audience
- Failure to adapt to cultural differences
- Absence of any evaluation.



- Devise tailored information, training and exercise programmes on cybersecurity with clearly defined learning outcomes for executives in the public, private, academic and civil society sectors.

Clear leadership and funding from senior executives is an important factor in driving behavioural change within both private and public sector organisations.<sup>394</sup> Developing tailored awareness campaigns and programmes for executives within specific sectors is one way of achieving senior-level buy-in, which in turn helps ensure that sufficient activity and resources are assigned to improving cybersecurity throughout the organisation. The development of an awareness-building campaign for senior executives should follow the same eight steps as outlined above: identifying stakeholders, determining goals, defining an audience, conducting a situational analysis, developing a strategy, developing tactics and identifying measurements of success – although the output of each of these steps will be tailored to a more defined purpose and outcome.



There are a number of ways of engaging with senior executives, including the following suggestions:<sup>395</sup>

- Produce regular, targeted and concise cybersecurity briefings and op-eds.
- Conduct high-level, semi-regular roundtable discussions for executives.
- Provide expert speakers to talk at monthly or annual meetings in organisations or at conferences.
- Provide training to executives through tailored training events.

## D3.1 – Awareness raising



It is critical to ensure that the training and education is geared towards current and emerging needs. Training needs will change due to technological advances and changes to the threat landscape, legal regulations and national security directives. It is important to ensure that the development of training and education is cognisant of future developments and incorporates this thinking early in the programme's development.<sup>396</sup>



- Evaluate the effectiveness of cybersecurity awareness-raising campaigns and learning interventions, and review existing initiatives on the basis of the results.

Measuring the effectiveness of a cybersecurity awareness campaign can be difficult, particularly when trying to evaluate changes in behaviour.<sup>397</sup> However, research suggests that the failure to evaluate a cybersecurity awareness campaign is a common feature of campaigns.<sup>398</sup> It is important to measure the success of awareness-raising campaigns and learning interventions, as this will allow the intervention team to **monitor progress towards the established objectives** and, in case of deviations, to implement the necessary changes. Lessons learned can also be taken into account in the design of future interventions.

There are a number of steps required to conduct an effective evaluation, namely:

- **Set intermediate objectives** based on the final goal of the campaign. If the causal link between them is well evidenced, the intermediate goals should allow the progress of the intervention to be monitored, and allow the campaign managers to anticipate whether or not it is on track to achieve the ultimate goal.
- **Determine which outputs, outcomes and impacts will be measured.** Outputs are tangible products of activities (e.g. the launch of an event or a website or the organisation of workshops, courses, contests, etc.) and outcomes are the results of those activities (e.g. participation in events, increased awareness in relation to the topic, etc.). The impact of a campaign concerns the causal link between the intervention and the observed result (i.e. the extent to which the creation of a cybersecurity mindset can be attributed to a specific campaign).
- **Determine which indicators will be used to measure the outputs, outcomes and results.** This should be done according to the size of the campaign, as well as the appropriateness and the availability of data, both quantitative and qualitative. Quantitative data demonstrates the extent to which a change has happened and can be measured with a number (e.g. number of articles written, number of visits to a website, number of attendees at an event, etc.). Qualitative data looks at the change in attitude, opinions or feelings, and can be collected through methods including interviews, focus groups and social network analysis.

- Determine the sources from which the data will be collected. This includes social media, visits to a website, interviews, media coverage, participation in events, etc.



When measuring visits to a website, it is important to pay attention to the number of visits, but also to **unique visitors**. Likewise, the number of **new visitors** will provide useful information to discern whether or not the campaign is reaching a broader audience.

The metrics for an evaluation of a cybersecurity awareness-raising campaign should be determined before the campaign is implemented, and examples are provided in Table 3.1 below.

**Table 3.1: Examples of metrics for success**

Metrics for output	Metrics for outcomes	Metrics for impact
Media coverage – quantity	Media coverage – quality	Less cybercrime
Web and media reach (number of potential people)	Brand awareness	More use of security software
Event attendance	Attitude shift	Cybersecurity budget inclusion
Web visits	Behaviour changes	Better cybercrime reporting
Social sharing events (number of forwarded news items, etc.)		Increased consumer confidence



One of the key challenges is progressing from measuring outputs to measuring outcomes. Outputs are easier to measure but less meaningful than outcomes.



- Periodically assess the level of correspondence between good practices and the cyber conduct of members of the public service, private sector and wider society.

In addition to evaluating individual awareness-raising campaigns, a periodic evaluation of the cybersecurity awareness and behaviour of individuals across the public and private sectors can be used to understand the existing capability and emerging trends at a societal level. To help contextualise and evolve campaigns over time, research should be performed to identify gaps in understanding of cybersecurity practice among different target groups, as well as broader areas where further attention is required. Governmental research departments, as well as academic and research institutions, would be well placed to undertake such endeavours. Research undertaken in this context should focus on a range of aspects of a national cyber ecosystems and cybersecurity habits, for example by investigating the following research

### D3.1 – Awareness raising

questions in respect of a particular country context and target audience (e.g. general public, public sector employees, private sector employees):<sup>399</sup>

- How connected is the country in question?
- Where and how are people connecting to the Internet? Who is online?
- How is the Internet being used for business?
- What are the cybersecurity risks the country in question is facing?
- What are the economic losses from cyber threats?



#### **Study on the Norwegian National Cyber Conduct<sup>400</sup>**

The Norwegian Centre for Information Security (NorSIS) published in 2016 a report that explores Norway's National Cyber Conduct. NorSIS is an independent organisation that partners with the Norwegian government to conduct research into cybersecurity. The study focused on Norway's general population and investigated the following research questions:

- What characterises the Norwegian cybersecurity culture?
- To what degree does cybersecurity education influence the Norwegian population's cybersecurity behaviour or awareness?
- How does the Norwegian population relate and react to cyber risks?
- To what degree does the individual take responsibility for the safety and security of the cyberspace?

The study found that, although cybersecurity education should not be seen as a comprehensive solution for all challenges in this domain, cybersecurity education correlates with positive behavioural patterns (i.e. people who are educated in cybersecurity act more securely online).

The study also found significant potential for improvement in how the Norwegian population is educated and behaves as regards cybersecurity. The study stressed that, due to limited governmental action, substantial responsibility for educating Norwegian citizens had been left to private sector actors. This, in turn, resulted in uneven levels of knowledge and awareness, particularly among different age-groups. The study recommended that a stronger commitment be made by the government to ensure that the population as a whole is educated in cybersecurity.



- Regulate provision and accreditation of awareness courses in cybersecurity to make these mandatory for executives across nearly all sectors.

Regulation and accreditation of awareness courses are useful tools which may be employed to ensure that executives receive cyber awareness courses, and that these courses adequately cover their needs.



Although the terms 'accreditation' and 'certification' are often used interchangeably, they refer to very different processes. **Accreditation** grants public recognition to education providers or training programmes, whereas **certification** is a qualification granted by a non-governmental institution to an individual who has met certain established requirements in the framework of a programme or activity (e.g. a qualifying exam). Certification does not imply public recognition.

If an appropriate accreditation body does not exist, then an accreditation body may be set up as a not-for-profit or for-profit organisation, or as a government agency or body. It is important to decide which **legal status** is the best fit for the tasks that the organisation will undertake.



Although there is no one-size-fits-all model, there has been a **tendency to favour not-for-profit organisations** over for-profit or governmental agencies. Not-for-profit organisations benefit from a positive external image, and their non-governmental status allows for greater flexibility.

Once established, it is necessary to adopt **assessment criteria** that will serve as a guide for the evaluation of programmes. To ensure transparency in the process, accreditation bodies often publish the framework or standards on which the criteria are based.



#### **Certification of an Executive Cyber Awareness course by GCHQ<sup>401</sup>**

The Executive Cyber Awareness course provided by Protection Group International is among the first to be certified by the UK National Technical Authority for Information Assurance. This scheme has been created to certify two levels of cybersecurity skills: awareness and application. GCHQ provides on its website a link to the *IISP Skills Framework*, which forms the basis of their assessment criteria.<sup>402</sup>

#### Additional resources



- ENISA. 2007. Information security awareness initiatives: Current practice and the measurement of success. Heraklion, Greece: European Network and Information Security Agency.
- Organization of American States. 2015. Cybersecurity Awareness Campaign Toolkit. Washington, DC: OAS Secretariat for Multidimensional Security.
- Security Awareness Program Special Interest Group PCI Security Standards Council. 2014. Information Supplement: Best Practices for Implementing a Security Awareness Program. PCI Security Standards Council.
- Wilson, Mark. & Joan Hash. 2003. Building an information technology security awareness and training program (NIST Special Publication 800-50). National Institute of Standards and Technology.

## D3.2 – Framework for cybersecurity education

### Overview

This factor focuses on improving the availability and provision of cybersecurity education at primary, secondary and tertiary levels of education. Education in a professional context (i.e. post-tertiary education) is not considered in this factor, as it is discussed in detail in Factor D3.3 (Framework for professional training) below.

At a general level, the aim of cybersecurity education is to provide students with sufficient knowledge and skills to pursue a successful career in cybersecurity or an IT-intensive domain, and to encourage students to select this career path. It is more than awareness raising, which, as discussed under the previous factor, aims simply to induce behavioural changes in order to increase security at a personal and corporate level. Cybersecurity education should develop the specific technical and non-technical (e.g. strategic and managerial) skills that are demanded in the aforementioned domains, both in the public and private sectors.

There are a number of steps involved in establishing a national framework for cybersecurity education, which are outlined in Box 3.2 below and expanded on in the following section.

### Box 3.2: Steps for developing a national framework for cybersecurity education (D3.2)

- Nominate a task owner responsible for (i) oversight of education initiatives; and (ii) liaising with public sector bodies and relevant private sector stakeholders.
- Map the existing cybersecurity education landscape and identify gaps in provision.
- Select the target audience(s) of the cybersecurity education programme.
- Develop an appropriate framework for the provision of the education programme.
- Evaluate and modify cybersecurity education and training in consultation with stakeholders from public and private sectors, academia and civil society; ensure the ongoing delivery and improvement of cyber education and training.

### Capacity-building steps



- Nominate a task owner responsible for (i) oversight of education initiatives; and (ii) liaising with public sector bodies and relevant private sector stakeholders.

The first step in developing a national framework for cybersecurity is assigning a task owner within the national government who is responsible for the provision of cybersecurity education at primary, secondary

and tertiary levels of education. The task owner should provide oversight and accountability for designing and implementing a national-level cybersecurity education framework.



Cybersecurity education is relevant to many different areas of society, from industry and government to academia, primary and secondary education. A designated task owner should be able to engage with each of these sectors, both internally through collaboration with other government departments that operate in these areas, and externally through engagement with private stakeholders.



### Cybersecurity education in the UK

In the UK, the National Cyber Security Strategy – which includes a strategy for cybersecurity education – is developed and led by the Cabinet Office. The Cabinet Office is a department of the UK civil service that not only supports the UK Prime Minister and the Prime Minister's close team, but also supports the government in the development, coordination and implementation of national-level policy. The Cabinet Office also leads on a select number of critical policy areas, including national security and joint intelligence.<sup>403</sup> This combination of broad cross-government interaction and select specialisations means that the Cabinet Office is well-placed to lead on national cybersecurity education development. Nonetheless, other government departments also play an important role in developing and implementing the provision of cybersecurity education, including: the Department for Culture, Media and Sport, which runs the *Cyber Schools Programme*<sup>404</sup> and provides funding for Master's degrees accredited by GCHQ;<sup>405</sup> the National Cyber Security Centre, which is structured under GCHQ, and which runs the Cyberfirst programme that provides a framework and funding for cybersecurity degrees and training;<sup>406</sup> and the Department for Education, which provides funding to a number of universities and higher education institutions to develop apprenticeship schemes that include specialised cybersecurity courses.<sup>407-408</sup>



- Map the existing cybersecurity education landscape and identify gaps in provision.

Once a task owner is assigned, a number of steps are required to design and plan any programme or initiative that seeks to provide effective cybersecurity education. One of the early steps in the process should involve a review and mapping of the existing cybersecurity education landscape that includes:

- Relevant stakeholders
- Existing provision of cybersecurity education
- Existing qualification and certification programmes
- Existing and future requirements in the professional environment.

### D3.2 – Framework for cybersecurity education

Expanding on the first of these points, it is important to be aware of the **relevant stakeholders** involved in cybersecurity. This includes organisations that are already involved in the direct provision of cybersecurity education, and organisations that may wish to engage with and support the provision of further cybersecurity education due to the nature of their organisation or field of work. There are a number of reasons for mapping relevant stakeholders, including reducing any unintentional duplications of activity, and supporting the development of more effective long-term policies through improved knowledge transfer and improved potential for effective government partnerships. The range of relevant stakeholders will differ on a country-by-country basis, but it may include public and private schools, universities and educational centres, ISPs, private sector cybersecurity companies, not-for-profit organisations, and other relevant publicly funded and government institutions.



#### Examples of different types of stakeholders involved in cybersecurity education

The International Association of Privacy Professionals (IAPP) is a **not-for-profit** organisation that offers training and resources for professional development, provides internationally recognised cybersecurity certification, and also facilitates a wider network of cybersecurity experts and enthusiasts.<sup>409</sup> IT Governance Ltd is a **private sector** professional services company that provides information, advice, books, tools, consultancy and training for IT governance, risk management, compliance and information security.<sup>410</sup> Carnegie Mellon is a **private research university** that offers a number of master-level courses in information security,<sup>411</sup> and the Singapore Institute of Technology is a **public university** that provides undergraduate education in information security.<sup>412</sup> The National Cyber Security Centre is a **public organisation** in the UK that provides technical incident response as well as leadership, education, advice and resources in cybersecurity.<sup>413</sup>

It is also important to understand **existing and future requirements in the professional environment**, and map these to educational requirements, primarily at secondary and tertiary levels of education. The purpose of this analysis is to identify gaps and shortfalls in any existing provision of cybersecurity education, and to inform the development of future cybersecurity education programmes so that the workforce meets future requirements of the cybersecurity sector.



Cybersecurity is a rapidly changing sector, and it is insufficient to develop educational programmes that address skills to meet the existing demand. The future of cybersecurity may be very different to the present, with artificial intelligence,<sup>414</sup> big data,<sup>415</sup> the Internet of Things and ethical hacking,<sup>416</sup> along with other as-yet unidentified trends, potentially increasing in importance.



➤ Select the target audience(s) of the cybersecurity education programme.

Following an initial mapping exercise, the target audience of a cybersecurity education programme should be selected. The categorisation and selection of a target audience can be made at varying degrees of granularity. For example, the audience may be broken down into the areas and associated aims presented in Table 3.2 below.

**Table 3.2: Cybersecurity education target audiences and associated educational aims**

Category	Aim
Students in primary education	Improve basic understanding of cybersecurity
Students in secondary education	Develop basic technical skills and policy awareness for cybersecurity
Students in university education	Acquire necessary skills and understanding to begin a successful career in cybersecurity

However, a more granular categorisation may be made, particularly when addressing more specific gaps in the provision of existing cybersecurity education or shortfalls in the existing or future professional environment.



**Underrepresentation among American cybersecurity professionals**

Women and African-American populations are underrepresented in the cybersecurity sector in the US. Only 14% of the information security workforce are women<sup>417</sup> and only 3% are African-American, whereas 48% of the general workforce are women<sup>418</sup> and 12% are African American.<sup>419</sup> To address these specific shortfalls in the cybersecurity workforce, a cybersecurity education programme may choose to be more granular and selective in its categorisation and selection of a target audience. In the US, there are organisations that focus specifically on these areas, such as GenCyber,<sup>420</sup> which runs cybersecurity camps, some of which are exclusively offered to girls,<sup>421</sup> and the International Consortium of Minority Cybersecurity Professionals, which aims to achieve a more consistent representation of women and minorities in the cybersecurity industry.<sup>422</sup>

The categorisation and selection of a target audience for a cybersecurity education programme is country-dependent and should be made on an individual country basis. Nonetheless, before finalising the design and implementation of any programme, it should be possible to clearly identify *who* is being targeted.

### D3.2 – Framework for cybersecurity education



- Develop an appropriate framework for the provision of the education programme.

Before implementing a cybersecurity educational programme, it is also important to establish an overarching framework for delivery. More simply, decisions should be taken as to how the educational programme will be delivered. This planning phase can be broken down into the following two areas:

- Relationship with stakeholders
- Format of content delivery.

The **relationship between the task owner and stakeholders** outside of central government can be developed according to a number of different models, including public sector only, PPPs, and private sector only. A *public sector only* model would seek to provide all cybersecurity education using internal government resources without outsourcing to the private sector, whereas a *private sector only* model would seek to use market-correction mechanisms alone to increase the volume and improve the quality of cybersecurity education provided by the private sector. However, one of the more commonly applied models is *public-private partnerships*, whereby a government and one or more private sector organisations agree to collectively provide a product or service through a formal agreement.

There are a number of different types of PPP, including: capital investment, where a government uses tax revenues to provide funding to private organisations to provide a service; private finance initiatives, where the private sector provides funding for the government to provide a service; and goods in kind, where the government provides grants or revenue subsidies to make a particular project more attractive for the private sector.<sup>423</sup> There are a number of advantages of PPPs, including the transfer of risk to the private sector, and increased efficiencies in using existing infrastructure and expertise already built up in private sector organisations. However, PPPs also present their own risks, such as higher transaction costs, reduced government control over public investment, and reduced quality of service if poorly implemented.<sup>424</sup> In cybersecurity, a considerable proportion of infrastructure and expertise are found in the private sector, but PPPs in cybersecurity are particularly challenging due to concerns surrounding trust, control and disclosure, as well as complex regulatory and legal cybersecurity frameworks that exist in some countries.<sup>425</sup>



### Examples of PPPs

PPPs have been used extensively in the cybersecurity domain in the UK, US and elsewhere.<sup>426</sup> The following are examples of these:<sup>427</sup>

- CISCO's Networking Academy has used a PPP model to develop 10,000 ICT academies in 165 countries which deliver a range of courses, including those in cybersecurity and network security.
- The US NCSA is a not-for-profit organisation which includes board members from ADP, AT&T, Bank of America, Comcast, EMC, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, Symantec, Verizon and VISA, and receives funding from both the private sector and the US DHS. The STOP. THINK. CONNECT. campaign was led by the NCSA (together with the Anti-Phishing Working Group) and brought together 25 companies and 7 government agencies to develop an awareness-raising and education platform.
- Trend Micro's Internet Safety for Kids and Families Programme was developed to provide education to parents, teachers and young people on Internet safety issues. Trend Micro is a private data security and cybersecurity company, but has worked with Childnet International, Twitter, Yahoo!, PTO Today and the UK government, among other partners, to develop and deliver the programme.
- The UK's Department for Digital, Culture, Media and Sport's Cyber Schools Programme was developed and implemented in partnership with a combination of public and private stakeholders, namely SANS, BT, FutureLearn and Cyber Security Challenge UK.<sup>428</sup>

In addition to developing a model to define the government's relationship with stakeholders, a cybersecurity education programme should also decide on the **format of content delivery** – put simply, *how* will the education programme actually be delivered? This is influenced to a large degree by the selection of a target audience and the nature of stakeholder relationships, but within each category there are a number of options. In this context, a significant role should be played by a country's Ministry of Education in determining:

- How to integrate cybersecurity into existing curricula;
- How to stimulate the development of cybersecurity courses at secondary and university level.

For example, at the primary or secondary school level, a cybersecurity education programme may focus on providing basic digital literacy to pupils, granting them access to adequate educational resources and ensuring that qualified instructors are available to teach cybersecurity-specific classes.<sup>429</sup> This may be achieved, for example, by providing cybersecurity training and certification to existing school teachers, or by employing external experts from academia, industry or government to visit schools and provide specialised lessons. These lessons can then be supported by tailored educational material that is either

### D3.2 – Framework for cybersecurity education

developed independently or through adapting the ready-to-use educational material that is available online.



#### **European Schoolnet**

European Schoolnet is a network of 31 European Ministries of Education that offers teaching material, resources for pupils, activities and frameworks for pupil- and teacher-led activities.<sup>430</sup>



#### **ENISA Continuing Professional Development Model for School Teachers**

As part of a 2014 Roadmap for Network and Information Security (NIS), ENISA developed an initial framework for providing continuing professional development for school teachers which includes a list of stakeholders, objectives, recommended syllabus, implementation tips, and suggestions for evaluation and metrics.<sup>431</sup>



#### **ISC2 School Presentation Visits**

The International Information Systems Security Certification Consortium (ISC2) is an organisation comprised of certified information and software security professionals that is best known as a certification body, for example for the Certified Information Systems Security Professional qualification, which is accredited by the American National Standards Institute compliant with International Organization for Standardization (ISO) Standard 17024:2003. ISC2 offers one-hour presentation visits to schools that are provided by volunteer security practitioners. The target groups are pupils aged 7–10 or 11–14 as well as parents.<sup>432</sup>

Furthermore, at university level, there are a number of ways in which a national government can facilitate and catalyse the provision of specialist cybersecurity education, including the following:<sup>433</sup>

- Provide funding to university departments to develop cybersecurity research and education provision.
- Incentivise students to select university degrees that include cybersecurity modules and/or specialise in cybersecurity by offering grants, industry placements and/or graduate career opportunities.
- Establish academic centres of excellence in cybersecurity to act as hubs of research and education.
- Encourage networking and information sharing between academic institutions, at both national and international level.
- Develop partnerships between education institutions and other cybersecurity stakeholders to stimulate cybersecurity education initiatives (e.g. collaborations

on course design and delivery, internships, traineeships, work placements, scholarships).



A study by ENISA found 526 graduate, postgraduate and university-level certification courses across the EU,<sup>434</sup> and a number of organisations have produced rankings of the best cybersecurity courses and educational institutes in different geographic regions.<sup>435</sup>



### **UK Centres of Excellence in Cyber Security Research**

The UK has established Centres of Excellence in Cyber Security Research at 14 universities, with the aim being to:<sup>436</sup>

- Enhance the volume and quality of cybersecurity research;
- Help direct practitioners and users of cybersecurity research to the latest academic work;
- Foster shared aims and collaboration in cybersecurity research.



### **Cyberfirst**

Cyberfirst is a scheme developed by the UK's National Cyber Security Centre (NCSC) that encourages uptake of cybersecurity university degrees through three mechanisms:<sup>437</sup>

- Bursaries of £4,000 per year when studying selected degrees;
- Annual summer placements and/or bespoke training in either industry or government, with a salary of £250 per week;
- Three-year graduate-level cybersecurity roles after graduation.



- Evaluate and modify cybersecurity education and training in consultation with stakeholders from the public and private sectors, academia and civil society; ensure the ongoing delivery and improvement of cyber education and training.

As with many areas of public policy, it is important to evaluate the effectiveness of any cybersecurity educational programme to estimate value for money, identify areas for improvement, and learn from elements that have proved less effective. Appropriate metrics – quantitative, qualitative, or both – should be developed in order to measure performance.

### D3.2 – Framework for cybersecurity education

For example, when evaluating the provision of network and information security training for school teachers, ENISA suggests a number of metrics, including:<sup>438</sup>

- Number of participants
- Qualitative review of training
- Changes in performance of students in tests
- Reduction in recorded cybersecurity incidents in schools, such as fraud or hacking.

As with all evaluations, different metrics and weightings should be applied to activities, outputs, outcomes and impacts of the programme in question.<sup>439</sup> Evaluations should be carried out periodically to assess performance in light of any contextual changes in the cybersecurity domain, or changes made to the programme following an earlier evaluation.

More advanced cybersecurity education programmes are likely to go beyond the capacity-building steps outlined above, and develop more complex mechanisms to ensure that the educational framework is able to adapt to any changes in the cybersecurity threat landscape. These may include, for example, establishing a network of experts and educators from industry, academia, government and education to facilitate effective information transfer. To develop more advanced education programmes, government stakeholders are advised to consider new and novel approaches being applied by different countries, and adapt these provisions to their local context where appropriate.

#### Additional resources



- ENISA. 2012. Collaborative Solutions for Network Information Security in Education. European Network and Information Security Agency, Greece.
- ENISA. 2012. Network Information Security in Education. European Network and Information Security Agency, Greece.
- ENISA. 2013. Brokerage model for NIS in Education. European Network and Information Security Agency, Greece.
- ENISA. 2014. PPPs and their role in NIS Education. European Network and Information Security Agency, Greece.

## D3.3 – Framework for professional training

### Overview

This chapter considers the provision of professional cybersecurity training and education, which is defined here as cybersecurity training provided to individuals who currently work or have formerly worked in a professional environment. It outlines some of the steps and considerations required when developing a professional cybersecurity training programme that meets the requirements of the current and future national cybersecurity workforce.

There is clear overlap between this chapter and the preceding factor in this toolkit, particularly within tertiary education. For example, the provision of tertiary education – through university degrees, vocational courses, apprenticeships, etc. – is not only aimed at students who have recently graduated from secondary education, but also provides opportunities to mid-career professionals who are looking to either progress within their current field of work or transfer into another area.

### Box 3.3: Steps for improving the framework for professional training in cybersecurity-related areas (D3.3)

- Assign a task owner to develop and implement a cybersecurity training programme on a national level.
- Conduct a cybersecurity training needs analysis for different target audiences within the public and the private sectors in order to identify gaps in publicly available cybersecurity training.
- Establish the availability of appropriate cybersecurity training offerings for different target audiences within the public and private sectors.
- Evaluate the availability of appropriate cybersecurity training offerings for cybersecurity professionals and non-cybersecurity professionals and the range of skills development offered.
- Develop specialised training for cybersecurity professionals focusing on required technical and non-technical knowledge, skills and attitudes.
- Ensure appropriate mechanisms are in place for the accreditation of education and training courses delivered to ensure they are aligned with international standards and practices.
- Evaluate the results of provided education and training.
- Evaluate the results of education and training based on the established metrics of effectiveness.

### Capacity-building steps

- Assign a task owner to develop and implement a cybersecurity training programme on a national level.

The first stage in developing and implementing a professional cybersecurity training programme at a national level is assigning a **task owner** within an appropriate government department. The task owner should take the lead in developing and coordinating a national-level programme for professional

### D3.3 – Framework for professional training

cybersecurity skills development, and should work in close collaboration with a range of other stakeholders in designing, implementing and evaluating individual education initiatives. The task owner for professional training and education is often the same as or closely linked to the task owner for primary, secondary and tertiary cybersecurity education (see D3.2 above), although this is not necessarily the case.



#### Professional cybersecurity development in the US

The US DHS is the lead government department for national cybersecurity, which includes professional cybersecurity workforce development.<sup>440</sup> However, a number of other US government departments are closely involved in this area. In particular, this includes the US Department of Commerce, under which sits the Applied Cybersecurity Division<sup>441</sup> as part of the NIST.<sup>442</sup> The DoD also supports professional cybersecurity development,<sup>443</sup> and the Department of Justice is involved in cybersecurity outreach and education.<sup>444</sup>



- Conduct a cybersecurity training needs analysis for different target audiences within the public and the private sectors in order to identify gaps in publicly available cybersecurity training.

Before developing any initiative that seeks to provide education to cybersecurity professionals, it is important to understand who the term ‘cybersecurity professionals’ refers to, as well as evaluate the degree to which the number and skills of cybersecurity professionals meet the demands of the market. In other words, it is important to understand to whom the terms ‘cybersecurity professional’ or the ‘cybersecurity workforce’ apply, and the degree to which this workforce is able to meet the cybersecurity demands of the public and private sectors.

At a general level, the term ‘cybersecurity professionals’ – who are the audience of any professional education initiative – can refer to both technical and non-technical professionals involved in cybersecurity and information security across private, public and not-for-profit organisations. This includes individuals from private cybersecurity firms, ICT providers, private companies that use IT-intensive processes and infrastructure, government departments that design and operate government e-services, national militaries, universities, private and not-for-profit cybersecurity education providers, and others.

A training needs assessment can be carried out at varying levels of granularity, and will differ according to the area of work within the public and private sectors. For example, a study led by RAND Europe for the European Defence Agency in 2013 identified four target audiences within European militaries for cybersecurity training: generalists, cyber defence specialists, C4 personnel and senior military officials. Each of these four target audiences required different levels of education in cyber defence, as well as different types of education and training activities tailored to increasing their levels of proficiency.<sup>445</sup> Conducting an initial mapping and evaluation of the cybersecurity workforce to this degree of granularity across all sectors may not be possible within available resource constraints, and so both the area of focus and degree of granularity may be adjusted accordingly.

A number of frameworks have been published that help break down and evaluate a cybersecurity workforce. In particular, NIST in the US has published a detailed framework that defines high-level and specialist categories within a cybersecurity workforce, and provides recommendations for assessing current capabilities and current and future requirements.<sup>446</sup> This is complemented by examples of US government analyses and evaluations of different elements of the cybersecurity workforce, such as the 2013 Information Technology Workforce Assessment for Cybersecurity (ITWAC), which assessed the US government's cybersecurity workforce composition, capabilities and requirements for further training.<sup>447</sup>



### CyberSeek

CyberSeek is data platform and interactive tool that provides users with an up-to-date and detailed overview of the supply of and demand for professionals and jobs in the cybersecurity sector. It tracks cybersecurity job openings and maps this against the supply of cybersecurity workers according to different categorisations of role, and then presents this information by geographic region and on a national level. The tool is not only aimed at policymakers and government, but also employers, job seekers, current workers, students and educators.<sup>448</sup> The tool was developed by three partners: NICE, which is led by NIST under the US Department of Commerce; the Computing Technology Industry Association, which is a not-for-profit trade association; and Burning Glass Technologies, which is a private job market analytics company.<sup>449</sup>



- Evaluate the availability of appropriate cybersecurity training offerings for different target audiences within the public and private sectors.

The next stage in developing a national professional cybersecurity education programme is to understand and map both the stakeholders involved in professional cybersecurity education provision, and the existing range and quality of available cybersecurity training. In other words, having evaluated the composition and the needs of the existing cybersecurity workforce (in the previous step), it is then important to assess the degree to which these needs can be met by the existing education provision. This is recommended even in instances when no publicly funded or publicly provided cybersecurity training has previously been offered, as it is possible that other sectors – specifically the private sector, universities and not-for-profit organisations – may have already been providing some form of professional education and development programmes.

## D3.3 – Framework for professional training

**International private cybersecurity training courses**

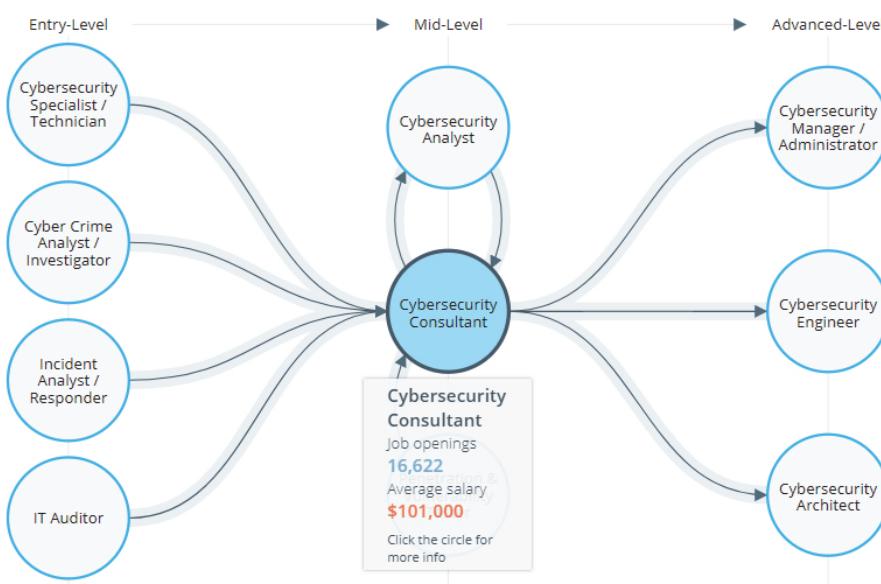
A number of multinational private sector companies provide accredited cybersecurity education courses throughout the world. For example, the **SANS Institute** provides a number of different types of training events, private training courses and online training to companies, government agencies and global enterprises. Courses are offered in areas including cyber defence, cyber penetration testing, digital forensics and cybersecurity management. Professionals are also able to obtain Global Information Assurance Certifications on completion of their courses.<sup>450</sup> The **International Council of E-Commerce Consultants**, also known as EC-Council, is a second example of an international private sector cybersecurity training body. The EC-Council operates in 145 countries, and offers courses and certification in areas such as Certified Ethical Hacker, Computer Hacking Forensics Investigator, Certified Security Analyst, License Penetration Testing (Practical) and others. By the end of 2017, EC-Council had trained and certified over 200,000 information security professionals, and their courses have been integrated into a number of different public sector career programmes, including the US National Security Agency and DoD, and the Malaysian Military Cyber Security Warfare Department.<sup>451</sup>

By comparing existing training requirements and current and future workforce needs against the available professional education, it is then possible to identify gaps in provision and areas of focus for government-supported professional cybersecurity training. This type of analysis may also help identify possible areas for collaboration and partnership, which may in turn enable a government to use, support and improve – as opposed to duplicate or ignore – the existing provision of cybersecurity training and education across different sectors.



- Develop specialised training for cybersecurity professionals, focusing on required technical and non-technical knowledge, skills and attitudes.

Having conducted a gap analysis of existing education programmes, the next stage is to decide on the *type* of education to be provided by the government, and design the mechanisms and platforms through which this education will be provided. According to results of the initial mapping exercises, the delivery of professional cybersecurity education may be tailored to cover technical cybersecurity areas (including computer science skills development), non-technical elements (including management and policy) and communication (including skills for communicating technical issues to non-technical audiences). Figure 3.2 below presents a visual example of a cybersecurity career path framework for professionals in this field.

**Figure 3.2: A visual framework of cybersecurity career paths**

SOURCE: CyberSeek (N.d.)

Depending on the local context, the government has the option to:

- Provide professional cyber education to the target audience;
- Provide direct support to cybersecurity education delivered by other stakeholders;
- Provide indirect support to new and existing professional cyber education programmes through standardisation and accreditation, educational resources, and facilitation of professional networks.

Expanding on these points in turn, a national government may provide internal (i.e. to government employees) and external cybersecurity training by setting up and running its own cyber training programme. This may be achieved, for example, by establishing a standalone training centre that offers training programmes to cybersecurity professionals.



If available resources and budgets are limited, this option may be difficult for some governments to implement due to the initial investment in resources and expertise required to establish and run a professional cyber education course.

Government-provided courses may be particularly appropriate in specific cases, such as training internal government employees on areas that are sensitive for national security reasons.

## D3.3 – Framework for professional training

**NATO Cooperative Cyber Defence Centre of Excellence**

Although not developed by one country alone, the NATO CCDCOE is an example of a government-provided initiative which includes professional-level cybersecurity training. For example, the CCDCOE delivers a five-day residential course twice per year for military cybersecurity professionals, and the curriculum includes an overview of the current status of international cyber affairs, an introduction to emerging technical aspects of cybersecurity, and more in-depth sessions on the peacetime international law that governs cyber operations, and the international humanitarian law that applies during armed conflicts that involve cyber operations.<sup>452</sup>

Providing funding and support to private sector or non-governmental organisations is a second option for establishing and increasing the number of available cybersecurity training programmes. This may include providing funding and support to universities when developing cybersecurity Master's programmes and vocational courses, or partnering with selected private or not-for-profit organisations who assist the government by providing substantive expertise, methodological experience or tailored cybersecurity training resources.

**Cybersecurity Training Lab at The Fraunhofer Academy**

The Cybersecurity Training Lab was developed by The Fraunhofer Academy and a number of collaborating universities to provide modular, part-time study programmes for cybersecurity managers and industry professionals. By 2017, 19 different Fraunhofer research institutions provided specialist cybersecurity training courses on areas ranging from industrial manufacturing cybersecurity and critical infrastructure protection to software quality assurance and the security of embedded network systems. These training courses are situated within active research institutions to allow theoretical and practical research findings to be incorporated more quickly into teaching programmes.<sup>453</sup> The Fraunhofer Academy is part of the Fraunhofer-Gesellschaft, which is a not-for-profit research organisation with 69 institutes and research units across Germany that focus on applied (as opposed to basic) scientific research.<sup>454</sup> During the first few years of operation, the Cybersecurity Training Lab received six million euros of funding per year from the German Ministry of Education and Research.<sup>455</sup>



It can be difficult to know which vendors are capable of providing cybersecurity education to a sufficiently high standard. Evaluation and accreditation of external education providers and professional training courses is therefore important in ensuring confidence and quality in the system.<sup>456</sup>

A government may also provide indirect support to cybersecurity professional education through a number of different mechanisms and platforms. This is often achieved through the development of an accreditation framework, both for practitioners and education providers, and the provision of open-source resources that provide guidance and tools for cybersecurity employers and employees.

### D3.3 – Framework for professional training

Establishing an accreditation framework is one way in which a government can seek to ensure that cybersecurity professional training is provided to a high standard. Accreditation is the process whereby an external organisation is assessed according to a set of standards – in this instance developed by a government – which outline the requirements for receiving formal recognition of the quality of cybersecurity training and education courses.<sup>457</sup> The development of an accreditation framework begins with the development a set of standards that should be achieved in order for an organisation to receive accreditation. Once these standards have been developed, a system should be put in place that allows organisations to demonstrate compliance with these standards.<sup>458</sup>

An accreditation framework not only ensures quality and consistent cybersecurity training, but also helps to build confidence in the cybersecurity sector. For both employers and employees, it ensures that a selected training course will increase an employee's skill level to a required, known and common standard. This assists employers in hiring sufficiently skilled cybersecurity specialists, and in enabling employees to build, confirm and communicate their skill level. Cybersecurity standards and accreditation can also help build cooperation across businesses and across sectors, both on a national and an international level.



International organisations, such as the EU together with ENISA, are currently developing international cybersecurity standards in an attempt to further increase international cybersecurity cooperation.<sup>459</sup>



#### GCHQ-certified training and APMG-International

The National Cyber Security Centre in the UK – which is part of GCHQ – provides certification for two levels of cybersecurity training courses:

- Awareness-level, which provides beginners with a thorough foundation in cybersecurity;
- Application-level, which provides in-depth courses for professional development.

GCHQ certification is awarded to cybersecurity training courses that meet a set of standards and assessment criteria developed and written by GCHQ. These courses may be provided by the public, private or not-for-profit sectors.<sup>460</sup>

The accreditation process itself is carried out by **APMG-International**, as opposed to GCHQ. APMG-International is a private sector organisation providing accreditation of professional training and consulting organisations in cybersecurity and resilience. By partnering with APMG-International, the accreditation programme benefits from APMG-International's assessment procedure, quality control processes, alignment of programmes with international standards and practices, and international recognition.<sup>461</sup>

A national government may also provide free-to-access resources and material to assist businesses and cybersecurity professionals in improving their own cybersecurity capabilities. For employers, this may include information and online tools that help structure their cybersecurity workforces,<sup>462</sup> information on accredited cybersecurity courses and qualifications for their employees, guidance on developing and

### D3.3 – Framework for professional training

implementing cybersecurity ranges,<sup>463</sup> and training resources that allow organisations to deliver their own internal cybersecurity courses.<sup>464</sup> For cybersecurity employees and individual professionals, a government information portal may provide resources that assist in understanding cybersecurity career paths and in finding appropriate cybersecurity training courses, and may also provide educational material that allows individuals to improve their skills and knowledge in their own time.<sup>465</sup>



#### National Initiative for Cybersecurity Careers and Studies (NICCS)

The National Initiative for Cybersecurity Careers and Studies (NICCS), run by the US DHS, is an online platform that provides cybersecurity education resources that target both professional organisations and individual cybersecurity employees. For cybersecurity employees, the platform provides a comprehensive guide to and catalogue of available professional cybersecurity training in the US, and also offers a free online training tool for government employees and veterans wishing to start or develop a degree in cybersecurity (the Federal Virtual Training Environment, or FVTE). For employers, NICCS offers a Cybersecurity Workforce Development Toolkit, which provides organisations with information, tools and planning templates to help organisations build and develop their cybersecurity workforces.<sup>466</sup> There is also a PushButtonPD™ Tool, which is targeted at Human Resource Managers in government, and a page for requesting technical assistance on cybersecurity workforce development from the DHS.



#### MOOCs

MOOCs, or Massive Open Online Courses, are online courses delivered via tailored online platforms that provide training and education to students and professionals. MOOCs are often delivered by elite universities from Europe and the US and promise top-level education,<sup>467</sup> and they often include recorded lectures, supplementary information, worksheets, small tasks, and sometimes formal accreditation. MOOCs are often free and open to access, although a fee is often charged if the course provides formal assessment and accreditation on completion. It has also been observed that MOOCs often experience high levels of enrolment coupled with a low level of completion.<sup>468</sup> There are a wide range of MOOCs available across a number of platforms, including edX, Coursera, FutureLearn, Udacity, OpenUpEd, iversity and Canvas Network. These include courses in cybersecurity and network and information security.<sup>469</sup>



- Evaluate the results of education and training based on the established metrics of effectiveness.

The design and implementation of any education initiative should be supported by a subsequent evaluation, the results of which should be used to inform and refine future training and education provision. This should be carried out using appropriate metrics that measure activities, outputs, outcomes and results, and any evaluation should also produce actionable recommendations to inform the development and refinement of future programmes.



Evaluation of activities and outputs is typically easier than an evaluation of outcomes or results. Activities and outcomes are often simple to measure, for example by measuring the number of training courses offered, the number of public-private partnerships or the number of professionals that have completed a cybersecurity training course. Measuring outcomes and results is more difficult, since it requires mapping and measurement of particular training initiatives to improve cybersecurity capabilities. This involves the use of more advanced metrics and evaluation methods.<sup>470</sup>



Where possible, the metrics for evaluation should be published openly in order to ensure confidence and transparency in the evaluation process, particularly when evaluating external providers of professional education.<sup>471</sup>



- Establish a dynamic process of development, implementation and review.

The fast-changing nature of cybersecurity means that workforces must be adaptable and responsive to the emerging technologies, threats and trends. It is therefore important that any professional cybersecurity education programme is not static in its development and implementation. Maintaining an effective evaluation cycle is an important element in ensuring this, but there are other initiatives that may be implemented to help facilitate a dynamic process.

In particular, establishing a network of experts across sectors can facilitate knowledge transfer between research, industry and government. If the government is able to establish partnerships and relationships with stakeholders across the cybersecurity domain, then this network can be used to help adapt training and education content according to new developments and emerging trends.



#### CAE Community Portal

The CAE Community Portal is a web-powered platform that aims to facilitate the exchange of relevant information, ideas and events between CAE (Centers of Academic Excellence in Cyber Security) institutions. CAE institutions are designated academic institutions in the US that have passed an in-depth assessment for their provision of cybersecurity education and research. The CAE Community Portal provides a single point for resources, news, events and online forums for discussion.<sup>472</sup>

It is also important to ensure that sufficient financial resources are assigned to cybersecurity and cybersecurity education, and that the budget allocation for cybersecurity is sufficiently agile to react to emerging changes in requirements. Although all government departments and initiatives are resource-constrained, it is important to ensure that funding and resources are able to support dynamic training programmes that meet the increasing and changing demands of cyberspace.

## D3.3 – Framework for professional training

**US cybersecurity budget increases**

The US recognised that in order to implement the required cybersecurity initiatives, it had to invest additional resources in the field. The 2017 'Budget allocates more than US\$19 billion for cybersecurity – a more than 35% increase over the 2016 enacted level. These resources will enable agencies to raise their level of cybersecurity, help private sector organisations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents.'<sup>473</sup>

## Additional resources



- National Institute For Cybersecurity Education (NICE). 2013. 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC): Summary Report. Department of Homeland Security and CIO Council.
- Newhouse, William, Stephanie Keith, Benjamin Scribner & Greg Witte. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181).
- US Department of Homeland Security. n.d. Cybersecurity Workforce Development Toolkit: How to Build a Strong Cybersecurity Workforce. Department of Homeland Security.
- Wilson, Mark. & Joan Hash. 2003. Building an information technology security awareness and training program (NIST Special Publication 800-50). National Institute of Standards and Technology.

## **Dimension 4**

### **Legal and regulatory frameworks**



## Dimension 4 – Legal and regulatory frameworks

---

Dimension 4 of the GSCC CMM looks at a government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, including for issues pertaining to cybercrime, privacy and data protection.

This dimension of the GSCC CMM comprises three factors. The following sections discuss capacity-building steps that national decision makers may implement to build capacity across these issue areas, which are:

### **1. D4.1 – Legal frameworks**

This factor focuses on legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks, privacy, freedom of speech, human rights online, data protection, child protection, consumer protection, intellectual property, and substantive and procedural cybercrime legislation.

### **2. D4.2 – Criminal justice system**

This factor focuses on national capacity to tackle cyber-enabled crimes, including the capacity of law enforcement agencies to investigate cybercrime, the capacity of prosecution services to pursue cyber-enabled crime and use electronic evidence, and the capacity of courts to preside over cybercrime cases and cases involving electronic evidence.

### **3. D4.3 – Formal and informal cooperation frameworks to combat cybercrime**

This factor focuses on national capacity to ensure formal and informal cooperation among domestic actors and with relevant counterparts from outside the country to deter and combat cyber-enabled crime.

## D4.1 – Legal frameworks

### Overview

A legal framework is a set of rules that governs the rights and obligations of government, companies and citizens. It encompasses national legislation, policy, regulations, contracts and – where applicable – a country's constitution.<sup>474</sup>

During the 1990s and the early development of the Internet, it was unclear whether additional legislation specific to cybersecurity was required.<sup>475</sup> Cyber security, it was argued, was simply another specialised case of general rules and legal principles already governed by existing legislation, meaning that additional cybersecurity-specific legal frameworks would not be required.<sup>476</sup> However, experience from the last two decades has demonstrated that while cybersecurity has not developed into a core, independent legal area, it is nonetheless essential on a national and international level to develop distinct legal frameworks that govern the behaviours, processes and actions that arise in cyberspace.<sup>477</sup>

Broadly speaking, legal frameworks in cybersecurity are developed in the context of either criminal law or the law of armed conflict.<sup>478</sup> This factor focuses on the development of legal frameworks within the criminal domain, with a specific focus on cybercrime. In particular, it considers the ways in which legal frameworks are developed to support the detection, investigation and prosecution of cybercrime, while also safeguarding due process, privacy rights and individual freedom of speech. This section does not consider the use of cyberspace within a military context, which is discussed in brief in the D1.5 section of this document.

A criminal law approach seeks to protect citizens, companies and governments from unjust or harmful activity. In cyberspace, this refers to a range of activities including illegal access to computer systems, illegal acquisition or interception of computer data, illegal interference with computer systems or data, fraud, forgery, spamming, copyright and trademark offences, and child pornography offences.<sup>479</sup> The development of an effective cybercrime legal framework is an important factor in countering these types of activities, as it provides the legal basis for investigation, prosecution and punishment of harmful or unjust behaviour in cyberspace.<sup>480</sup> Without a clear legal basis, it can be difficult or impossible to carry out these functions, which in turn places significant limitations on a country's ability to effectively secure cyberspace.<sup>481</sup>

As is the case with many of the issues and challenges falling under cybersecurity capacity building, there is no one-size-fits-all approach to developing an effective legislative framework, but a number of steps can be taken to help improve a country's legal system. Box 4.1 provides an overview of these capacity-building steps, which are presented in greater detail in the following pages.

**Box 4.1: Steps for developing legal frameworks' capacity to tackle cyber-enabled crimes (D4.1)**

- Develop substantive and procedural law that can be applied to cases of cybercrime.
- Ratify regional and international instruments on cybercrime and seek to implement measures contained in these instruments within domestic law.
- Review substantive and procedural law, and ensure processes exist for updating legislation when required.

*Capacity-building steps*


- Develop substantive and procedural law that can be applied to cases of cybercrime.

When developing national legislation, it is useful to differentiate between different types of law, including **substantive law**, **procedural law<sup>482</sup>** and **jurisdictional law**.



**Substantive law** is a set of rules that define particular activities as illegal. In the case of cybercrime, this refers to activities such as unauthorised access to and interference with computer systems, access to and communication of illegal content such as child pornography and hate speech, and computer-related offences such as online fraud and identity theft.<sup>483</sup>

**Procedural law** refers to the set of rules that govern the way in which the criminal justice system – including law enforcement, prosecution and the courts – is able to identify, investigate and prosecute an individual who has committed a criminal act.<sup>484</sup> Procedural law defines the power that lies with authority,<sup>485</sup> and covers areas including search and seizure procedures and cooperation with third parties.<sup>486</sup>

**Jurisdictional law** defines the set of rules that govern jurisdiction, which is the way in which the power to enforce substantive and procedural law extends across international borders.<sup>487</sup> Jurisdictional law is based on principles of territoriality, nationality, protection and universality.<sup>488</sup>

Beginning with **substantive law**, it is first useful to understand the degree to which existing legislation covers cases of cybercrime. Many activities defined as cybercrime – such as online fraud, identity theft and hate speech – are not new forms of crime, but rather constitute manifestations of more traditional criminal activity carried out on new, digital platforms. In some instances, existing criminal legislation may be sufficient to define and prosecute cases of cybercrime without any adaptation or extension to existing legal frameworks.<sup>489</sup>

In other instances, however, it may be apparent that existing law is insufficient in defining new forms of cybercriminal activity. In such cases, the process of updating substantive law begins with the recognition

## D4.1 – Legal frameworks

of an abuse of new technology, or a new abuse of existing technology, and the identification of a gap in the penal code. New legislation must then be drafted to cover this gap.<sup>490</sup>



### Dilemmas in drafting substantive law

A number of **dilemmas** exist when drafting substantive cybercrime laws. In particular, legislators must decide whether to extend existing laws to cover new forms of cybercrime, or introduce new cyber-specific laws into the national legal framework.<sup>491</sup> Legislators must also balance the degree to which new laws are specific or general, with the former allowing the criminalisation of particular crimes, and the latter facilitating greater resilience against future developments and uses of technology.<sup>492</sup> Finally, legislators must balance the severity of substantive law against human rights and civil liberties, and introduce sufficient safeguards to protect, for example, freedom of speech and freedom of access to the Internet.<sup>493</sup>

When developing substantive legislation for cybercrime, it may be beneficial to first review existing international standards and legislation in this area to reduce duplication of effort and ensure that legislation being developed is harmonised with international standards.<sup>494</sup> This may be achieved through bilateral or multilateral engagement with other countries, or through engagement with international cybercrime legislation and initiatives, such as various resolutions outlined by the United Nations General Assembly and United Nations Office on Drugs and Crime,<sup>495</sup> or the Budapest Convention developed by the Council of Europe. Moreover, various support documents and toolkits have been developed by international organisations to assist countries in adapting substantive law, including the World Bank's *Combatting Cybercrime* toolkit, which provides a comprehensive overview of legal frameworks and capacity-building steps,<sup>496</sup> and the *ITU Toolkit for Cybercrime Legislation*, which provides sample legislative drafts that may be adapted for particular national contexts.<sup>497</sup>

In addition to substantive law, **procedural law** must also be adapted to enable the criminal justice system to detect, investigate and prosecute cases of cybercrime in a fair and effective manner. In the case of cybercrime, procedural law focuses primarily on **digital evidence**, and defines the laws governing search and seizure procedures, and the way in which digital evidence can be stored, accessed and analysed so that it is admissible in court.



Developing procedural law is typically more difficult than substantive law due to the high level of detail required in administrative proceedings, coupled with the challenge of ensuring that legislation covers new technologies and methods in digital forensics.<sup>498</sup>



### Procedural law and cloud computing

The development of **cloud computing** has created significant challenges in developing procedural and jurisdictional law. Focusing on the former, the decentralisation of data in cloud storage removes the traditional concept of search and seizure. It removes ‘a location for evidence to be seized’, as fragmentations and copies of evidence exist across multiple servers in multiple jurisdictions. This is compounded by techniques such as ‘virtualisation’, whereby virtual computer resources are created by combining physical hardware that may be located in multiple locations. Designing procedural law that allows law enforcement to search and collect evidence from cloud computing is particularly challenging, and typically relies on cooperating with ISPs who control the cloud storage mechanism, as well as developing specific legal procedures for different forms of digital evidence that may be stored on the cloud.<sup>499</sup>

As the previous example demonstrates, developing laws that facilitate cooperation with third parties, such as ISPs, is an important element of procedural law in cybercrime, as a substantial amount of network infrastructure is owned and maintained by the private sector. Procedural law should clearly define the types of information that may be required, the processes for requesting this information from third parties, and the mechanisms that may be used to compel third parties to provide this information when requested.<sup>500</sup>

Finally, it is also important to develop and adapt **jurisdictional law**, which governs the way in which law enforcement and the criminal justice system can exert and enforce legislative power across different jurisdictions. Traditionally, jurisdiction has been defined by nation states and the sovereign control of territory, and has included jurisdiction over the crime itself, the evidence and the perpetrator.<sup>501</sup> The cross-border nature of cybercrime, however, has led to the development of several adaptations to this traditional notion of nation state jurisdiction, including adaptations of territoriality, active nationality, passive nationality, protection and universality.<sup>502</sup>

A number of different approaches may be taken to enable nation states to manage the jurisdictional complications that arise through international cybercrime, including:<sup>503</sup>

- Adapting existing legislation to include new principles of jurisdiction (territoriality, active nationality, passive nationality, protection and universality);
- Addressing questions of jurisdiction on a case-by-case basis according to existing legislation;
- Developing formal and informal jurisdiction arrangements with other countries;
- Engaging in regional and international cooperation agreements on cybercrime, many of which include considerations of jurisdiction.

#### D4.1 – Legal frameworks



- Ratify regional and international instruments on cybercrime and seek to implement measures contained in these instruments within domestic law.

Information and telecommunication systems enable high-speed connection and communication around the world. While this has created numerous benefits for global society, it also enables cybercriminal activity to occur with relative ease across national borders. Unlike more traditional types of crime that occur in a single, real-world location, the perpetrators, victims, computer infrastructure, digital information and software involved in a single cybercrime incident may all be located in different countries that fall under different legal jurisdictions.

When developing national-level legislation for cybersecurity, it is therefore important to consider the international aspects of cybercrime, and where possible incorporate these considerations into national legislation. This can be achieved in a number of different ways, including formal cyber-specific multilateral treaties and initiatives, formal (yet more general) mutual legal assistance treaties (MLATs) and extradition treaties, and through informal collaboration mechanisms such as developing professional networks and standardising information-sharing procedures.<sup>504</sup>

Countries are largely free to decide which international treaties to join, although legal commitments often become mandatory on joining these treaties, and some treaties within international law are largely unavoidable.<sup>505</sup> Engagement in international organisations and treaties is often a political decision, but it can have a number of benefits for countries, such as providing a framework and support for the development of national-level legislation, communicating a statement of intent to internal stakeholders and other states, supporting harmonisation of legislative frameworks across borders, and improving interoperability between states when tackling instances of cybercriminal activity.<sup>506</sup>



There are a number of important **multilateral treaties on cybercrime**, including the Budapest Convention, the Arab Convention, the Commonwealth of Independent States Agreement, and the Shanghai Cooperation Organisation Agreement. Although different in their exact construction, these multilateral treaties generally attempt to increase international cooperation and harmonisation through mechanisms including the standardisation of substantive and procedural law, the development of common cybercrime policies, and formal agreements regarding jurisdictional and international cooperation issues.<sup>507</sup> In addition, there are a number of different **international organisations** that support and facilitate the growth of international cooperation, including the International Court of Justice, the International Law Commission, the ITU Global Cybersecurity Agenda, the United Nations Group of Governmental Experts on Information Security, the Council of Europe Convention on Cybercrime, and the EU's Ministry of Justice.<sup>508</sup>



- Review substantive and procedural law, and ensure processes exist for updating legislation when required.

There are a number of difficulties in drafting and maintaining legislation in the field of cybersecurity. In particular, it is difficult to ensure that legislation is able to keep up with the speed of contemporary technological development, which includes both new types and ways of carrying out cybercriminal activity, and new methods for law enforcement to detect and investigate instances of cybercrime. It is inevitable that delays will exist between the development of new technologies and the drafting of appropriate security legislation that provides sufficient legal support to the criminal justice system while also maintaining an appropriate balance between security and individual rights.<sup>509</sup>



There is an important **trade-off between legal regulations, human rights and civil liberties**. Legal regulations should be sufficiently rigorous in providing security and confidence to a system, but equally, if they are too overbearing then they can restrict innovation and growth, and over-criminalise low-level behaviour in a way that is ultimately counterproductive. Legal systems should also ensure due process is observed at all times, and that privacy, personal data and freedom of expression are safeguarded in a reasoned and balanced manner.<sup>510</sup> There are ways of reducing the prevalence of this trade-off by, for example, constructing legislation that differentiates between different sectors and actors, and allowing designated organisations more flexibility where appropriate.<sup>511</sup>

One way of mitigating some of these difficulties is to develop legislation that is more general in nature, which in turn provides greater flexibility of interpretation when applied to new technologies. This is a form of *future-proofing* that seeks to ensure existing law can be applied to an unpredictable future, although the inevitable cost of such an approach is a loss of granularity and specificity within the legal system itself.<sup>512</sup>

It is also important that procedures are in place to allow both substantive and procedural law to be updated when required.<sup>513</sup> The process through which laws are changed varies according to individual countries, and an assessment should be made on a case-by-case basis to decide whether existing processes for updating national legislation are sufficient when dealing with cybercrime.



#### Cybercrime legislation in the UK

In the last 30 years, the UK government has introduced a series of legal acts that tackle new and emerging types of cybercrime. This includes the Computer Misuse Act (1990), the Data Protection Act (1998), the Regulation of Investigatory Powers Act (2000), the Communications Act (2003), the Fraud Act (2006), the Video Recordings Act (2010) and the Criminal Justice and Courts Act (2015).<sup>514</sup> For new laws to be passed in the UK, a proposal must be made by the incumbent government, which must then be passed by parliament following several parliamentary stages.<sup>515</sup>

## D4.1 – Legal frameworks

### Additional resources



- ITU. 2011. ITU Toolkit For Cybercrime Legislation. Geneva, Switzerland: International Telecommunication Union.
- ITU. 2011. Understanding Cybercrime: A Guide For Developing Countries. Geneva, Switzerland: International Telecommunication Union.
- ITU. 2012. HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts. Geneva, Switzerland: International Telecommunication Union.
- World Bank. 2016. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 GO).

## D4.2 – Criminal justice system

### Overview

The criminal justice system is the mechanism through which a crime is identified and the perpetrator prosecuted and sentenced within an existing legislative framework. More specifically, the criminal justice system encompasses detection of criminal activity, identification of suspects, gathering of evidence, presentation of a prosecution in court, determination of guilt and, where required, application of an appropriate sentence. This is typically carried out through three separate functions: law enforcement, prosecution and the courts.<sup>516</sup> In general terms, **law enforcement** is primarily concerned with disrupting ongoing criminal activity, and responding to instances of crime through the identification and detention of suspects, and the gathering of evidence to be used in court. It is the role of the **prosecutor** to determine whether the evidence collected by law enforcement is sufficiently rigorous to warrant a court case, and if so, to present this evidence in court with the aim of achieving a conviction. Finally, it is the role of the **courts** – specifically judges, magistrates and justices of the peace – to assess the case presented by the prosecution and the defence, and, together with a jury, decide on guilt, sentencing, appeals, bail and the protection of the rights of the defendant.<sup>517</sup> Although there are variations between national criminal justice systems, this approximate structure and delineation of tasks is widely applicable not only to general cases of crime, but also specifically to **cybercrime**.

The precise definition of cybercrime varies between countries, organisations and academia, with disagreements arising due to differences in the scope, specificity, context and role of a definition.<sup>518</sup> In particular, cybercrime can be defined using either a narrow understanding, where the term *cybercrime* is restricted to sophisticated attacks against software or hardware, or in a broader sense, where cybercrime includes traditional crimes that are committed through the use of ICT.<sup>519</sup> In this section, a broader definition is applied, with cybercrime understood as ‘any crime that is facilitated or committed using a computer, network or hardware device’ where a ‘computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime.’<sup>520</sup>

Cybercrime not only refers to traditional crimes such as fraud and identity theft that are carried out on a new technology platforms, but also the development of new types of crime that only exist on computer and network systems. This includes a range of different types of criminal activity, including: offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access, illegal data acquisition and systems interference; content-related offences, such as child pornography, online hate speech and the distribution of libel information; copyright- and trademark-related offences; computer-related offences, such as fraud, forgery and identity theft; and combination offences, such as cyberterrorism, cyber-laundering and phishing.<sup>521</sup>

Cybercrime has existed in some form since at least the 1960s and the introduction of transistor-based computer systems,<sup>522</sup> although in recent years the variety, frequency and impact of cybercrime has increased considerably. This is due in part to an increased use of and reliance on computer and network systems across industry, government and the general public, as well as the increased availability of cheaper and more powerful hardware and software such as encryption technology, online anonymisation platforms and systems that enable automated cyber-attacks.<sup>523</sup>

## D4.2 - Criminal justice system

Tackling cybercrime through an effective criminal justice system is an important element in maintaining the security and functioning of information and communication technologies, and maintaining trust in the institutions and platforms that rely on these systems.<sup>524</sup> Tackling cybercrime, however, poses a number of unique challenges for law enforcement, prosecutors and the courts that are not encountered when dealing with more traditional forms of criminal activity. In particular, the use of technology to facilitate, transform and create new types of criminal activity requires additional legislation, new types and methods of processing evidence, new methods of investigation, and new considerations when presenting and deciding on cybercrime cases in court. This is further compounded by the rapid pace of technological development that enables cybercrime, and the geographical detachment between the perpetrator(s) and victim(s) of a cyber-attack, who may be located in different countries that fall under different jurisdictions and legal frameworks.<sup>525</sup>

In spite of these difficulties, it is possible for a country to improve the effectiveness of its criminal justice system in tackling cybercrime. The following section outlines a series of steps that may be taken to enable an existing criminal justice system to tackle cybercrime in a more effective manner, although it should be noted that these steps do not consider the role of cybercrime legal frameworks, which is covered in D4.1 above, nor the value of formal and informal cooperation, which is discussed in D4.3 below.

### **Box 4.2: Steps for developing a criminal justice system's capacity to tackle cyber-enabled crimes (D4.2)**

- Assign a task owner and develop a cybercrime strategy.
- Establish institutional capacity in law enforcement agencies to investigate cybercrime cases and preserve digital evidence for court proceedings.
- Establish institutional capacity in prosecution and court services so that they are able to deal with cases of cybercrime.
- Collect and analyse data and trends on cybercrime and the criminal justice system.
- Establish specialised cybercrime units within law enforcement agencies.
- Implement a process for continued improvement.

#### *Capacity-building steps*



- Assign a task owner and develop a cybercrime strategy.

Assigning a national-level cybercrime task owner is an important initial step in developing cybercrime capabilities within the criminal justice system. It is the role of the task owner to develop the overall strategic direction with regards to countering cybercrime, and coordinate the implementation of this strategy across the different elements of the criminal justice system. Cybercrime and the criminal justice system cover multiple different functions of government, including cybersecurity, law enforcement and the judicial system. A government department that interacts with each of these areas may be best placed to become the overarching cybercrime task owner.<sup>526</sup>



### UK cybercrime strategy and organisation

In the UK, overall ownership of cybercrime is held by the Home Office,<sup>527</sup> which is the government department that oversees immigration, law enforcement and domestic security.<sup>528</sup> The Home Office works in close collaboration with a number of other government departments in countering cybercrime, including the Cabinet Office, which is also responsible for the National Cyber Security Strategy;<sup>529</sup> the National Crime Agency, which is the lead government department for cybercrime law enforcement;<sup>530</sup> and the Ministry of Justice, which is the lead government department for substantive and procedural legislation, and the administration of the courts system.<sup>531</sup> Strategic direction for combatting cybercrime has been outlined in a standalone strategy – comprising the Home Office's 2010 *Cyber Crime Strategy*<sup>532</sup> and 2013 *Serious and Organised Crime Strategy*<sup>533</sup> – which is supported by the Cabinet Office's *National Cyber Security Strategy*<sup>534</sup> and the Ministry of Justice's strategy for *Transforming the Criminal Justice System*.<sup>535</sup>

A strategy for combatting cybercrime should outline the aims and ways in which the institutional capacity (including technical and human capacity, infrastructure, training, funding, and processes of improvement) can be increased to enable law enforcement to better detect and respond to cybercrime incidents.<sup>536</sup> A cybercrime strategy may form a standalone document, or be incorporated into broader cybersecurity or serious crime strategies.<sup>537</sup> Given the range and complexity of the topic, it is likely that the overarching task owner will need to work closely with and distribute responsibilities to other, more specialist government departments, such as those that govern law enforcement or the legal system.



### Cybercrime assessment tools

Before developing a national-level cybercrime strategy, it is advised that a country carries out an assessment of existing threats, and evaluates the existing capabilities of the criminal justice system. A number of tools have been developed to assist this assessment, including examples from the EU, the ITU, the United Nations and the World Bank. These resources are listed at the end of this section.<sup>538</sup>



- Establish institutional capacity in law enforcement agencies to investigate cybercrime cases and preserve digital evidence for court proceedings.

As described in the introduction to this section, law enforcement agencies are involved in both the detection of criminal activity and the response to crimes that have already occurred. When applied to cybercrime, this translates to the **detection** of cybercrime and the development of **digital forensic** capabilities that allow digital evidence to be obtained, stored and analysed in a manner that maintains its authenticity, integrity and reliability.<sup>539</sup>

## D4.2 - Criminal justice system

Beginning with cybercrime **detection**, instances of cybercrime may be reported by victims (including individuals, companies and ISPs) and by CSIRTs, although independent police methods may also be used to uncover criminal activity.<sup>540</sup> To increase the rate and quality of reporting, a centralised reporting tool may be set up which enables victims to communicate instances of cybercrime directly to law enforcement. A broader discussion of reporting mechanisms, their purposes and ways in which they can be established is included in **Section D2.4** of this document.

A number of active detection techniques and systems may also be implemented and assist law enforcement agencies in identifying instances of cybercrime. These include tripwires, configuration-checking tools, honey pots, anomaly-detection systems and operating system commands.<sup>541</sup>



When implementing intrusive detection techniques, it is important to consider the implications for **personal privacy, human rights and civil liberties**, as well as conforming to national and international legislation. To preserve these rights and maintain trust and integrity in the criminal justice system, it is important that any security measures are balanced against individual and collective protections.<sup>542</sup>

In addition to detecting crime, it is also important for law enforcement agencies to develop **digital forensics** capabilities that allow officers to obtain, store and analyse **digital evidence** in a manner that maintains its authenticity, integrity and reliability.<sup>543</sup>



The term **digital evidence** refers to any form of information that is stored in binary units, and that is accessible via computational software or a specific piece of code.<sup>544</sup> This includes digital photographs, spreadsheets, website pages, email messages, intercepted mobile phone calls, operating system event logs, and a large number of other digital formats. In contrast to traditional sources of evidence, digital evidence does not exist in the physical world, but instead is stored and accessed through digital devices including computers, smart phones, WiFi routers and smart devices.<sup>545</sup> It is independent from hardware, which in turn introduces an inherent fragility into digital evidence as it may be copied, edited and erased on any number of compatible hardware devices.<sup>546</sup>



**Digital forensics** is 'the process by which information is extracted from data storage media, rendered into a useable form, and processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings.'<sup>547</sup> In other words, digital forensics refers to the way in which data is recovered, analysed and presented within the criminal justice system.<sup>548</sup> In the recovery stage, digital evidence is typically recovered by creating a forensic image, which is a digital copy of a hard disk (or partition of a hard disk) that may be analysed and used as evidence in court.<sup>549</sup> The analysis stage includes mounting this forensic image onto local hardware, reducing the search space, and searching for relevant digital evidence within the image, including deleted data.<sup>550</sup> This should recorded within a **chain of custody** (see below) so that the evidence can be presented and accepted in court.<sup>551</sup>

Digital forensic capabilities are important both in the initial search and seizure of digital evidence by **frontline officers**, and in the subsequent analysis and presentation of evidence in court by **digital forensics specialists**.

Beginning with the first of these two areas, digital forensic techniques should be carried out by **frontline officers** to ensure that digital evidence is obtained in a manner that is compliant with procedural law, and that ensures the authenticity, integrity and reliability of the digital information. As discussed in Section D4.1 above, procedural law for search and seizure processes is often adapted for cases of cybercrime, and in some instances may not permit the removal of physical evidence (i.e. hardware) from a crime scene.<sup>552</sup> Frontline officers may therefore be required to copy data from hardware onto external storage devices at a crime scene.<sup>553</sup> This should be completed in compliance with procedural law, and in a manner that enables further forensic analysis and future presentation as evidence in court.



A failure to collect evidence from a crime scene according to procedural law can render the evidence inadmissible in court. Frontline officers therefore play an important role in ensuring that digital evidence can be used throughout the remainder of the criminal justice system.<sup>554</sup>



Digital evidence is not only collected at the physical crime scene, but also through remote digital forensics methods, and through close **collaboration with third parties** including ISPs. This may involve voluntary or involuntary cooperation with the third party, and may include subscriber information, communication logs and, where appropriate, the content of digital files and communication messages.<sup>555</sup>

Digital forensics capabilities should also be developed so that law enforcement agencies are able to process, interpret and analyse digital evidence once it has been recovered from a crime scene.<sup>556</sup> This not only relies on sufficient technical capacity, but also requires sufficient human capital in the form of **digital forensic specialists**, who are able to implement digital forensics techniques as part of a criminal investigation.



Digital forensics is a technical field that requires trained individuals with a strong computer science and programming background. **Digital forensic specialists** should have a detailed understanding of computer security vulnerabilities and the latest intruder tools, and be able to apply digital forensic tools while maintaining a **digital chain of custody**. Specialists should also have an understanding of cryptography and steganography, and be able to present evidence in court as an expert witness.<sup>557</sup>

## D4.2 - Criminal justice system



A **digital chain of custody** is a chronological record of digital evidence from the moment of recovery at a crime scene to the presentation of this evidence in court. This record typically includes the signature of the object, the identity of all parties with access to the evidence, the location where the evidence is stored, the timestamp of any access to the evidence, and descriptions of all transactions with and access to the evidence. Maintaining a chain of custody can be particularly difficult for digital evidence for a number of reasons, including difficulties in tracing the activity of individuals once they have access to the evidence (including duplication and transferring of evidence), and difficulties in recording all types of analysis applied to the data, particularly when accessing and analysing remotely.<sup>558</sup> Ensuring a robust chain of custody is essential in maintaining the integrity of digital evidence so that it can be presented in court.<sup>559</sup>

In order to improve the capacity for digital forensics within a law enforcement agency, both in frontline officers and in digital forensic officers, a number of measures can be implemented, including the following:<sup>560</sup>

- **Provide regular training for frontline officers** on procedural law and methods of digital evidence recovery at a crime scene.
- **Hire professionals** with a computer science background, and ideally with some training in digital forensics.
- **Provide regular training to cyber forensics specialists** as part of a systematic training and development programme.
- Ensure sufficient **technical tools and equipment** are available to cyber forensics specialists through coordinated procurement mechanisms.
- Develop a single, national-level **digital evidence database and management system** that stores all digital evidence in a central repository, and records metadata as part of the digital chain of custody.
- Develop **clear digital chain of custody procedures** that are clearly communicated across the criminal justice system.
- **Standardise the procedures and guidelines** for handling and sharing digital information, ideally in line with international guidelines to enable cross-border cooperation.



**Training** for cyber forensics personnel should not only address the technical skills required in investigating instances of cybercrime, but also provide an overview of the management of criminal investigations, and present the functions and ways of cooperating with various stakeholders involved in countering cybercrime, including ISPs, cybercrime reporting platforms, and private cybersecurity firms.<sup>561</sup>



### UK cyber forensics training

In addition to internal training provided within UK law enforcement agencies, cyber forensics training courses are also provided by private sector firms, not-for-profit organisations and academic institutions. For example, a range of different cyber forensics courses are available through the College of Policing, including courses on data recovery and analysis, digital forensics management, and advanced Internet digital forensics. The College of Policing is a not-for-profit police professional body.<sup>562</sup> A range of master-level qualifications are also available in digital forensics at UK universities, including an MSc in Digital Forensics at Cranfield University and an MSc in Computer Forensics at the University of South Wales. These courses are certified by the UK National Cyber Security Centre, which is part of GCHQ.<sup>563</sup>



Cyber forensics training and development is also provided by **multinational organisations**, such as Europol,<sup>564</sup> INTERPOL<sup>565</sup> and ASEAN.<sup>566</sup> Training courses provided by multinational organisations may be particularly useful in countries where the domestic provision of cyber forensics training is limited.



- Establish institutional capacity in prosecution and court services so that they are able to deal with cybercrime cases.

In addition to law enforcement agencies, it is also important to build institutional capacity within the **prosecution and judicial systems** to enable the trial and conviction of cybercrime offences.

As discussed in the introduction to this section, it is the role of the prosecution service to determine whether a case should be tried in court, and to present the case supported by both digital and traditional forms of evidence. Both prosecutors and attorneys should develop sufficient understanding of both the procedural and substantive law surrounding cybercrime to carry out these functions. This can be achieved through a number of mechanisms, including specialised training within the prosecution service,<sup>567</sup> the facilitation of the exchange of information and good practice between prosecutors and judges,<sup>568</sup> and the publication of central legal guidance on cybercrime to facilitate an understanding of cybercrime and the supporting legislative framework.<sup>569</sup>

Similarly, for the judicial system, both judges and magistrates preside over cases of cybercrime in the courts, and an awareness of the different types of cybercrime is required alongside an understanding of digital evidence, and an appreciation of sentencing options available for convicted cases. This may be developed through specialised training courses, and facilitated through information sharing between prosecutors, judges and different judicial systems.<sup>570</sup>

## D4.2 - Criminal justice system



**Cybercrime specialist units** may be established in law enforcement agencies, and in some instances in prosecution services, but they are not advised in judicial systems. The near-ubiquitous nature of technology means that almost all court judges will have to consider cybercrime on a somewhat regular basis. In place of specialised units, it is advised that a selection of judges initially receive specialised training on cybercrime, and these individuals then act as focal points for information and knowledge-sharing within the judicial system.<sup>571</sup>



### Cybercrime training topics for judges

Cybercrime capacity training in the judicial system should cover a range of topics, including:<sup>572</sup>

- The legal implications of cybersecurity in relation to criminal laws;
- The legal framework on cybercrimes;
- The legal issues relating to information security, data protection and security standards;
- The legal issues relating to cybersecurity and the nature of cybercrimes;
- Procedural law and legal procedures governing cyber prosecution;
- The legal issues surrounding computer privacy and data protection principles, including cross-border data flows;
- The legal issues on admissibility of digital evidence;
- Judicial considerations and case studies;
- Criminal law and copyright law (including piracy and other related offences).



- Collect and analyse data and trends on cybercrime and the criminal justice system.

Once institutional capacity is established across the criminal justice system, it may be useful to begin collecting statistics on incidences of and responses to different forms of cybercrime. These statistics can be used to monitor emerging trends in cybercriminal activity, and highlight particular areas of importance for the criminal justice system. When collected over a number of years, these statistics can also be used to monitor the degree to which reporting platforms are used, and evaluate the performance of law enforcement agencies, prosecutors and the judicial system in identifying and convicting individuals who are involved in cybercrime.<sup>573</sup>



Cybercrime statistics cover criminal activity that is detected or reported to law enforcement agencies, but there are a number of factors that contribute to the under-reporting of such incidents. For example, private companies are often unwilling to report instances of cybercrime due to fears of damage to their commercial reputation. Moreover, cybercrimes that target individual citizens through automated processes are often small in value but large in scale (i.e. number of people targeted). The reluctance of individual victims to report small-scale cybercrimes can lead to a significant underrepresentation of the scale of these instances. When analysing cybercrime statistics, it is often unclear whether the number of unreported crimes is significant, which in turn reduces the strength and validity of any statistical analysis.<sup>574</sup>



- Establish specialised cybercrime units within law enforcement agencies.

Once an initial institutional cybercrime capacity is developed within national law enforcement, it may be beneficial to establish **specialised, dedicated law enforcement units** that focus exclusively on cybercrime.<sup>575</sup> A number of different types of specialised units may be established, including investigative cybercrime units, high-tech crime units, computer forensic units, central coordinating units, crime-specific units (such as counter-fraud, counter-illicit content, etc.), and specialised prosecution units.<sup>576</sup> Specialist cybercrime units facilitate the development of more advanced knowledge and skills, as they allow employees to focus on specific areas of criminal activity and also attract specialists with an interest in a particular field of law enforcement. Specialist law enforcement units are particularly useful when tackling large and/or complex cybercrime cases.<sup>577</sup> However, due to the widespread integration and use of ICT, it should be expected that non-specialised law enforcement units will still be required to deal with criminal activity that involves ICT.<sup>578</sup>



#### Netherlands High-Tech Crime Team

In 2007, a **High-Tech Crime Team** was established in the Dutch national police, initially with 15 employees but quickly rising to 120 employees by 2014. However, despite these increases in personnel and resources, the team were only able to respond to a small proportion of the reported cyber-attacks, and the majority were left untouched. To help resolve this shortfall in capacity, the investigatory capacity of the High-Tech Crime Team was extended to general investigatory teams in regional police units, meaning that regional teams were now tasked with carrying out cybercrime investigations. To ensure sufficient capacity within these teams, continued support was provided by digital experts, and in time these regional teams have formed their own dedicated teams of cyber investigators. This approach has meant that small incidents are dealt with on a local level, which allows the central High-Tech Crime Team to focus on larger, more complex cases.<sup>579</sup>

## D4.2 - Criminal justice system



- Implement a process for continued improvement.

It is important to periodically review the institutional capacity of law enforcement, prosecution and the court system based on an assessment of the effectiveness of their work. This is typically based on the continuous collection and analysis of statistics and the use of quantitative and qualitative performance metrics to measure performance against strategic goals, such as those presented in the case study below. There are few examples of pre-existing evaluations of criminal justice systems and their effectiveness in tackling cybercrime, although general frameworks for evaluation of criminal justice initiatives do exist and may be applied in this area. For example, the government of Queensland (Australia) issued a criminal justice evaluation framework, which is referenced along with other relevant resources at the end of this section.<sup>580</sup>



### UK strategic goals vis-à-vis cybercrime

In the UK National Cyber Security Strategy 2016–2021, the UK government identifies a number of metrics for measuring success in tackling cybercrime, namely:<sup>581</sup>

- 1) Implement a greater disruptive effect on cybercriminals attacking the UK, including higher numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention.
- 2) Improve law enforcement capabilities, including greater capacity and skills of dedicated specialists and mainstream officers, and enhanced law enforcement capability among overseas partners.
- 3) Improve the effectiveness and scale of early intervention measures to dissuade and reform offenders.
- 4) Observe fewer low-level cyber offences due to more effective preventative measures.

### Additional resources



- European Union and Council Of Europe. 2011. Specialised cybercrime units: Good practice study. Strasbourg, France: Directorate General of Human Rights and Rule of Law.
- Home Office. 2010. Cyber Crime Strategy (Cm 7842). UK Parliament, London: The Stationery Office Limited.
- ITU. 2011. Understanding Cybercrime: A Guide For Developing Countries. Geneva, Switzerland: International Telecommunication Union.
- World Bank. 2016. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 GO).

## D4.3 – Formal and informal cooperation frameworks to combat cybercrime

### Overview

This factor looks at national capacity to ensure formal and informal cooperation among domestic and international actors to deter and combat cybercrime. Cybercrime is often considered an international or transnational issue, given the tendency of criminals to exploit the jurisdictional boundaries of the global Internet.<sup>582</sup> Criminals use the infrastructure of the Internet to perpetrate crimes internationally, far from the sovereign reach of law enforcement agencies in the places where the crime is committed. In order to protect the confidentiality, integrity and availability of data and IT systems, stakeholders from around the world have entered into formal and informal cooperation frameworks.

Box 4.3 provides an overview of capacity-building steps for increasing national capacity to cooperate in the tackling of cybercrime through formal and informal mechanisms.

### **Box 4.3: Steps for developing or joining formal and informal cooperation mechanisms to combat cybercrime (D4.3)**

- Join formal international cooperation mechanisms to prevent and combat cybercrime through its detection, investigation and prosecution, and facilitate the development of informal cooperation mechanisms to aid the exchange of information on cybercrime issues.
- Establish effective informal cooperation mechanisms and clear communication channels between private sector actors and law enforcement agencies.

### *Capacity-building steps*

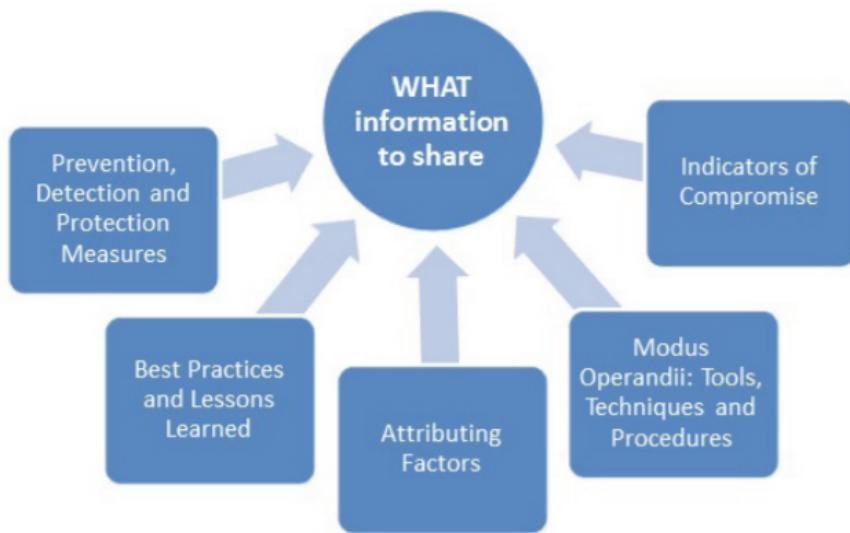


- Join formal international cooperation mechanisms to prevent and combat cybercrime through its detection, investigation and prosecution, and facilitate the development of informal cooperation mechanisms to aid the exchange of information on cybercrime issues.

Criminals have increasingly exploited the cross-border nature of cyberspace to carry out cybercrimes, posing jurisdictional issues for actors and stakeholders involved in tackling them. Consequently, in order to combat cybercrime, a significant degree of international cooperation has become increasingly necessary for governments, international organisations and private sector actors affected by this phenomenon. Figure 4.1 provides a visual overview of the sort of information such cooperation platforms should be used to share.

#### D4.3 - Formal and informal cooperation frameworks to combat cybercrime

**Figure 4.1: Information sharing in the international fight against cybercrime**



SOURCE: WEF (2017)

International cooperation in the fight against cybercrime occurs through both formal and informal mechanisms. Establishing and joining **formal cooperation mechanisms** in the fight against cybercrime can help states address a number of problems which would otherwise hinder their ability to pursue cybercriminals, including:<sup>583</sup>

1. National criminal laws that are inadequate to combat cybercrime as they do not deal with this phenomenon or do not allow for the degree of transnational cooperation required in this context;
2. Procedural powers not equipped to combat cybercrime;
3. Lack of enforceable mutual legal assistance provisions.

Furthermore, even for countries that have fully developed legislative frameworks and procedural powers to deal with cybercrime at the national level, international cooperation mechanisms help ensure the interoperability of their provisions with those of other states.

Formal international cooperation comes in various forms and can employ a range of different mechanisms, including cybercrime-specific multilateral treaties, MLATs, extradition treaties, and law enforcement cooperation agencies and organisations. These instruments are discussed below alongside examples of their use and implementation.



##### Cybercrime-specific multilateral treaties<sup>584</sup>

The purpose of international treaties is to encourage cooperation among signatories on a particular matter. Recent years have seen a wealth of cyber-focused treaties and international agreements, including ones specific to cybercrime.

## D4.3 - Formal and informal cooperation frameworks to combat cybercrime



### The Convention on Cybercrime<sup>585</sup>

The Convention on Cybercrime, also known as the Budapest Convention, was devised by the Council of Europe and represents the first international treaty addressing cybercrime. The Budapest Convention contributed to the harmonisation of international laws on cybercrime by introducing a comprehensive set of rules focusing on substantive, procedural, jurisdictional and international cooperation. The Budapest Convention is legally binding for its signatories, which can include countries that are not part of the Council of Europe, provided that an invite to accede to the Convention is issued by its members.



### Mutual Legal Assistance Treaties<sup>586</sup>

MLATs are treaties, both binding and non-binding, into which two or more states enter to collaborate in the fight against cybercrimes by gathering and exchanging information. The use of MLATs has contributed in several regions to the development of interoperable legislative standards, as states joining such agreements were first required to develop domestic legal frameworks and measures on which MLATs could build and act.



### Extradition treaties<sup>587</sup>

Extradition treaties are instruments designed for enabling a state wishing to prosecute a crime to obtain the required jurisdiction over its perpetrator. Measures providing for extradition are sometimes embedded in multilateral treaties, such as those discussed above, but may be also the subject of separate, *ad hoc* agreements. Extradition treaties establish mechanisms whereby a state commits to honouring a warrant issued by another state, taking wanted individuals into custody and ensuring their transfer to the requesting state.



### International law enforcement cooperation agencies and organisations

International law enforcement cooperation agencies and organisations, such as INTERPOL, are designed to enable police forces from across different countries to collaborate on a range of different issues.

#### D4.3 - Formal and informal cooperation frameworks to combat cybercrime



##### **European Cybercrime Centre (EC3)<sup>588</sup>**

EC3 was first established in 2013 to bolster law enforcement efforts in cyberspace and to help protect European citizens, businesses and governments.

As part of Europol, EC3 serves all EU Member States, institutions and agencies. Furthermore, Europol is able to enter into agreements with third countries and international organisations to enhance its cooperation capacity. This is done through bilateral partnership agreements. EC3 also connects with a range of companies, professional bodies and NGOs.



##### **INTERPOL<sup>589</sup>**

INTERPOL uses its unique role to work with law enforcement agencies to investigate crimes on a cooperative level. With 190 member countries, INTERPOL enables cooperation between law enforcement agencies when diplomatic relations do not exist between governments. By working with private industry, INTERPOL is able to provide local law enforcement with cyber intelligence from a variety of sources around the globe. INTERPOL also established a *Global Complex for Innovation (IGCI)* in Singapore in 2015. The IGCI is a cutting-edge R&D facility for the identification of crimes and criminals, innovative training, operational support and partnerships. The IGCI focuses on cybercrime, including through (i) a forensics laboratory to support digital crime investigations; (ii) research activities to test protocols, tools and services and to analyse trends in cyber-attacks; (iii) the development of practical solutions to cybercrime in collaboration with police, research laboratories, academia and the public and private sectors; and (iv) addressing issues such as Internet security governance.

Looking beyond the frameworks and mechanisms established by formal cooperation mechanisms, states looking to cooperate in the fight against cybercrime should further their participation in and contribution to **informal cooperation mechanisms**.

For the purpose of cooperation among states, informal cooperation mechanisms comprise the use of 24/7 contact networks. Countries should establish a list of directly reachable 24/7 contact points to be shared with partners and allies. Contact points should be able to collaborate with international partners, having an understanding of how different laws, mechanisms and regulations on cybercrime interact at the national and international levels, and having the required operational and technical knowledge necessary to handle an unfolding cybercrime case.<sup>590</sup> These mechanisms and networks do not replace MLATs and other formal instruments for obtaining assistance, but rather enhance and supplement traditional methods in a context where investigators may be required to act very quickly to preserve electronic data and locate suspects.

#### D4.3 - Formal and informal cooperation frameworks to combat cybercrime



##### G8 24/7 Network for Data Preservation<sup>591</sup>

The G8 24/7 Network for Data Preservation is an informal collective set up to help facilitate quick response to international cybercrime investigations. The Network was established in 1999 by the G8 and currently brings together 70 specialist points of contact. The network is used in instances requiring urgent international assistance on investigations involving electronic evidence.



- Establish effective informal cooperation mechanisms and clear communication channels between private sector actors and law enforcement agencies.

In addition to international cooperation among states and law enforcement agencies, the nature of cybercrime requires that effective **cooperation and partnership mechanisms** be established **among public and private sector actors**. Part of the infrastructure on which the cyber environment relies for its functioning is developed or controlled by non-state actors, whose involvement may be necessary as regards issues of access to data and digital forensics. For example, law enforcement investigations into cybercrime would not be possible without the cooperation of ISPs to access the identity of a customer who used a known IP address at a specific time, or the identification of the IP address used by a customer of an ISP whose identity is already known.<sup>592</sup> The effective use of informal cooperation mechanisms and clear communications channels enables law enforcement to bring criminals to justice.



Law enforcement agencies may establish a working group to better engage with ISPs and other industry leaders in the IT sector. The function of the working group could be to:

- Establish common, specific guidelines for positive engagement and cooperation, rather than confrontation, between law enforcement and service providers.
- Encourage information exchange to strengthen their capacity to identify and combat emerging types of cybercrime.
- Provide assurance that the partnership will not infringe any legal rights for industry or interfere with any legal powers on the side of law enforcement.

Within the working group:

- Limits of cooperation should be predicated on the protection of fundamental rights of citizens according to internationally agreed human rights and fundamental agreements.
- The cooperative arrangement should enforce privacy and data protection standards at the domestic level, as well as in relation to cross-border data exchange.
- The financial impact of activities should be fairly distributed, and the subsequent costs of such agreements born by either party should be considered when responding to requests from each party.

#### D4.3 - Formal and informal cooperation frameworks to combat cybercrime

To this end, information-sharing communities and platforms already exist. These are initiatives that bring public and private sector stakeholders affected by cybercrime together in a secure environment to better coordinate their activities and benefit from their respective strengths and expertise. Within these platforms, law enforcement agencies should operate with cognisance of the practical challenges and concerns of private sector institutions (e.g. confidentiality of information provided) that may otherwise stimulate under-reporting of cybercrime incidents. Reporting of cybercrime should be further incentivised, for example by allowing private sector organisations to report attacks confidentially. Increased reporting of cybercrime activities can, in turn, benefit private sector actors as well as facilitating law enforcement investigation activities and improving remediation and risk-management approaches.



##### **Cyber Security Information Sharing Partnership (CiSP)<sup>593</sup>**

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time in a secure, confidential and dynamic environment. The initiative is designed to increase situational awareness and reduce the impact of cybercrime on UK business. Benefits for CiSP members include:

- Engagement with industry and government counterparts in a secure environment;
- Early warning of cyber threats;
- Ability to learn from experiences, mistakes and successes of other users and seek advice;
- An improved ability to protect their company network;
- Access to free network monitoring reports tailored to organisations' requirements.

Further to information-sharing communities and platforms, a number of private sector companies have also launched internal projects and taskforces that aim to tackle cybercrime or vulnerabilities exploited by criminals. Law enforcement agencies and other public sector stakeholders engaged in cybercrime-related activities should be cognisant of such programmes and establish cooperation mechanisms with them.



##### **Microsoft Digital Crimes Unit (DCU)<sup>594</sup>**

Since 2010, Microsoft has worked with law enforcement and industry in the fight against cybercrime. The DCU is an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals based in 30 countries working on cybercrime issues and leveraging innovative approaches and technology solutions for this purpose. The DCU's activities focus on disrupting malware, reducing digital risk, and protecting vulnerable populations.

Additional resources



- World Bank. 2016. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).
- World Economic Forum. 2016. Recommendations for Public-Private Partnership against Cybercrime.
- World Economic Forum. 2017. Guidance on Public-Private Information Sharing against Cybercrime.



## **Dimension 5**

### **Standards, organisations and technologies**



## Dimension 5 – Standards, organisations and technologies

---

Dimension 5 of the GCSCC CMM considers the use of formal standards, international guidelines and information controls to help develop a secure, open and resilient cyber ecosystem.

A large body of literature is constantly evolving on the topics of technical information controls, Internet protocols, cryptographic standards, and cybersecurity compliance, auditing and certification processes. In order to build capacity in these areas, it is advisable to refer to the latest version of official vendor documentation and the state-of-the-art standards due to the rapid pace of technological development.

This dimension of the GCSCC CMM comprises seven factors. The following sections discuss capacity-building steps that national decision makers may implement to build capacity across these issue areas, which are:

### **1. D5.1 – Adherence to standards**

This factor focuses on adoption of and adherence to international standards and good practices in cybersecurity, risk management, procurement and software development.

### **2. D5.2 – Internet infrastructure resilience**

This factor focuses on the availability and resilience of national Internet services and infrastructure, as well as the security processes underpinning their maintenance.

### **3. D5.3 – Software quality**

This factor focuses on securing coding practices to reduce the prevalence of vulnerable software code across the public and private sectors, as well as policies and mechanisms for ensuring adequate software updating and maintenance.

### **4. D5.4 – Technical security controls**

This factor focuses on the technical security controls to achieve security in cyberspace through the adoption of international standards and good practices.

### **5. D5.5 – Cryptographic controls**

This factor focuses on the use at national level of cryptographic and secure communications for data at rest and data in motion, and the adherence of national practice with international standards.

### **6. D5.6 – Cybersecurity marketplace**

This factor considers the cybersecurity marketplace, looking at the availability and development of competitive cybersecurity technologies, and the availability and uptake of cybersecurity insurance.

### 7. D5.7 – Responsible disclosure

This factor focuses on capacity and mechanisms for the responsible disclosure of cyber intrusions and vulnerabilities.

## D5.1 – Adherence to standards

### Overview

This factor looks at adoption of and adherence to international standards and good practices in ICTs, cybersecurity, risk management, procurement and software development. Adherence to international standards is a challenging task, given the rapid pace of technological development and near-constant struggle to implement the latest guidelines. The benefits of adhering to international standards are clear, since they ensure a minimum security level among international stakeholders, reduce complexity and increase the resiliency of systems. Standards also have the effect of lowering the barriers to trade and thereby open up new foreign markets and enable economic growth. The challenge for standards organisations is to achieve consensus among their own members while producing globally acceptable standards. Compounding the difficulty of this challenge, almost all ICT standards are voluntarily adopted. Few standards are mandated by law, and businesses, industry, government and even private citizens should therefore be incentivised to practice and implement standards and guidelines.

Another challenge stems from the multiple meanings of the term ‘standards’. The meaning of the term will differ depending on the context – i.e. whether they are standards in a technical document to implement cryptographic standards for user authentication, a standard to be audited or certified against, or standards of behaviour for states in the international arena. Indeed, common definitions, terminology and spelling are just as integral to the interoperability of information systems as joined-up government.<sup>595</sup>

This section gives national standards leads and policymakers practical steps to implement ICT guidelines and realise the economic benefits of global standards. Box 5.1 provides an overview of the steps proposed, which are discussed in more detail below.

### Box 5.1: Steps for increasing national adherence to ICT standards (D5.1)

- Identify baseline ICT security, cybersecurity and risk-management standards and promote their adoption across the public and private sectors.
- Establish or nominate a task owner body within government responsible for assessing the level of adoption of identified ICT security standards through metrics.
- Establish secure procurement practices that meet international ICT guidelines, standards and good practices.
- Establish a government programme for promoting and monitoring the adoption of relevant standards in software development, for both public and commercial systems.
- Promote the continuous enhancement of ICT security standards and explore their applicability to address risks within the supply chain for critical infrastructure.
- Contribute to the work of international standards bodies.
- Contribute to the ongoing work on norms and international governance of cyberspace.

## D5.1 - Adherence to standards

### Capacity-building steps



- Identify baseline ICT security, cybersecurity and risk-management standards and promote their adoption across the public and private sectors.

Standards and guidelines should be continually adopted in order to benefit from best practice and the economic advantages of global coordination. All governments, businesses and institutions have a role to play in adopting voluntary and common ICT security, technology, cybersecurity, and risk-management standards and protocols, such as those published by ISO and the International Electrotechnical Commission (IEC).

In order to build capacity in the area of ICT standards, stakeholders should consult the state-of-the-art versions of standards and guidelines by **standards developing organisations (SDOs)**. A number of general resources for building capacity in cryptographic controls are listed at the end of this dimension. Specific documentation should be sought out from the following SDOs:

- **International Organization for Standardization and the International Electrotechnical Commission**
  - ISO and the IEC produce a range of standards for cryptographic schemes to support their implementation by global stakeholders. Both organisations are private and voluntary; their members are national standards bodies.
- **National Institute of Standards and Technology**
  - NIST aims to produce strong and effective cryptographic standards and guidelines that are globally accepted and trusted by its stakeholders, with its primary stakeholder being the US federal government.<sup>596</sup>
- **International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)**
  - ITU-T is one of three ITU units, which coordinates standards in telecommunications. Standardisation work is carried out by technical Study Groups where representatives of ITU-T develop recommendations (i.e. standards) for the various fields of international telecommunications.
- Further to the above, there are a number of other SDOs which are relevant for ICTs, such as the Internet Engineering Task Force, Institute of Electrical and Electronics Engineers (IEEE) and the World Wide Web Consortium.

The production of standards by SDOs is typically the result of consensus among national leads from standards organisations and international experts. The resulting standards can be implemented by any organisation, large or small. The implementation of standards provides specific and repeatable steps that organisations can implement to achieve their goals or objectives as they relate to information security. The adoption of relevant ICT security, cybersecurity and risk-management standards should be promoted across the public and private sectors. Relevant standards that organisations and institutions could focus on include:

- **ICT security standards:**
  - ISO/IEC 27001 – **Information security management systems:**<sup>597</sup> The standards set out the requirements for an organisation establishing, implementing, maintaining and continually improving an information security management system.
  - NIST Special Publication 800-14 – **Generally Accepted Principles and Practices for Securing Information Technology Systems:** The publication provides a high-level description of what should be incorporated within a computer security policy.
  - ITU-T Security Compendium:<sup>598</sup> The compendium lists all the ITU-T security-related recommendations on approved, new and revised ICT security measures.
  - The ITU has a database of existing, approved ICT standards which are available for download by the original SDO.<sup>599</sup>
- **Cybersecurity standards:**
  - ISO/IEC 27032 – **Guidelines for cybersecurity:**<sup>600</sup> The standard provides guidance on improving state cybersecurity by drawing out the dependencies in other domains, such as information security, network security, Internet security and CIIP.
  - NIST Framework for Improving Critical Infrastructure Cybersecurity:<sup>601</sup> The framework enables all organisations, regardless of their size or level of maturity, to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.
  - ITU-T X.1205:<sup>602</sup> The standard provides a definition of cybersecurity and a taxonomy of security threats from an organisational point of view. Cybersecurity threats and vulnerabilities, including hackers' most common tools of the trade, are presented.
- **Risk-management standards:**
  - ISO/IEC 27005 – **Information security risk management:**<sup>603</sup> The standard is valuable for all private and public organisations of all sizes in managing risks that could compromise the organisation's information security.<sup>604</sup>
  - NIST Special Publication 800-30 – **Guide for Conducting Risk Assessments:**<sup>605</sup> The standard provides guidance for conducting risk assessments of federal information systems and organisations. The document provides guidance for carrying out each of the three steps in the risk-assessment process (prepare for the assessment, conduct the assessment, maintain the assessment) and on how risk assessments and other organisational risk-management processes complement and inform each other.

## D5.1 - Adherence to standards

- NISP Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View:<sup>606</sup> The special publication offers guidance for an integrated, organisation-wide programme for managing information security risk to organisational operations (i.e. mission, functions, image and reputation), organisational assets, individuals, other organisations and the state, resulting from the operation and use of federal information systems.



ISO/IEC offer a select list of free standards for download online. All the standards are protected by copyright; however, they allow vendors to consult international best practice without any financial cost.<sup>607</sup>



- Establish or nominate a task owner body within government responsible for assessing the level of adoption of identified ICT security standards through metrics.

Audits verify whether a company is compliant with a standard. Importantly, many SDOs do not provide auditing services. Organisations that implement ICT security, cybersecurity and risk-management standards can choose to undergo a compliance audit by **an independent and accredited body**. Auditing companies are a vital part of the quality assurance process and **states should support and promote** a list of local IT security auditors. As **certification is the achievement of a standard**, many companies use certificates to reassure customers of their quality and as a means of building trust. **Periodic review of industry standards is necessary**, as they are updated and respond to the changing threat landscape. A number of steps to build capacity in the adoption and monitoring of ICT security standards (i.e. standards which are referred to by industry as cybersecurity standards and IT risk-management standards) are detailed below.



The onus is on all actors from the public and private sectors to continually adopt and implement the latest information security updates. Often there are no legal consequences of failing to meet industry standards and pass compliance audits, unless they are *de jure* standards, meaning national or international legislation requires that they be met. Depending on the organisational structure, the responsibility to meet industry standards should reside with a Chief Information Security Officer, or similar position, in order to ensure compliance.

As part of the compliance regime, the standard is managed by a SDO and is reviewed and updated as required. Certification bodies are then licensed by the SDO to certify candidate organisations. Standards can be assessed at two levels of assurance.

The first level is verified self-assessment, under which the candidate organisation completes an online questionnaire. This is marked by a certification body which awards the certification if all of the answers given are compliant with the standard.

The second level is audited assessment, under which the candidate organisation is visited by a licensed certification body which verifies compliance with the standard and, if appropriate, issues certification.

Governments have a role to play in **promoting good cybersecurity practices** by encouraging businesses and institutions to adopt voluntary technical security controls. National governments should **lead and endorse the implementation of technical standards** through programmes, initiatives and schemes to build capacity in their businesses and institutions. A **government task owner should be established or nominated** to lead adoption of ICT security standards in the public and private sectors, while collecting metrics relating to compliant organisations. National governments can build capacity by committing national experts to join the creation of non-treaty international standards, such as ISO/IEC and the ITU.

For instance, the UK has a Cyber Essentials programme that encourages companies and organisations to conform to cybersecurity standards in order to compete for government contracts (see the case study box below). The standard used to assess compliant businesses is the IASME information assurance standard, which is particularly suitable for SMEs. IASME controls are aligned with the Cyber Essentials scheme and certification of compliance with the IASME standard usually includes certification under Cyber Essentials.



### UK Cyber Essentials

The Cyber Essentials scheme broadly targets private sector organisations, regardless of their size or sector of operation. Universities, charities, public sector organisations and not-for-profits can also seek certification through the scheme.

With one in four businesses in the UK experiencing an attack or breach in 2015, the UK government put in place the Cyber Essentials initiative to protect organisations from the most common kinds of cyber threat. Organisations are able to contact an accreditation body in order to receive a Cyber Essentials certificate. A self-assessment questionnaire is completed by the organisation against a number of technical requirements and a certification body can process and award the Cyber Essentials certificate. Upon completion, the organisation is then able to apply for government contracts.

The Cyber Essentials scheme requires organisations to have five technical controls in place:

- Boundary firewalls to prevent unauthorised access
- Secure configuration
- User access control (restricting access to those who need it)
- Malware protection (i.e. using anti-virus software)
- Patch management (i.e. updating software).

## D5.1 - Adherence to standards



- Establish secure procurement practices that meet international ICT guidelines, standards and good practices.

Secure procurement practices should be aligned with IT guidelines, standards and good practices. Organisations in the private and public sectors should ensure that all hardware and software purchases are compliant with national and international standards. These purchasing practices should also comply with supply chain security standards (as explained in the following step), considerations of interoperability, and existing ICT security standards. The following practices should be followed by all public and private sector organisations involved in, or impacted by, procurement decisions and processes (i.e. those responsible for the procurement of IT-related goods and services):

- **Ensure purchased products are compliant with national and international technical standards.** Organisations should consider whether or not the products they procure adhere to national and international standards. For instance, computer networking equipment (e.g. routers, switches and cabling) should be compliant with industry standards (e.g. IEEE 802.11b networking equipment).
- **Consider whether the purchase of additional hardware or software products will impact accreditation under existing standards.** For instance, businesses should consider how purchasing new IT equipment or cloud-based services will impact their ability to secure customer data. Organisations compliant with ISO 27001:2013, for instance, should be aware of how new procurements impact their operating risks.
- **Ensure interoperability of new products with existing systems.** Organisations should be aware of interoperability between legacy systems and new systems being procured. For instance, many operating systems only permit certain software programs and applications to execute to ensure interoperability. Designing interoperable systems is one of the principles underpinning technical standards. Conversely, interdependent systems may cause a whole system to crash if one sub-system fails. Vulnerability disclosure programmes (as outlined in D5.7 – Responsible disclosure) mitigate the risks posed by interdependent and common systems used by vendors.
- **Consider the security of the supply chain.** Businesses should be conscious of supply chain security and how their products are delivered to other suppliers or vendors, as well as securing incoming goods and services to their company. ISO 28000 on specification for security management systems for the supply chain explains how companies can manage supply chain security through linked business management activities, while increasing business resilience.



### Sustainable procurement practices

Every business or government agency has environmental, social and economic impacts. Sustainable procurement is an opportunity for organisations to provide value by improving productivity, assessing value and performance, and enabling communication between purchasers, suppliers and all relevant stakeholders.<sup>608</sup> Guidance for organisations, regardless of their activity or size, on integrating sustainability within procurement is available through ISO 20400.



- Establish a government programme for promoting and monitoring the adoption of relevant standards in software development, for both public and commercial systems.

Insecure software development practices lead to vulnerabilities in physical and virtual systems. These vulnerabilities can be exploited, typically to the detriment of users and organisations across the private and public sectors. In an effort to code secure software and reduce the prevalence of vulnerabilities, governments could monitor the adoption and implementation of software-development standards.

The first step to building capacity in this area is for governments to establish a programme to promote and monitor the adoption of relevant software standards. Governments could collect information on compliant organisations, businesses and government agencies. This programme could be similar to the UK's Cyber Essentials but tailored to software coding. A task lead (e.g. a national cybersecurity centre, national CERT or another organisation) should be **nominated by government appointment**, and should be accountable for the monitoring of compliance with standards.

There are a number of industry standards on secure software development that could be monitored, including:

- **ISO/IEC 25010:2011 System and software quality models:**<sup>609</sup> The standard presents quality models which support the specification and evaluation of software and software-intensive computer programs.
- **NISTR 8151 Dramatically Reducing Software Vulnerabilities:**<sup>610</sup> The document responds to the call to drastically reduce software vulnerabilities, which have outpaced processes to find and fix them.

There are a number of other steps governments could take to establish a monitoring function for software-development standards, such as:

- **Prioritise critical national infrastructure and single points of failure.** For instance, government could focus on critical information infrastructure systems, as well as those critical infrastructures which rely heavily on information systems (e.g. defence and security, telecommunications, transportation and energy sectors).
- **Promote standards for responsible software development.** Secure coding standards encourage programmers to follow a uniform set of rules and

## D5.1 - Adherence to standards

guidelines determined by the requirements of the project and organisation, rather than by the programmer's familiarity or preference. For instance, the **Secure Coding Initiative** led by US CERT coordinates the development of secure coding standards by security researchers, language experts and software developers using a wiki-based community process.<sup>611</sup>

- **Encourage organisations to develop software according to security-by-design and privacy-by-default practices.** Organisations in the private and public sectors should be encouraged to develop software according to security- and privacy-related principles.

Section D5.3 on software quality provides further detail on the adherence to standards to support the development of secure code.



- Promote the continuous enhancement of ICT security standards and explore their applicability to address risks within the supply chain, particularly for critical infrastructure.

Expertise in the area is vital to address cybersecurity risks along the supply chain, given IT systems and their components are often composed of numerous foreign sources. These risks ought to be mitigated and treated, especially in critical infrastructure sectors (such as energy and power generation, communications networks, water and waste systems, and transport networks).

As businesses and organisations become more interconnected, there are greater risks to the supply chain of goods and services. Increasingly, there are links between suppliers who hold long-term access to their clients' information, assets and people, which can present serious vulnerabilities if not monitored. Examples of this type of supplier include:<sup>612</sup>

- Cloud computing providers that hold large amounts of their clients' data (e.g. credit information, personally identifiable information, staff records, intellectual property) in other organisations and foreign countries;
- IT contractors who work with multiple client organisations and can hold sensitive access at two competing companies simultaneously;
- Network service suppliers that provide data storage or security functions at remote locations (often overseas);
- Overseas call centres;
- Organisations that maintain physical security of sensitive sites (e.g. datacentres);
- Third-party recruitment organisations.

Security management systems to mitigate supply chain risks (e.g. ISO 28001:2007 – Best practices for implementing supply chain security, assessments and plans; NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations) allow for the mitigation of risks along the ICT supply chain for critical infrastructure. They enable organisations in international supply chains to:

- Develop and implement supply chain security processes;
- Establish and document a minimum level of security in a supply chain;
- Assist in meeting the applicable authorised economic operator criteria, conforming to national supply chain security programmes.

Additionally, the supply chain security management system establishes requirements for organisations which would permit verification of security practices. It allows an organisation to show part of the international supply chain they have securely established, develop adequate countermeasures and train personnel in security-related duties.



➤ Contribute to the work of international standards bodies.

The development of technical standards and guidelines aims to codify an established norm or convention for technical systems. Those involved in the process of establishing formal standards are typically from a country's national standards body and lead contributions to the setting of global and international standards.

Many standards organisations have a diverse range of inputs to the development of voluntary standards. National standards leads may want to consider **contributing to the following technical standards bodies, working and study groups**. States should balance competing priorities and constraints stemming from limited resources, prioritising contributions in accordance with national priorities and levels of ambition. A non-exhaustive list of technical standards bodies and working groups includes:

- **Technical standards:**
  - ISO, the IEC and the ITU run working groups to which national leads can contribute.<sup>613</sup>
  - The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) is a consensus building organisation that nurtures, develops and advances global technologies through the IEEE. With collaborative partners in over 160 countries, the IEEE-SA aims to facilitate standards development and standards-related collaboration.<sup>614</sup>
- **Internet technical standards:**
  - The Internet Engineering Task Force (IETF) is a ‘large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.’<sup>615</sup>
  - The Internet Engineering Steering Group is ‘responsible for technical management of IETF activities and the Internet standards process.’<sup>616</sup>
  - The World Wide Web Consortium is ‘an international community where Member organisations, a full-time staff, and the public work together to develop Web standards.’<sup>617</sup>

## D5.1 - Adherence to standards

- The Internet Assigned Number Authority's (IANA) function is the global coordination of the DNS root, IP addressing, and other Internet protocol assignments and registrations.<sup>618</sup>
- The Internet Corporation for Assigned Names and Numbers (ICANN) is a private sector, not-for-profit corporation with global participants dedicated to keeping the Internet secure, stable and interoperable.<sup>619</sup>



➤ Contribute to the ongoing work on norms and international governance of cyberspace.

Internet governance is comprised of the **principles, norms, rules, procedures and programmes** that shape the evolution and use of the Internet.<sup>620</sup> Many actors are involved in governing the Internet, from **governments to the private sector and civil society**. There are numerous standards organisations to which cyber policymakers could contribute in order to build expertise and capacity, both domestically and internationally. For instance, the following international policy organisations tasked with setting standards often seek consultation with **international experts and national standards leads** in their working groups, as well as issuing standing calls for collaboration between interested individuals. The following organisations have been selected as possible options for national experts to contribute towards:

- IANA, ICANN and ITU, which are presented in greater detail under the previous capacity-building step;
- A regional Internet registry, which is a not-for-profit organisation that administers, manages and registers IP address space and Autonomous System numbers within a defined region of the world;<sup>621</sup>
- The United Nations Group of Governmental Experts (UN-GGE) in the field of information and telecommunications in the context of international security, which regularly holds meetings with approximately 20 experts from as many countries to examine the existing and potential threats from the cyber sphere and possible cooperative measures to address them.<sup>622</sup>



Government policymakers involved in the cyber domain can be expected to contribute and advise according to the emerging norms of responsible state behaviour in cyberspace. A number of consensus reports produced by the UN-GGE have led to the development of norms, rules and principles of responsible behaviour of states in the cyber domain. These norms are:

- States should commit to an accessible, open, interoperable, reliable and secure cyberspace.
- States should recognise the economic, social and political developments empowered by ICTs.
- States should guarantee full respect for human rights, including privacy and freedom of expression.

- States should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure.

#### Additional resources



- ENISA. 2016. Definition of Cybersecurity: Gaps and overlaps in standardisation. Heraklion, Greece: ENISA.
- ENISA. 2015. Standardisation in the field of Electronic Identities and Trust Service Providers. Heraklion, Greece: ENISA.
- ISO. 2013. ISO/IEC 27001:2013 – Information technology, security techniques, Information security management systems, requirements. Geneva, Switzerland: ISO.
- ISO. 2013. ISO/IEC 27032:2012 – Information technology, security techniques, guidelines for cybersecurity. Geneva, Switzerland: ISO.
- ISO. 2013. ISO/IEC 27005:2011 – Information technology, security techniques, information security risk management. Geneva, Switzerland: ISO.
- ISO. 2013. ISO/IEC 25010:2011 – Systems and software engineering, systems and software, quality requirements and evaluation (SQuaRE), system and software quality models. Geneva, Switzerland: ISO.

## D5.2 – Internet infrastructure resilience

### Overview

This factor looks at the availability and resilience of national Internet services and infrastructure, as well as at the security processes underpinning their maintenance. The proper functioning of the Internet and associated information technologies is central to national security and economic prosperity as more businesses, governments, academic institutions and private citizens become dependent on it for their day-to-day functioning.

The Internet infrastructure is operated by a combination of entities from the private and public sectors. These actors work together to maintain and manage the networks. However, it is useful to distinguish between two kinds of Internet infrastructure:

- Core physical infrastructure (e.g. backbones, fibre cables, routing equipment);
- Core protocols and services, which include the Internet layer (e.g. IPv4/6), transport layer (e.g. TCP/UDP) and application layer (e.g. DNS, HTTP etc.).

The resilience of a system is measured by its capacity to recover quickly from adversity and return to proper functioning. The Internet infrastructure has a certain level of inherent resilience, given its capacity to serve increasingly large volumes of legitimate user requests.<sup>623</sup> The Internet's resilience is underpinned by applied network science and the ability of data packets to route around blockages in the system.

The interdependence and interconnected nature of computer networks comprising the free and open Internet presents a number of challenges and opportunities for coordinating public and private sector preparedness and exercises.<sup>624</sup> Governments should be mindful that much of the responsibility for Internet resilience lies with non-governmental organisations and the private sector since these own, operate and maintain much of the infrastructure that undergirds the Internet. However, in order to build capacity in the area of Internet infrastructure resilience, a number of policy areas may be addressed. In particular: (i) good practice guides should be implemented to strengthen the capacity, resilience and survivability of networks; and (ii) critical national infrastructure plans for the IT sector should be commissioned.

Box 5.2 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 5.2: Steps for improving Internet infrastructure resilience (D5.2)

- Facilitate the establishment of reliable Internet infrastructure and Internet services in the country.
- Ensure that rules, regulations and national strategies are in place to control and strategically manage critical and infrastructure technologies.
- Ensure that national Internet infrastructure is managed formally through documented processes, roles and responsibilities.
- Periodically assess communications technology and processes deployed nationally for Internet infrastructure to ensure that they meet international IT guidelines, standards and good practices.
- Establish service continuity processes for critical technologies.

- Ensure the continuous availability and advancement of the national scientific, technical, industrial and human capabilities required to maintain the country's independent resilience.

### *Capacity-building steps*



- Facilitate the establishment of reliable Internet infrastructure and Internet services in the country.

A range of actors from the private and public sectors contribute to the development of the cyber ecosystem on which a national Internet relies, including:

- Organisations that provide Internet access (e.g. Tier 1 service providers and ISPs);
- Organisations that support the proper functioning of the Internet (e.g. CERTs, national cybersecurity centres).

Improving the capacity of the national Internet infrastructure can assist countries in the event of an incident, crisis or natural disaster which may otherwise cripple the functioning of fundamental services or broader public and private sector activities. The Internet infrastructure can be sub-divided into the physical and logical components, as follows:

- Physical protection encompasses all the physical parts of the infrastructure, such as cable links, radio equipment, connection points and satellite links. To physically protect the entire network is a virtually impossible task due to the enormity of the network. However, prioritising protection of weak points, designing redundancy and resilient systems can overcome some physical vulnerabilities.
- The logical components of the Internet infrastructure include the domain name system, secure transmission of data (i.e. using cryptography and secure Internet protocols, such as HTTPS). The security of the Internet's logical components is dependent on the proper implementation of information security standards.

There is no one-size-fits-all approach for stimulating the development of Internet infrastructure. Governments may lead such activities by providing direct investment or adopting policies to trigger greater private investment in infrastructure development (e.g. tax cuts; subsidies), while ensuring that infrastructure security also remains an area of focus.<sup>625</sup> Furthermore, developing countries may benefit from international programmes and investments under the Sustainable Development Goals (SDG) initiative.<sup>626</sup> SDG 9 aims to 'significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020', which has resulted in assistance and funds being provided by donors and international organisations for this purpose.<sup>627</sup>



**The Korean Trust Fund on ICT to development challenges (ICT4D)<sup>628</sup>**

### D5.2 - Internet infrastructure resilience

Innovators seeking to apply ICT to development challenges have recently contributed to a number of World Bank projects. This approach has been supported by the Republic of Korea since 2008 with a \$15 million trust fund that supports activities that serve as inputs to the preparation of projects in three areas. Actions include increasing access to affordable broadband infrastructure services through policy and regulatory interventions, and where needed through catalytic PPP investment, with a focus on mobile broadband. Proposals are submitted periodically to the Korean government for review and approval.



National governments should be prepared for a number of possible scenarios which could result in the Internet suffering from a systemic failure, leading to a localised collapse of infrastructure, system-wide congestion or cascading technical failures.<sup>629</sup>

**Physical failure:** A regional failure of the physical infrastructure supporting the Internet, such as a prolonged and widespread blackout, severed fibre cable or planned maintenance to undersea cables could take the Internet offline.

**Technical failure:** A range of cascading technical failures (i.e. IoT vulnerabilities or major insecurity in networking equipment) could lead to instability of the Internet.

**Intentional attack:** A coordinated attack to disrupt the fabric and routing protocols could take the Internet offline. For instance, in 2016 a US DNS provider, Dyn, was hit by a DDoS attack.<sup>630</sup> By exploiting the inherent vulnerability of the interconnections of the Internet, a sustained attack could eventually break access to the Internet for a period of time.



- Ensure that rules, regulations and national strategies are in place to control and strategically manage critical infrastructure.

Global communications is an enabling function across many CNI sectors.<sup>631</sup> The Internet, as a subcomponent of the global communications system, should be secured to ensure the continued flow of information, capital, people and goods.

For this purpose, protection plans should be devised for critical infrastructure underpinning the functioning of the Internet at the national level. A CNI plan should be commissioned by national governments in order to support the resilience of Internet infrastructure and, more broadly, the IT sector.<sup>632</sup> A detailed overview of steps for developing critical infrastructure protection plans is provided in Section D1.3 on critical infrastructure protection. This section will discuss only those details specific to a CNI-IT plan.

The aim of a CNI-IT plan should be clearly expressed in its vision statement and strategic priorities. Any priorities identified should be aligned with other relevant policy goals identified in the national

cybersecurity strategy, or with broader CNI priorities in other sectors. Example priorities specific to the CNI-IT sector are:

- Increasing the resilience of CNI through effective risk management and alignment with the NIST cybersecurity framework for the IT sector;
- Strengthening collaboration across sectors by improving information sharing arrangements, incident handling and situational awareness;
- Increasing engagement and collaborative PPPs to enhance incident response, recovery and resilience efforts.



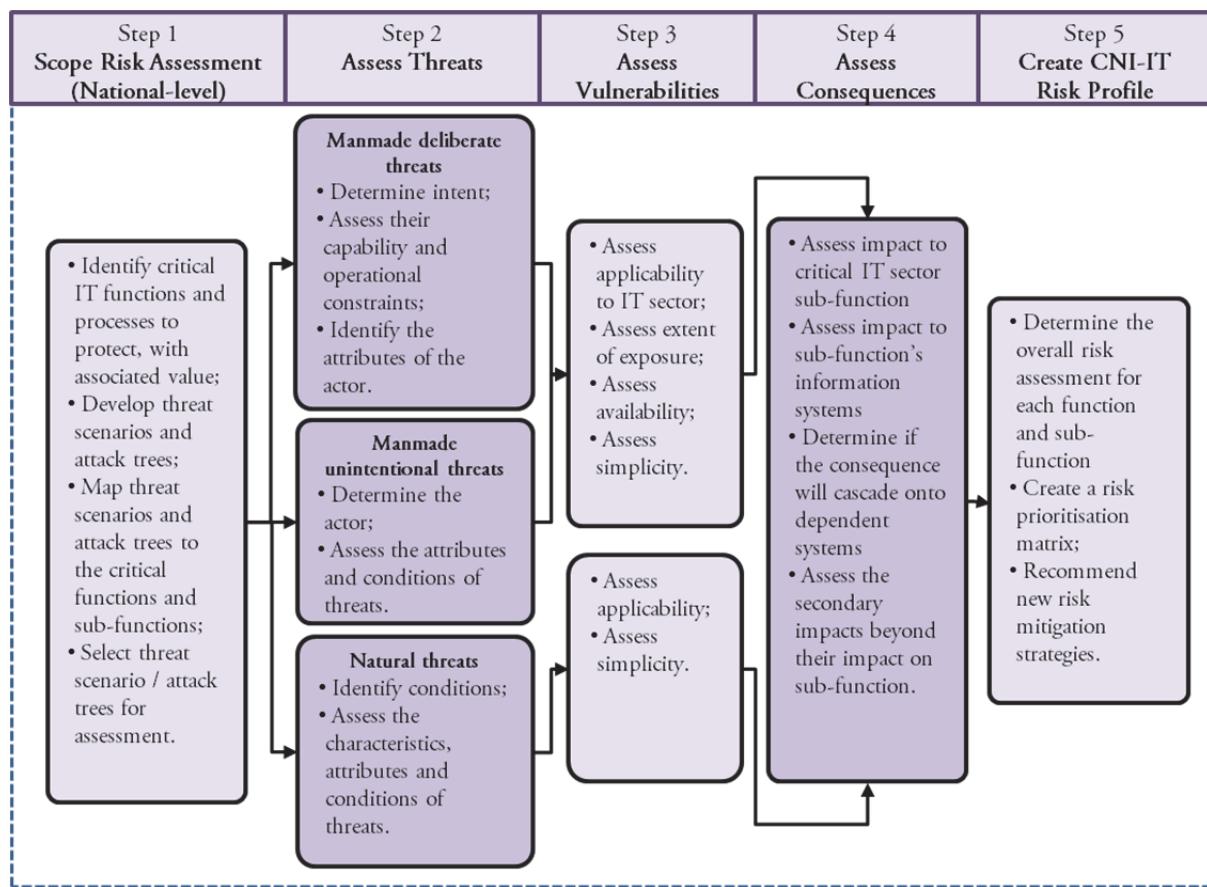
The responsibility to produce a plan would typically be taken on by a domestic security ministry or department with responsibility for public security and safety. A steering board or coordinating council, comprised of experts from the sector, should be sought along with leadership from senior government policymakers. Updates to the original document should be conducted on a regular basis (e.g. every 4 to 6 years) and aligned closely with (at a minimum) CNI resilience reports in other sectors and the national cybersecurity strategy.

Achieving the vision statement depends in part on the adoption of a risk-management methodology to identify, assess and help facilitate the management of risks to the IT sector. A range of sector-specific risks are commonly identified, including risks to the supply chain, dependencies and interdependencies, third-party suppliers, backup systems and designed redundancy.

An all-hazards risk assessment method should be implemented to capture the national-level risks to CNI, applying a top-down, functions-based approach. After identifying a range of threats which meet a minimum consequence threshold, resources can be allocated to effectively mitigate threats. An all-hazards approach is able to capture physical threats to cyber resources and digital assets. Figure 5.1 provides an overview of an example all-hazards risk assessment for CNI-IT.

## D5.2 - Internet infrastructure resilience

**Figure 5.1: Risk assessment steps for CNI-IT**



SOURCE: RAND Europe adaptation of US Department of Homeland Security (2013)



- Ensure that national Internet infrastructure is managed formally through documented processes, roles and responsibilities.

To ensure the adequate protection of the Internet infrastructure at a national level, the national government should support protection, through formal management and documentation, of the processes, roles and responsibilities of each actor. At a minimum, telecommunications and cybersecurity policy leads should clarify the roles and responsibilities of their national organisations, stakeholders and agencies for those within the telecommunications and regulations departments who will work with these stakeholders. Actors with roles and responsibilities to be clarified could include:

- CSIRTs: CSIRTs respond to computer security indents at a national or regional level, research security vulnerabilities in software products, contribute to long-term changes in networked systems, and develop cutting-edge information and training to help improve cybersecurity (e.g. CERT-EU). Further information on these is available in Section D1.2 on incident response.
- National Cybersecurity Centre: Where present, this type of institution represents the lead government department on shared cybersecurity situational

awareness. Centres bring together critical infrastructure protection, government information assurance functions, CERTs and law enforcement to combat cybersecurity incidents and threats.

- Internet service providers: ISPs purchase network capacity from backbone providers (e.g. Tier 1 providers) to sell their services to customers such as businesses, organisations and consumers. Tier 1 providers are those companies with a comprehensive network and that as such do not have to purchase transit agreements from other providers. The providers of some of the largest backbone networks are long-distance telephone networks, supported by undersea cables. These backbone providers sell their services to ISPs (e.g. Level 3 Communications).
- ITU's National Spectrum Management:<sup>633</sup> ITU provides guidance on key elements of spectrum management, spectrum planning, frequency assignment and licensing, spectrum monitoring, spectrum inspection and investigation, spectrum engineering, spectrum economics, automation of spectrum management activities, and measures of spectrum utilisation and spectrum utilisation efficiency.



- Periodically assess communications technology and processes deployed nationally for Internet infrastructure to ensure that they meet international IT guidelines, standards and good practices.

Measuring the effectiveness of communications technology and associated processes begins with the vision statement and strategic priorities of a national security strategy, cybersecurity strategy or critical infrastructure strategy. Developing policy and strategy documents with measurable outputs in mind allows for progress to be tracked, measured and improved.

Governments may nominate an authority to assess a sector's progress on implementation and on compliance with international IT guidelines, standards and good practices. Such an authority may take the form of a cross-industry taskforce, supporting the work of a regulatory body led by a ministry or governmental department with responsibility for cybersecurity, telecommunications or related areas.

There are a number of sectors that may be relevant to monitor in the context of IT standards compliance, including banking, finance, telecommunications, IT and defence. Below are some examples of standards which could be assessed in the telecommunications sector:

- Telecommunications good practice guide:
  - UK's good practice guide to telecommunications resilience – the guide offers a number of recommendations for the provision of resilient networks.<sup>634</sup>
- Telecommunications standards:
  - ISO/IEC 17568:2013 on close-proximity electric induction wireless communications;
  - ISO/IEC TR 8802 suite on telecommunications and information exchange between systems.

## D5.2 - Internet infrastructure resilience

Evaluating compliance of the telecommunications sector with international standards entails tracking and capturing sector-wide progress towards strategic priorities through SMART objectives. The authority tasked with evaluating compliance and progress should report on annual progress of the sector and feed back to inform future updates of strategies.



- Establish service continuity processes for critical technologies.

For national governments, critical technologies may include any service or data repository required for the proper functioning of public administration. This definition could be applied to any database or register supporting the delivery of functions pertaining to:

- E-identification services
- Land registers
- Health data
- Social services registers
- Judiciary documents
- Roads, rail and transportation information
- Telecommunications systems
- Defence and military systems.

While further considerations around approaches to assuring protection and continuity of service of critical infrastructure are presented in Section D1.3 of this document, governments may also consider the option of contracting external providers. For example, a digital or data embassy is one such solution to ensuring service continuity for vital government datasets.



### Estonia's digital embassy

Estonia is the pioneer of 'digital embassies'. The purpose of a digital embassy is to securely store government data in another sovereign territory. Estonia signed an agreement with Luxembourg on 20 June 2017 for the housing of data and information systems, creating the world's first data embassy. The aim of the data embassy is to ensure service functionality and data continuity.<sup>635</sup>



### Standards for IT security and critical infrastructure

Standards bodies offer guidance and good practice on the protection of critical infrastructure. ISO/IEC 27010:2015 – **Information security management for inter-sector and inter-organisational communications** is one such standard.<sup>636</sup> The standard provides guidance on information risks, security controls, issues and/or incidents that span the boundaries between industry sectors and/or nations, particularly those affecting critical infrastructure.



- Ensure the continuous availability and advancement of the national scientific, technical, industrial and human capabilities required to maintain the country's independent resilience.

The training, education and skills required to secure the Internet infrastructure relies on national scientific, technical, industrial and human capabilities. Science, technology, engineering and mathematics (STEM) degrees offer a broad range of technical skills and knowledge required to support the telecommunications and IT sectors. Universities should offer degrees in these areas, as well as leading research efforts in a number of academic disciplines that underpin the Internet's proper functioning, such as:

- **Computer science:** The discipline and study of theory, experimentation and engineering that forms the basis of computing.
- **Network science:** The study of complex networks (e.g. telecommunications networks, computer networks, cognitive networks and social networks) where connections are represented by nodes (vertices) and connected by links (edges).
- **Systems science:** The interdisciplinary field of studies that concern complex and simple systems, in nature, society, cognition and science itself.

Moreover, a working knowledge of policies and regulations in telecommunications should be a priority for educational and vocational institutions. Sponsorships and scholarships between private industry and educational institutions should be supported by government programmes as a means of investing in human capabilities. The section of this document on Dimension 3 (Cybersecurity education, training and skills) provides an in-depth overview of initiatives and approaches that a government may adopt to foster the availability and accessibility of cybersecurity education and training at different levels of society.



### GCHQ-accredited university degrees

The UK's signals intelligence agency, GCHQ, has accredited six UK universities to teach specialist master's degree courses for future Internet security experts,<sup>637</sup> having first invited the universities to submit their courses for certification. This initiative stems from a recognition of education and workforce development as a means of improving defences against hackers and online fraud. The universities now running GCHQ-approved programmes in cybersecurity are Edinburgh Napier University, Lancaster University, the University of Oxford and Royal Holloway, University of London.

## D5.2 - Internet infrastructure resilience

### Additional resources



- Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis & Panagiotis Trimintzios. 2013. Resilience of the internet interconnection ecosystem. In *Economics of Information Security and Privacy III*. Springer.
- US Department of Homeland Security. 2008. Recommended Practice for Patch Management of Control Systems. Geneva, Switzerland: International Telecommunication Union.
- ITU (International Telecommunications Union). 2015. National Spectrum Management. Geneva, Switzerland: International Telecommunication Union.
- NICCS (National Initiative for Cybersecurity Careers and Studies). 2017. Cybersecurity. London, UK: Security Co-Ordination Centre.
- ISO. 2015. ISO/IEC 27010:2015 – Information technology, security techniques, information security management for inter-sector and inter-organizational communications. Geneva, Switzerland: ISO.

## D5.3 – Software quality

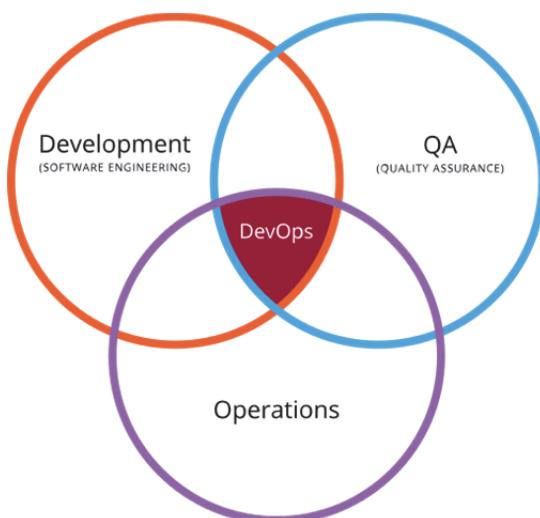
### Overview

This factor focuses on secure software development practices designed to reduce the prevalence of vulnerable software code across the public and private sectors. It also looks at policies and mechanisms for ensuring adequate updating and maintenance of software.

Software development involves coding, computer programming and the writing and maintenance of source code through the use of a structured or planned process. There are number of elements to software development, such as software programming, documentation, testing and bug fixing, as well as maintaining code bases and frameworks which result in the software product. Quality assurance (QA) processes have been applied to software development in order to ensure rigorous methods and high-quality, secure and consistent software code across applications.

The delivery of timely, frequent and reliable software updates is the responsibility of professional software engineers. These professional coders often work in close coordination with IT operations to provide securely developed software updates. DevOps<sup>638</sup> employs agile methods to maintain continuous delivery of software upgrades, as well as the monitoring of released software and elements from Quality Assurance procedures, as shown in Figure 5.2 below. Box 5.3 provides an overview of capacity-building steps for increasing national capacity in this area.

**Figure 5.2: DevOps showing the intersection of software development, operations and quality assurance.**



SOURCE: Released under the Creative Commons Licence 3.0. Unedited, Author: Pant, Rajiv.

## D5.3 - Software quality

### Box 5.3: Steps for improving software quality (D5.3)

- Identify software quality standards and functional requirements for public and private sector software developers.
- Appoint a task lead to monitor and assess on a regular basis the quality of software design methods and processes used in the public sector.
- Review policies and processes regulating software updates and patching systems on the basis of risk assessments and criticality of services involved.
- Continuously review software quality processes, updating and adapting these to the changing cybersecurity environment.

### Capacity-building steps



- Identify software quality standards and functional requirements for public and private sector software developers.

Software quality management (SQM) is the process of managing the final product of software development in order to satisfy the needs and requirements of the end-user. The advantage of practicing SQM is that it reduces the number of errors and bugs encountered by the end-user, and also reduces the risk of fraud and theft of proprietary code through proper development. The practice of SQM is often found in organisational settings, where software as a service (SaaS) is carried out by trained and professional coders. Software quality can be enhanced by a number of factors in organisational settings, including:

- An organisational quality culture whereby quality is viewed as everyone's responsibility;
- An appreciation that security is 'baked in' rather than 'bolted on';
- **Implementation of software quality standards**, such as:
  - ISO 25000:2014 Systems and software Quality Requirements and Evaluation (SQuaRE). This standard provides a guide and common reference model and definitions for practicing SQuaRE, as well as the relationship among the ISO 25000 series documents.
  - ISO/IEC 25010:2011 System and software quality models.<sup>639</sup> This standard presents quality models which support the specification and evaluation of software and software-intensive computer programs.
- The use of **good practice** guides to support secure coding practices:
  - NISTR 8151 Dramatically Reducing Software Vulnerabilities.<sup>640</sup> This document responds to the call to drastically reduce software vulnerabilities, which have outpaced processes for finding and fixing them.
  - The implementation of **non-technical approaches to reduce software vulnerabilities**, such as engaging the research community at universities,

think tanks and policy institutes to identify state-of-the-art secure coding practices.

These good practices and organisational characteristics should be developed and nurtured in both public and private organisations that focus on high-quality software code.



- Appoint a task lead to monitor and assess on a regular basis the quality of software design methods and processes used in the public sector.

A digital and innovation task lead for government services (similar to the UK government's digital services department within the Cabinet Office) should be appointed to ensure that digital services (especially high-quality software code) are being delivered through the public sector. This role will enable government to practise secure coding throughout the public sector and to more effectively monitor and assess software-intensive projects. For instance, the task lead can implement the 'agile' project management method to deliver projects rapidly, to tight deadlines and in a manner that is responsive to evolving needs. SaaS has moved away from the 'waterfall' method for software development and toward agile, which is widely regarded as being better for the delivery of services to meet user needs.<sup>641</sup>



The core tenets of agile software development are expressed in the *Manifesto for Agile Software Development*, first published in 2001. These are:<sup>642</sup>

- **Individuals and interactions** are valued over processes and tools
- **Working software** is valued over comprehensive documentation
- **Customer collaboration** is valued over contract negotiation
- **Responding to change** is valued over following a plan.



#### Agile and lean software in the UK public sector

In the United Kingdom, the government published in 2016 a detailed service manual outlining the principles, tools and governance processes that underpin agile working. Lean software development, as part of the agile approach, is practiced by the UK government in order to achieve:

- Waste reduction
- Quick delivery
- Learning and improving
- Using evidence and data to make decisions.

For instance, the Government Digital Service (GDS), which is leading the digital transformation of government, worked with the Office of the Public Guardian to build the digital service allowing users to make a lasting power of attorney. The new system removes the burden of filling out long paper forms and expedites the process. The agile method was used in the coding of the project by GDS software developers.

### D5.3 - Software quality



Governments can adopt agile processes for IT-specific projects, especially for software development. Agile has the following benefits:<sup>643</sup>

- **Prioritising user-centric, iterative development:** An iterative or spiral approach is used that seeks to deliver cyber and information capabilities earlier in their lifecycles and refine them in light of end-user feedback and evolving needs.
- **Aiming to fail fast/fail early:** At the start-up phase of a new project, overall approval is sought and is followed by the launch of a number of small experimental projects to prove or disprove hypotheses, allowing potential solutions to 'fail fast/fail early' and to ensure that the latest – but demonstrably feasible – technology is taken forward.
- **Shortening approval timelines:** New projects should move from initial concept to business case approval in an expedited timeframe.
- **Contracting for outcomes:** Once procurement is approved and potential suppliers are identified, contracts should focus on measuring success against goals and objectives, rather than prescriptive and atomised requirements with performance measures.
- **Ensuring proportionate security and assurance:** Security activities should not hinder rapid adoption of new technologies or hold up the process of implementing new software solutions.



- Review policies and processes regulating software updates and patching systems on the basis of risk assessments and criticality of services involved.

The private and public sectors should seek to implement processes to ensure that software is patched and updated at regular intervals. In most organisations and government departments, software maintenance is not the responsibility of the end-user but the IT department. The reliance on software means regular updates are required at the end-user level, as well as from IT managers. The implementation of these processes can require IT support if there are any errors or unanticipated consequences, despite the highly automated process of installing software updates.



The time between the discovery of a vulnerability in an operating system or application and the emergence of a way of exploiting that vulnerability is shortening, and is sometimes only a matter of hours.<sup>644</sup>

Updating software and patching vulnerable systems is necessary to reduce vulnerabilities and the risk of their exploitation. There are standard policies and processes for regularly updating software and patching systems. IT departments in businesses and companies should force the installation of software patches across enterprise systems on the second Tuesday of every month, according to Microsoft practices.<sup>645</sup> Other software products and services might require patching at different intervals. In the event of

disclosure of a major vulnerability, steps should be taken to remedy the situation based on a risk assessment and the criticality of the services involved.

Specific guidance and good practices on the topic of security management and patching is available from:

- **SANS Institute – A Practical Methodology for Implementing a Patch Management Process:**<sup>646</sup> The document offers a method for identifying, evaluating and applying security patches in a real-world environment, along with descriptions of tools that can be used to automate the process.
- **Symantec – Patch Management Best Practices:**<sup>647</sup> The document offers good practices based on industry experience for setting IT policies and/or developing patch-management solutions. The latter half of the document explores system administration and provides advanced administrative techniques for automating the process.
- **US-CERT – Recommended Practice for Patch Management of Control Systems:**<sup>648</sup> The document recommends patch-management practices for consideration and deployment by industrial control system asset owners.



#### Industry terminology – Patch Tuesday

'Patch Tuesday' or 'Update Tuesday' has been coined after Microsoft's use of the term and weekly release of software updates.<sup>649</sup> The term has become known in the IT and security industry to refer to the release of weekly software updates on Tuesdays. In response, many software exploits and vulnerabilities are observed shortly after the release of a patch, leading to the term 'Exploit Wednesday'.



- Continuously review software quality processes, updating and adapting these to the changing cybersecurity environment.

The continuous review of software quality typically occurs with the disclosure of a software vulnerability to a vendor selling a product or online service to customers. Vendors should present clear vulnerability policies to the public and provide those who discover vulnerabilities with contact information to report bugs and flaws in both software and hardware systems. Vulnerability disclosure measures and steps for vendors (e.g. businesses and companies), governments and users (e.g. consumers, customers and the public) are discussed under Dimension 5.7 on responsible disclosure.

## D5.3 - Software quality



There are often competing sources of information available to software developers. For instance, source documentation and user guides are freely available, depending on the operating system (e.g. Windows, Linux or OSX) and development tools being used. However, it is common for developers to first search online information resources (e.g. Stack Overflow) to fix general programming problems, which researchers have found can often lead to insecure code. Querying a search engine is another method of resolving a programming issue. Good practice, when viewed from a security perspective, is to rely on books for secure coding training and education.<sup>650</sup>

However, some malicious exploits are not mitigated by this method of continuous review. There a number of issues to address and steps that software vendors and government departments or agencies can take to build capacity in this area, including:

- **Ensure the timely patching of vulnerable systems.** As soon as a patch or update to a system becomes available, IT managers and end-users should install the patch to reduce the risk of known vulnerabilities.
- **Phase out legacy systems.** Legacy systems refer to those IT systems or software platforms no longer supported by the proprietary company (e.g. Windows XP and Windows Vista) and suffer from persistent zero-day exploits.
- **Conduct software auditing in development operations.** Tailored software applications require debugging to remove any exploitable code. By combining software development with security operations, DevOps continuously deliver software updates and monitor the effects of their patches and work through any regression issues or unintended consequences reported by end-users.
- **Conduct penetration testing (pen-testing) of software-intensive systems and networks.** Bug bounty programmes have proved effective ways to test defences in legacy systems and specific software systems. Organisations can host hack-a-thons and bug bounty programmes to engage with ethical hackers to find unknown vulnerabilities in systems.

## Additional resources



- Black, Paul E, Lee Badger, Barbara Guttman & Elizabeth Fong. 2016. Dramatically Reducing Software Vulnerabilities. NIST. NISTIR 8151.
- Pressman, Roger. 2009. Agile Development. Available online: <http://nlp.chonbuk.ac.kr/SE/ch05.pdf>
- Acar, Yasemin, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek & Christian Stransky. 2017. How Internet Resources Might Be Helping You Develop Faster but Less Securely. IEEE Security & Privacy 15(2): 50-60.
- ISO. 2011. ISO/IEC 25010:2011 – Systems and software engineering, systems and Qofware, Quality Requirements and Evaluation (SQuaRE), system and software quality models. Geneva, Switzerland: ISO.

## D5.4 – Technical security controls

### Overview

This factor focuses on how technical security controls for information systems can be implemented. Technical security controls are any repeatable steps performed by information systems to achieve a security goal. The implementation of technical security controls is essential to building cybersecurity capacity, since the absence of good practice may contribute to the proliferation of security vulnerabilities, which harm confidence and trust in the digital ecosystem. Technical security controls are technical or administrative safeguards or countermeasures designed to prevent, counteract or minimise data loss or unavailability due to security threats.<sup>651</sup>

Box 5.4 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 5.4: Steps for increasing technical security controls capacity (D5.4)

- Ensure that technical security controls are deployed in all relevant sectors and are based on established cybersecurity frameworks.
- Promote the use of antivirus software and network firewalls across devices.
- Ensure that ISPs establish policies for deployment of technical security controls as part of their services.
- Ensure that technical security controls within the public and private sectors are kept up to date, monitored and reviewed for effectiveness on a regular basis.
- Contribute to the development of technical standards by resourcing and investing in technical working groups.

### Capacity-building steps



- Ensure that technical security controls are deployed in all relevant sectors and are based on established cybersecurity frameworks.

Encouraging the adoption of secure computing practices is a responsibility for all actors in the private and public sectors. There are a number of good practices and technical security controls that can be implemented, including multi-factor authentication, digital certificates and application whitelisting. The following steps can be applied in any order to protect either public or private organisations:

- **Multi-factor authentication** (e.g. push notification, one-time password, SMS codes and biometrics) can be adopted by businesses operating in the e-commerce sector, as well as cloud computing operators with private user profiles containing sensitive information.
- **Application whitelisting** is the practice of approving certain applications that are permitted to execute on a host machine. This practice helps to stop the execution of malware, unlicensed software and other unauthorised software.

## D5.4 - Technical security controls

NIST's *Special Publication 800-167: Guide to Application Whitelisting* offers organisations an overview of the basics of whitelisting and explains how to plan and implement solutions throughout the security deployment lifecycle.<sup>652</sup>

- **Digital certificates**, or a ‘public key certificate’, are used in email encryption, code signing and e-signature systems to secure communications via encryption. Possession of a valid and signed digital certificate or public key allows for trust to form in a secure web of subjects (i.e. those who hold signed certificates) and owners (i.e. those issuing the certificates). Notably, public key certificates are used to secure Transport Layer Security (TLS) communications, which are part of the secure web protocol of HTTPS. TLS communications are described in more detail in section D5.5 on cryptographic controls.



The adoption and implementation of information security measures is a minimum requirement in order to mitigate cybersecurity risks to an organisation, business or institution. The top four strategies to mitigate targeted cyber intrusions have been shown to thwart 85% of typical intrusion techniques, as reported by the Australian Government.<sup>653</sup> They are:

1. Application whitelisting
2. Patching and updating applications and software
3. Patching and updating operating systems
4. Minimising administrative privileges.



- Promote the use of antivirus software and network firewalls across devices.

The use of antivirus software (i.e. protection against malware) and network firewalls (i.e. network monitoring tools) assists with the security of networked and wireless devices, including laptops, smartphones and printers. These anti-malware solutions should be promoted and used in the public and private sectors to protect online privacy and defend against social engineering techniques, botnet attacks and APTs. Any organisation can harden its defences by adopting the following approaches:

- **Apply antivirus solutions.** Single-user licences or full-enterprise support for antivirus software can be purchased from a range of suppliers and vendors. For instance, a range of antivirus products is offered by vendors specialising in different computing environments (e.g. Unix, Windows).
- **Enable endpoint security.** Endpoint security refers to devices connected to networks, typically wireless devices such as smartphones, tablets and laptops. Endpoint security products offer a range of measures to ensure that endpoints can securely connect while remaining compliant with technical standards.
- **Install networking monitoring tools.** Networking monitoring can be managed by software products looking for anomalous activity, which might

indicate the exploitation of a vulnerability. Many commercial-grade networks are defended by machine learning and artificially intelligent software. Organisations can then effectively monitor their systems by using network monitoring tools.



Antivirus computer software is used to prevent, detect, quarantine and remove malware. With the proliferation of cybersecurity threats, the term antivirus has broadened to include protections against malware, spyware, rootkits, keyloggers, backdoors, remote access trojans, and scam and spam tools. Next-generation antivirus solutions use machine learning to identify and respond to cybersecurity threats in real time.



- Ensure that ISPs establish policies for deployment of technical security controls as part of their services.

ISPs have a number of protective measures and technical security controls to combat cybersecurity threats, such as blacklisting botnets and spam servers.<sup>654</sup> These measures should be directed by national governments through open consultation with ISPs to ensure buy-in and a minimum standard in the industry. ISPs in many countries are legally obliged to comply with law enforcement agencies to monitor all or some of the metadata transmitted by the ISP (e.g. browsing history). Government could increase capacity in this area by working with ISPs and telecommunication industry regulators to implement upstream technical solutions for customers. In addition, national intelligence agencies often work with ISPs to enable the broad monitoring of all information traffic on domestic networks.



ISPs are organisations that provide services accessing and using the Internet via computer modems. ISPs can be commercial, community-owned, non-profit or privately owned businesses. Users typically connect to their ISP through a local network router connected by copper telephone wire, fiberoptic cables or Wi-Fi. Services provided by ISPs typically include Internet access, domain name registration, and email and web hosting,



- Ensure that technical security controls within the public and private sectors are kept up to date, monitored and reviewed for effectiveness on a regular basis.

As indicated in section D5.1 on adherence to standards, many cybersecurity and ICT standards are voluntary to implement, but can bring direct benefits to businesses and institutions choosing to implement them. Secondary benefits are also realised in the form of a healthier, stronger and more resilient cyberspace, where business can thrive and drive the economy.

## D5.4 - Technical security controls

However, training staff, maintaining valid certificates, undergoing audits and updating state-of-the-art standards are all costs for businesses and organisations. Consequently, while the benefits of implementing security controls are clear, incentivising industry to comply with standards may require policy incentives.

In order to build capacity across all sectors relying on IT systems, government can require that companies achieve a minimum level of compliance (e.g. a certificate of an ISO/IEC standard) before competing for public tenders. Dimension 5.1 on adherence to standards discusses in greater detail the Cyber Essentials programme as an example of how the public and private sectors can be encouraged to keep up to date, monitor and review cybersecurity measures.

Governments can also support the development of a cybersecurity insurance market, further details on which are presented in Section D5.6 on the cybersecurity marketplace. By reducing the premiums paid by compliant and certified organisations, market forces will drive more businesses to adopt good practices and seek to meet industry standards. A robust cybersecurity marketplace should aim to protect security, personally identifiable information and customer data.



- Contribute to the development of technical standards by resourcing and investing in technical working groups.

Technical security standards are developed by a range of SDOs. SDOs' approach to developing and updating standards normally relies on the input and contribution of technical working groups that gather industry experts, academics and national technical leads.

Governments may want to **contribute to technical standards bodies, working groups and study groups** in order to build capacity in the area of technical security standards. Working groups can be approached directly, typically by contacting the committee lead by email or online form. Technical security working groups include ISO/IEC committees,<sup>655</sup> ITU-T technical working groups<sup>656</sup> and IEEE-SA standards working groups.<sup>657</sup>

### Additional resources



- Northcutt, Stephen. 2009. Security Controls. SANS Technology Institute.
- Sedgewick, Adam, Murugiah Souppaya & Karen Scarfone. 2017. Guide to Application Whitelisting. NIST. 800-167.
- Australian Department of Defence. 2013. Top 4 strategies to mitigate targeted cyber intrusions: Mandatory requirements explained. Available online: <https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>

## D5.5 – Cryptographic controls

### Overview

This section focuses on the use of cryptographic controls to secure information, which may contain personal, private or commercially sensitive data that should be kept secure during transmission. According to NIST SP 800-33, there are technical foundations that underpin secure IT,<sup>658</sup> such as the ‘CIA’ triad of confidentiality, integrity and availability. The CIA triad is at the core of information security, and is defined as follows:

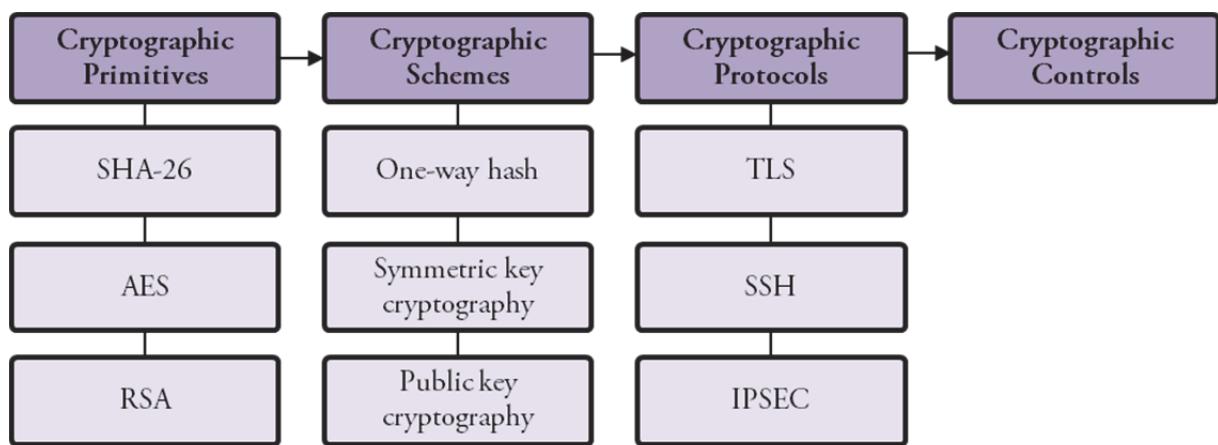
- Confidentiality refers to the security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorised data reads. Confidentiality covers data during storage, processing and transit.
- Integrity refers to the security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (i.e. the absence of any unauthorised alteration of the data) or system integrity (i.e. the system’s performance of its intended function in an unimpaired manner, free from unauthorised manipulation).
- Availability refers to the security objective that generates the requirement for protection against intentional or accidental attempts to perform unauthorised deletion of data, or otherwise cause a denial of service or data.

Cryptography is used to protect the confidentiality and integrity of information. Fundamentally, all cryptographic controls support the secure communication of data over open networks to prevent eavesdropping. This supports data security for information at rest and in transit.

A cryptographic protocol is a procedure carried out by two communicating parties to perform a security task.<sup>659</sup> The security task would not be possible without the constituent cryptographic schemes (e.g. public key encryption and signature schemes). Cryptographic primitives (i.e. low-level encryption algorithms) are the building blocks from which cryptographic protocols and controls are constituted. As such, they should be highly reliable, rigorously tested by the cryptologist community and assumed to be robust enough to withstand an error, collision or other security vulnerability. Figure 5.3 below shows the hierarchy of cryptographic controls.

## D5.5 - Cryptographic controls

**Figure 5.3: Hierarchy of cryptographic controls**



SOURCE: RAND Europe, based on ENISA (2014)

A number of capacity-building steps can assist governments to improve the implementation of cryptographic controls to secure information. Moreover, there are **steps for policymakers** to follow which identify prudent measures to adapt encryption and cryptographic controls to prepare for the advent of quantum computing. Box 5.5 provides an overview of the capacity-building steps which are discussed in more detail in the following pages.

### Box 5.5: Steps for improving cryptographic control capacity (D5.5)

- Ensure that up-to-date cryptographic techniques and controls are available for all sectors and users to protect data in transit or at rest, and that these meet international standards and guidelines.
- Ensure that state-of-the-art cryptographic control tools are deployed by web service providers to secure all communications between servers and web browsers.
- Promote widespread understanding of issues related to secure communications services.
- Ensure that public and private sector actors continuously assess and update encryption and cryptographic controls according to their objectives and priorities.

#### Capacity-building steps



- Ensure that up-to-date cryptographic techniques and controls are available for all sectors and users to protect data in transit or at rest, and that these meet international standards and guidelines.

In order to build capacity, **national standards organisations** should work with existing SDOs and closely follow the general guidelines for security professionals who implement cryptographic controls in the field. Moreover, national cryptographic leads should continually engage and collaborate with academic experts, foreign policy leads and wider stakeholder groups in order to research cryptographic controls. There are a

number of steps organisations can take to maintain secure information assets in line with international standards and guidelines, including:

- **Secure storage solutions:** There are proprietary solutions to prevent the theft of data from laptops and desktops by encrypting all user and systems files on a disk or volume. This protection is achieved by encrypting the entire Windows volume using BitLocker™. NIST has offered direction on the use of full-volume encryption in line with **Federal Information Processing Standard** Publication 140-2, which offers cryptographic security for both hardware and software components.<sup>660</sup>
- **Secure communications:** Encrypting emails using **Pretty Good Privacy (PGP)** allows for the secure signing, encrypting and decrypting of texts, emails, files, directories and whole-disk partitions, and helps increase the security of email communications.<sup>661</sup> PGP follows the OpenPGP standard (RFC 4880) for encrypting and decrypting data.<sup>662</sup>
- **Secure mobile devices:** Mobile devices require security measures to meet the abovementioned CIA triad underpinning IT. NIST SP 800-124 Rev 1 offers organisations the ability to centrally manage the security of mobile devices against a variety of threats.<sup>663</sup>



Implementers of cryptographic and security protocols for specific applications (e.g. instant messaging) should refrain from altering and optimising well-studied protocols to suit their specific service. Minor changes can permit larger, unforeseen vulnerabilities to emerge. Unless implementers are willing to re-evaluate the security proofs (mathematical proofs of security achieved by the protocol) for the protocol at the same time as making the amendment, then these should not be altered.

Below are resources on general cryptographic studies, which outline best practices or common pitfalls when interpreting or implementing cryptographic controls. The following are useful sources of information for all sectors to assist with the protection of data in transit or at rest:

- **ENISA's recommended cryptographic measures – securing personal data:**<sup>664</sup> The document addresses protection measures applied to protect sensitive and/or personal data. These measures can be implemented by users with a basic knowledge of information security and use of cryptographic techniques to protect personal data.
- **ENISA's study on cryptographic protocols:**<sup>665</sup> The report focuses on the current status of cryptographic protocols and encourages further research, given the lack of new protocols. This is compared to the work on cryptographic primitives and schemes – while these can be deemed secure, the underlying protocol may still contain vulnerabilities. The report covers protocols for

## D5.5 - Cryptographic controls

wireless, mobile communications and banking (e.g. Bluetooth, WPA/WEP<sup>666</sup> authentication protocols, ZigBee wireless protocol, EMV<sup>667</sup>) and specific environments focusing on cloud computing.

- **ENISA's algorithms, key size and parameters report (2014):**<sup>668</sup> The report is a reference document providing a set of guidelines to decision makers, in particular specialists and those designing and implementing cryptographic solutions for personal data protection in the public and private sectors. It builds on the 2013 report, which addressed the need for a minimum level of requirements for cryptography across EU Member States.
- **NIST Cryptographic Standards and Guidelines Development Process (NISTIR 7977):**<sup>669</sup> The document describes the principles, processes and procedures that drive cryptographic standards and guidelines development at NIST. It serves as the basis for NIST's future cryptographic standards and guideline-development efforts.

Specific guidance should be sought if organisations are seeking to implement innovative solutions where new standards do not exist. Subscribing to the news alerts of the technical working group at the SDO is one method of obtaining the latest information. If an organisation wishes to engage with emerging cryptographic protocols for custom solutions, organisations should be aware of the principles underpinning the development of all cryptographic standards and act according to them.



In order to achieve broadly accepted cryptographic standards and guidelines, the following principles have been adapted from NIST's cryptographic development processes:

- **Transparency:** All parties should have access to essential information and documentation relating to the development of standards and guidance.
- **Openness:** Participation is open to all interested parties.
- **Balance:** By weighing up the views of various stakeholder groups, the process of developing standards is intended to be built on consensus and result in the production of strong and interoperable standards.
- **Integrity:** The coordinating body should serve as an impartial technical authority and value objectivity while avoiding conflicts of interest.
- **Global acceptability:** Cryptographic standards for controls are intended to be globally accepted by a wide range of stakeholder groups.
- **Usability:** The implementation of standards should minimise the demands on the user and limit the adverse consequences of human error and equipment failure.
- **Continuous improvement:** In order to stay current, the cryptographic community is encouraged to identify weaknesses, vulnerabilities or other deficiencies, and patch them where possible.
- **Innovation and IP:** Cryptographic standards should be unencumbered by intellectual property claims.



- Ensure that state-of-the-art cryptographic control tools are deployed by web service providers to secure all communications between servers and web browsers.

Cryptographic primitives, schemes and protocols should be employed by web service providers to secure communication between servers and web browsers. The relevant standard for secure web services is HTTPS,<sup>670</sup> which enables a connection encrypted by TSL. HTTPS provides bi-directional encryption of communications between a client and server, which protects against eavesdropping, tampering or forging of the contents of the communication.<sup>671</sup>

The majority of standards and guidelines are voluntary, rather than being mandated by law. Standards organisations often produce formal guidelines to promote the use of strong cryptography using open and transparent processes. Despite their voluntary status, cryptographic standards and guidelines should be supported, promoted and implemented by relevant stakeholder groups – including governments, businesses and industry – to secure communication networks and personal or sensitive information where possible. All stakeholders can support initiatives to use HTTPS to protect page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

## D5.5 - Cryptographic controls

**HTTPS Everywhere Project**

HTTPS Everywhere is a collaboration between the Tor Project and the Electronic Frontier Foundation.<sup>672</sup> HTTPS Everywhere is a Firefox, Chrome and Opera extension that encrypts data in transit and communications with many major websites, making browsing the Internet more secure.

Many sites on the web offer some limited support for encryption over HTTPS. For instance, websites may default to unencrypted HTTP, or fill encrypted pages with links that circle back to the unencrypted site. The HTTPS Everywhere extension for a web browser fixes these problems using a technology that rewrites requests to these sites to HTTPS.

In order to support HTTPS, all relevant stakeholders in the public and private sector should enable HTTPS on their websites. Asking site operators to add HTTPS is one method of encouraging its usage. More information and instruction on how server operators can add HTTPS is available in online guides.<sup>673</sup>

**Let's Encrypt<sup>674</sup>**

Let's Encrypt (LE) is a free, automated and open certificate authority run by the Internet Security Research Group. LE provides digital certificates to enable users to create HTTPS (using TLS or Secure Sockets Layer (SSL)) for websites, for free and in a user-friendly way. The key principles behind LE are that it is:

- Free – anyone who owns a domain name can use LE to obtain a trusted certificate.
- Automatic – software running on a web server can interact with LE to obtain a certificate, securely configure it for use, and automatically take care of renewal.
- Secure – LE aims to serve as a platform for advancing TLS security best practices.
- Transparent – all certificates issued or revoked are publicly recorded and available for inspection.
- Open – the automatic issuance and renewal protocol is published as an open standard that others can adopt.



- Promote widespread understanding of issues related to secure communications services.

Esoteric information controls and protocols can have impacts on human rights ('the right to privacy'), free speech and civil rights. Moreover, the continual adoption of new and innovative technologies has sparked debates on net neutrality, mass surveillance and intellectual property rights. Consequently, the media has a role to play in shaping public debate and broadcasting proposed changes which affect society. Further

information on the role of media as regards cybersecurity and the surrounding public debate is provided under section D2.5 of this document.

Furthermore, to contribute to public discourse and debate, government has a role to play in the raising of awareness and education levels among the general public. This can be done through awareness-raising campaigns, and education and training programmes. Further information on such initiatives is provided under Dimension 3 (Cybersecurity education, training and skills) of this document.



#### **Public debate over standards: FBI v. Apple**

Following the terrorist attack in San Bernardino in December 2015, the FBI pursued the personal data on the locked iPhone of one of the shooters. The FBI demanded that Apple create a software tool to bypass the passcode lock on the iPhone to enable the authorities to gain access to the encrypted data on the phone.

Public debate ensued, as the legal issue between Apple and the US federal government touched on questions of security, privacy and human rights. The balance between national security concerns and electronic privacy is an issue that is ultimately presided over by courts, but the role played by the media and informed public debate should not be discounted.



- Ensure that public and private sector actors continuously assess and update encryption and cryptographic controls according to their objectives and priorities.

Private and public sector actors should assess the applicability of cryptographic standards and be prepared to migrate to new, secure standards once patches and updates are released. Many cryptographic protocols were designed decades ago and can suffer from legacy issues. An incorrect implementation of legacy cryptographic controls with new applications can create the emergence of unforeseen security vulnerabilities. Security proofs (i.e. mathematical proofs of security achieved by the protocol) are necessary at every layer of cryptographic controls to ensure sensitive data is not exposed during transmission. For this reason, cryptographic protocols should be aligned with an organisation's privacy policy and service offerings, as well as its business objectives and priorities.

The public and private sectors can plan for updates to cryptographic standards and guidelines, including ongoing and future work, by keeping abreast of announcements posted on SDO websites. For instance, the following SDOs announce their final publications online:

- **IEC:** The IEC provides email alerts and RSS feeds to keep members, technical committees and customers informed of activities and any changes to standards.<sup>675</sup>
- **IEEE:** The IEEE hosts its standards online where they can be browsed with a valid subscription. Users can sign up for email alerts. However, the GET Program gives the private and public sectors access to IEEE standards at no cost.<sup>676</sup>

## D5.5 - Cryptographic controls

- **IETF:** Overseeing the TLS protocol, the IETF announces updates through their email notifications on working group lists.<sup>677</sup>
- **NIST:** The Computer Security Resource Center has provided access to NIST's cybersecurity and information security projects, publications, news and events.<sup>678</sup>

By using these SDO notification services, organisations can stay informed about ongoing security developments and ensure that systems and configurations are up to date. They can also use these services to stay abreast of long-term work to improve cryptographic standards.

The following case study of the TLS cryptographic protocol is illustrative of the legacy issues affecting protocols today. Updates to the protocol might mitigate and remediate any security vulnerabilities. This is another reason why organisations should continuously assess and update their encryption standards.



### TLS: an example of a cryptographic protocol and its current challenges

The TLS protocol was initially designed to secure communication between a web browser and a website. Given **the legacy of the protocol**, which is based on SSL v1.0 from 1993, the TLS protocol is now widely used in applications such as email, instant messaging and VoIP (voice-over-IP), along with Internet browsers, to secure information exchanges from being intercepted and read by eavesdroppers. The two distinct layers of the protocol have not changed over time – these are the TLS record protocol and the TLS handshake protocol (a process of negotiation that sets parameters of a communications channel established between two entities before normal communication begins).

The **IETF is the standardisation body** for the TLS protocol and a long-established working group whose main role is to develop TLS v1.3.<sup>679</sup> Overall, the protocol suffers from **increasing levels of complexity, backwards compatibility and a widening scope**. Mindful of these challenges, the working group aims to encrypt as much of the handshake as possible to both active and passive attackers, consider privacy issues and minimise gratuitous changes to TLS extensions and cipher suites.



Security research on the topic of cryptographic **protocols is limited** in volume when compared to studies on cryptographic primitives and schemes.<sup>680</sup> The design and verification of cryptographic protocols are difficult to execute, as the underlying mathematical and computational proofs can be corrupted if improperly implemented. Moreover, security and network protocol designers have historically attempted to produce cryptographic protocols with mixed success.<sup>681</sup> Consequently, there have been **few attempts to design and verify new cryptographic protocols**, despite many updated versions of existing protocols. The field of cryptographic protocol design and development would **benefit from contributions from national cryptographic leads** to technical working groups in international standards bodies.

## Additional resources



- ENISA. 2014. Study on cryptographic protocols. Heraklion, Greece: ENISA.
- NIST. 2016. IST Cryptographic Standards and Guidelines Development Process. Gaithersburg, MD, US: National Institute of Standards and Technology Internal Report 7977.
- ENISA. 2014. Algorithms, key size and parameters report 2014. Heraklion, Greece: ENISA.
- ENISA. 2013. Recommended cryptographic measures – Securing personal data. Heraklion, Greece: ENISA.
- ENISA. 2014. Study on cryptographic protocols. Heraklion, Greece: ENISA.
- Stoneburner, Gary. 2001. Underlying Technical Models for Information Technology Security. Gaithersburg, MD, US: National Institute of Standards and Technology.

## D5.6 – Cybersecurity marketplace

### Overview

This factor focuses on the cybersecurity marketplace, specifically the availability and development of competitive cybersecurity technologies, and the availability and uptake of cybersecurity insurance. A thriving cybersecurity marketplace is underpinned by an innovative technology sector, a robust cybersecurity insurance market and excellent indigenous cyber products for export. In order to develop capacity in the sector, governments need to work in concert with industry leaders, and insurance brokers and companies, in order to stimulate the nascent market. Box 5.6 provides an overview of capacity-building steps for increasing national capacity in this area.

### Box 5.6: Steps for improving cybersecurity marketplace capacity (D5.6)

- Promote the development of an innovative cyber insurance market and products capable of adapting to emerging risks, standards and practices while addressing the full scope of cyber harm.
- Encourage information sharing among actors participating in the cyber insurance market.
- Ensure that governments support cybersecurity insurance so that the market offers first-party and third-party insurance.
- Encourage the development of cyber insurance products suitable for SMEs.
- Promote the development by domestic providers of cybersecurity products in accordance with market needs and with a view to mitigating dependency on foreign cybersecurity technologies.

### Capacity-building steps



- Promote the development of an innovative cyber insurance market and products capable of adapting to emerging risks, standards and practices while addressing the full scope of cyber harm.

Cybersecurity insurance is designed to mitigate losses from data breaches, cyber-attacks, network downtime and interruptions to business.<sup>682</sup> Cybersecurity insurance is a standalone product available to transfer some of the risk of a cybersecurity breach from a business to an insurer. Cyber insurance products are a growth sector for many insurers that see the exponential increase in mobile and digital devices, coupled with greater risks of data breaches and exposure to losses, theft and fraud. The aims of a robust cybersecurity insurance market are as follows:

- Promote the adoption of preventative measures in order to increase insurance coverage.
- Encourage the implementation of industry standards and guidelines to reduce premiums.

Protecting businesses against cybersecurity incidents goes beyond safeguarding data and networks against attack. For businesses, cyber incidents are closely linked to reputation and regulatory compliance. Insurance enables businesses to enhance their financial stability by transferring risks and potential litigation costs to a third party.<sup>683</sup>



The threat of a single, cascading and catastrophic cybersecurity incident has fuelled concerns that cyber insurers do not know the full extent of the risks they face.<sup>684</sup> A major attack or digital blackout could send losses spiralling and the effects would be felt nationally, perhaps globally, and dampen the impact of the expansion of the cybersecurity insurance market.

In order to build national capacity in this area, government can support the development of a vibrant and innovative domestic cybersecurity market both for insurance products and for cybersecurity services and products. For example, governments may promote through R&D the development of risk-modelling approaches to sustain the growth of cyber insurance for emerging areas and needs. For example, several intangible assets that are vulnerable from a cybersecurity perspective remain completely or partially uninsured in contemporary markets, including reputational harm and intellectual property theft.<sup>685</sup>



From the perspective of cyber insurance opportunities, there is a lack of experienced insurance personnel with cybersecurity backgrounds. This affects the ability of insurers to create risk models, develop sound pricing strategies and establish loss reserves. Without analytical advances, insurance companies will struggle to help potential business clients assess vulnerabilities in line with their coverage gaps, minimum requirements and regulatory processes.<sup>686</sup>

Furthermore, governments may encourage adoption of and compliance with international standards by public and private sector companies and institutions, as discussed in section D5.1 of this document on international standards. This may facilitate entry onto the national insurance market by international companies looking to expand their client base to certified organisations and companies in a particular country.



- Encourage information sharing among actors participating in the cyber insurance market.

Depending on the national context, there is varying access to reporting mechanisms, either mandatory or voluntary, for organisations to share information about cybersecurity incidents. In order to build capacity in this area, national governments could:

## D5.6 - Cybersecurity marketplace

- **Increase information sharing among insurers and financial institutions.** Due to the risk transfer between insurers and businesses, these risk reports could be shared more widely with other financial institutions and market regulators to offer better reporting on the risk carried by organisations.
- **Consider the reporting regime for cybersecurity incidents.** National governments could develop an anonymised cyber incident data repository to foster the voluntary sharing of data about breaches, business interruption events and industrial control system attacks that is needed for enhanced risk mitigation. For example, governments could consider appointing CERTs and government cybersecurity operations centres in order to generate accurate reports without duplication.



### Reporting of cyber incidents in the US

The US DHS has a cyber incident reporting mechanism where members of the public can report cyber incidents, phishing, malware and other vulnerabilities they may encounter. The incident reports are collected by the US Computer Emergency Readiness Team (US-CERT), which also offers advice to vendors, government users, and home and business users on staying safe online. Malware and vulnerability reports can also be shared with DHS over email.

- **Share information with cybercrime agencies.** In order to secure the marketplace, the most severe cases of vulnerabilities resulting in identity theft, fraud and cyber-enabled crime can be forwarded onto cybercrime agencies. Incidents can be then actioned according to police processes to investigate the crime and whether to pursue criminal charges.



### ACORN – Australia's cybercrime online reporting system

The Australian Cybercrime Online Reporting Network (ACORN) is a secure reporting and referral system for cybercrime and online incidents.<sup>687</sup> These kinds of incidents may be in breach of Australian law, and certain reports will be directed to Australian law enforcement and government agencies for further investigation. The ACORN reporting system is designed to capture information on common types of cybercrime include hacking, scams, fraud, identity theft, attacks on computer systems, and illegal or prohibited online content. A similar system with information-sharing capabilities could be established to support risk transfer (i.e. cybersecurity insurance).



- Ensure governments support cybersecurity insurance so that the market offers first-party and third-party insurance.

Governments can facilitate the development of cybersecurity insurance by devising a regulatory framework that does not hinder private sector insurers in bringing their products to market. The following steps may guide both governments and insurers in their efforts to foster an insurance market:

- **State the minimum cybersecurity standards with which organisations should comply.** Industry standards should first be set by market regulators. Cyber insurers could then emphasise specific risk-management steps in the pricing of their cyber coverage.
- **Insurers should develop risk tables for pricing insurance products.** The development of new cybersecurity insurance markets requires insurers and industry executives to consider cyber risk assessments and market forces in the pricing of cybersecurity insurance products.
- **Review certifications and accreditations obtained by the organisation.** Applicants for cyber insurance could demonstrate the steps they have taken to be secure (prevention), vigilant (detection) and resilient (loss control and recovery) in their cyber-related operations.<sup>688</sup> These three features could raise the level of cybersecurity competence in organisations.



With more companies increasingly reliant on digital technology, exposure to business interruptions is becoming ever more significant. Recent years have also seen growing concern about the vulnerability of industrial control systems, which are used to monitor or control processes in industrial and manufacturing sectors. Despite common misunderstanding, cybersecurity insurance is not only for those operating in the IT domain but could also be relevant for almost all companies across most economic sectors.

Cybersecurity insurance providers offer different coverage levels so that businesses are protected in the event of data loss or a cybersecurity incident. Tiers of cover vary depending on the insurance provider and the maximum cover limit. Depending on the insurance product, first-party insurance can cover damage to data, business interruptions and reputational harm.<sup>689</sup> Interruption to business and subsequent loss of reputation can be a significant cause of economic loss and competitive disadvantage for businesses.

Cybersecurity insurance is a standalone product offered with different premium prices, inclusions and exclusions, and loss limits. Overall, many insurers report finding it difficult to price cyber insurance due to the difficulty of calculating loss exposure given the relative lack of data on the extent of losses.<sup>690</sup> Moreover, rapidly changing technology and threats mean that insurers struggle to keep pace.

Given the impacts of data breaches in terms of reputational damage, loss of consumer confidence and regulatory fines, there is a need for cybersecurity insurance products to account for these risks to businesses in economic terms. However, it should be noted that risk modelling in these areas is still in development, and that cyber insurers, for the most part, have yet to add these issues to their portfolio of work.<sup>691</sup>



In the US, only a few cybersecurity insurance products offer protection against cyber-attacks where the primary effect causes physical damage or bodily harm. The possibility of such an attack on a power grid, water supply, transport network or other CNI is of increasing concern to insurers, governments, industry leaders and the public.<sup>692</sup>

### D5.6 - Cybersecurity marketplace



- Encourage the development of cyber insurance products suitable for SMEs.

In order to develop the insurance market for SMEs, government policymakers and industry leaders should call on insurers and insurance brokers to **simplify their insurance products and offerings**. SMEs have little capacity to dedicate time to understanding complex insurance products. Simplification may contribute to increased uptake of cybersecurity insurance in the marketplace as a whole. Such a move would also ensure that firms understand the extent of their coverage against cyber-attacks.<sup>693</sup>



Many companies have not signed up for cybersecurity insurance and purchase policies, despite analysts' predictions of strong future growth in the insurance sector.<sup>694</sup> This may be for a number of reasons, including:

- The perceived high cost of insurance;
- Confusion among buyers over the coverage offered;
- Lack of standardisation of cyber insurance policies (with vast differences between the US and European markets);
- Uncertainty in relation to legal requirements;
- Uncertainty over whether a company will suffer a cyber-attack costly enough to warrant purchasing insurance.



- Promote the development by domestic providers of cybersecurity products in accordance with market needs and with a view to mitigating dependency on foreign cybersecurity technologies.

The presence of a strong domestic marketplace creating indigenous cybersecurity products and technologies is a sign of an innovative and dynamic national cyber industry. In order to achieve this end-state, governments can promote their cybersecurity products and stimulate domestic innovation. This will alleviate dependency on foreign cybersecurity technologies. Governments can take the following capacity-building steps:

- **Establish a multidisciplinary taskforce.** This taskforce could be a consortium between the public and private sectors, tasked with identifying options for a joint cyber offering. The taskforce may also look to contribute to the development of the country's national cybersecurity strategy, with a view to embedding activities aimed at fostering market growth.
- **Embrace emerging opportunities in high-growth sectors.** Cybersecurity markets that show promise for future development could be identified and prioritised through co-funded public-private business incubators. Promising markets may include threat intelligence services, software auditing and escrow

services, high-security datacentres, machine learning and artificial intelligence network monitoring tools, and cybersecurity operations centres).

- **Reduce reliance on foreign cybersecurity services and products.** The reliance on cybersecurity products and services from abroad creates risks in relation to the security of supply, quality control, security assurance and potentially even espionage.



#### **US federal agencies ban Kaspersky software**

In September 2017, the US government moved to ban the use of a Russian brand of security software by federal agencies amid concerns the company has ties to state-sponsored cyber espionage activities.<sup>695</sup> The homeland security secretary issued a binding directive ordering that federal civilian agencies identify Kaspersky Lab software on their networks, which must be removed within 90 days, unless otherwise instructed. These links to foreign intelligence agencies are damaging for Kaspersky in terms of their brand and their financial position.

- **Establish cybersecurity industry sectors, alliances and regional clusters.** For instance, the **ITU Regional Cybersecurity Centre (RCC)** is a physical centre hosted by an ITU member state to act as the regional ITU focal point for cybersecurity issues, and to deliver ITU's cybersecurity services to all partner countries (e.g. Oman ITU RCC to cater for the cybersecurity needs of the Gulf region).<sup>696</sup> In Europe, the **NATO CCDCOE** is a multinationally funded institution that trains and educates leaders and specialists from NATO countries in cyber defence. The CCDCOE also assists in doctrine development, identifies lessons learned, improves interoperability, and tests and validates concepts through experimentation.

#### Additional resources



- Friedman, Sam and Adam Thomas. 2017. Demystifying cyber insurance coverage. Deloitte University Press.
- US Department of Homeland Security. 2017. Cybersecurity Insurance. Available online: <https://www.dhs.gov/cybersecurity-insurance>
- Merrey, Paul, Matthew Smith, Matthew Martindale and Arturs Kokins. 2017. Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age. KPMG International Cooperative.

## D5.7 – Responsible disclosure

### Overview

This factor focuses on the existence of responsible disclosure policies and on the national capacity to implement, review and update these policies as required. Responsible disclosure frameworks should be employed to ensure that vulnerability disclosure occurs in a coordinated manner while achieving a number of other goals, including the following:

- Ensure that vulnerabilities can be eliminated effectively and efficiently for all parties, employing minimal time and resources.
- Minimise the risk to customers from vulnerabilities and provide them with sufficient information to assess the security of a vendor's products.
- Minimise tensions between competing incentives among stakeholders involved in a vulnerability disclosure procedure.
- Provide the research community with the information necessary to develop the tools, methods and techniques to identify, manage and reduce the risk posed by vulnerabilities.

Capacity building in this area should be seen as the result of a distributed, iterative effort at the level of individual organisations, companies and institutions. These efforts may entail activities such as those presented in Box 5.7.

### Box 5.7: Steps for increasing responsible disclosure capacity (D5.7)

- Encourage vendors to use vulnerability disclosure frameworks and consult the most recent industry standards, documentation and good practice guides.
- Encourage vendors and service providers to develop a clearly structured vulnerability disclosure policy, based on internal organisational processes, to address bug and vulnerability reports.
- Ensure that responsible disclosure processes are set for all stakeholders involved (product vendors, discoverers, users and the public).
- Encourage vendors and service providers to commit to refrain from legal action against parties disclosing vulnerabilities.
- Ensure that technical details of vulnerabilities are published and advisory information is disseminated according to individual roles and responsibilities.
- Continuously review responsible disclosure policies on the basis of the needs of stakeholders affected.
- Share responsible disclosure frameworks internationally and contribute to the development of best practices in this area.

### Capacity-building steps



- Encourage vendors to use vulnerability disclosure frameworks and consult the most recent industry standards, documentation and good practice guides.

Although competing definitions exist, in the context of cybersecurity the term ‘vulnerability’ encapsulates any bug, flaw, mistake, event or behaviour in a computer-based system or solution that may be exploited or lead to an increased risk of a security exploit.<sup>697</sup> Given the widespread prevalence of vulnerabilities in many systems, collectively they pose a significant threat to users and organisations. It is vital that appropriate processes and procedures are put in place to protect, handle and make use of information on vulnerabilities within vendor organisations. Vulnerability disclosure frameworks should be used to ensure the proper reporting, coordination and publication of information about a vulnerability, bug or flaw and its resolution and remediation. Such a framework allows for protection against vulnerabilities in products or online services, while ensuring that all stakeholders understand their roles, responsibilities and obligations within the process.

Questions exist within the information security community as to how, when and by whom a vulnerability is disclosed and to whom the disclosure is made. These questions are resolved in the following capacity-building steps, which outline good practices for vendors, organisations and nations looking to develop their cybersecurity capacity. There are four different types of vulnerability disclosure approaches which determine how vendors are notified of a flaw or bug. These are:

- **Non-disclosure:** The discoverer keeps the vulnerability secret and does not report it to the vendor or to public authorities. The discoverer may sell on the vulnerabilities to third parties.
- **Full disclosure:** The vulnerability is disclosed to the public in a complete format, without distinguishing between the actors to be notified. In this approach, vendors may not have sufficient time or warning to resolve the vulnerability or issue patches or security updates, which leaves open the possibility of attackers exploiting vulnerable systems.
- **Responsible disclosure:** The responsible disclosure of vulnerabilities involves approaching the vendor with the intention of resolving the vulnerability in a sustainable way and mitigating the possibility of a follow-on attack on vulnerable systems. This method of disclosure varies in practice, since a number of actors and stakeholders should be notified to remediate the vulnerability. Simply put, in a responsible disclosure scenario the public is only notified once a solution and mitigation are made available by a vendor. This chapter focuses on building capacity in the area of responsible disclosure.
- **Limited disclosure:** Similar to responsible disclosure, limited disclosure occurs when only specific parties are informed about a vulnerability. In this method, a third-party coordinator (e.g. a mediator) could lead the vulnerability disclosure process and relationships between discoverer, vendor, government and the public.

## D5.7 - Responsible disclosure



Inappropriate disclosure of a vulnerability may hinder resolution of the vulnerability by a vendor, and may also give attackers hints to exploit a weakness. That is why vulnerability disclosure should be carried out following a framework with distinct policies, disclosure deadlines, resolution schedules, acknowledgement reports and effective communication with the discoverer.

The goals of vulnerability disclosure frameworks include the following:

- Ensuring that identified vulnerabilities are addressed through to resolution;
- Minimising the cybersecurity risks from vulnerabilities;
- Providing users with timely and useful information to evaluate the risks posed by vulnerabilities;
- Setting the roles for all stakeholders and promoting positive communication and coordination.

There are a number of vulnerability disclosure frameworks that should be consulted in the establishment of a vulnerability reporting system, including:

- **ISO/IEC 29147 (vulnerability disclosure):<sup>698</sup>** The first edition of ISO/IEC 29147:2014 provides guidelines for the disclosure of potential vulnerabilities in products and online services. It details the methods a vendor should use to address issues related to vulnerability disclosure. The standard outlines how vendors should receive disclosure reports and disseminate resolution information on their products or online services. The standard also provides information on how vendors should design policies and share relevant processes with the public and discoverers so that they are able to disclose vulnerabilities to the vendor. The standard is freely available online (see information box below).
- **ISO/IEC 30111 (vulnerability handling processes):<sup>699</sup>** ISO/IEC 30111:2011 provides guidelines for how to process and resolve information on potential vulnerability in a product or online service. This standard targets organisations who want to strengthen their internal processing to deal with vulnerability reports they receive. At the time of publication, the standard is under review by ISO working groups in the IT security techniques section.
- **ENISA's good practice guide on vulnerability disclosure:<sup>700</sup>** Published in 2016, the CERT Capability team at ENISA, in consultation with RAND Europe, delivered a good practice guide on vulnerability disclosure. The study team worked with the EU, its Member States, the private sector and European experts to develop advice and recommendations on good practice based on a mixed-methods approach comprising a literature review and a number of interviews.



ISO/IEC offer a select list of free standards available for download online. All the standards are protected by copyright; however, they allow vendors to consult international best practices without any financial cost.<sup>701</sup>



- Encourage vendors and service providers to develop a clearly structured vulnerability disclosure policy, based on internal organisational processes, to address bug and vulnerability reports.

A vendor should create an overall vulnerability disclosure policy. To help efficiently manage the vulnerability lifecycle, a vendor's vulnerability disclosure policy should be mirrored in their internal organisational processes. Vendors may choose to publicise only part of their internal vulnerability disclosure process, as the policy may contain sensitive proprietary information. Vendors can develop their vulnerability reporting and resolution capacity by implementing a number of clearly defined steps, such as:

- **Developing a vulnerability disclosure policy:** This should be a brief statement aimed at presenting a company's philosophy and approach to vulnerability disclosure. It should demonstrate the organisation's commitment to the safety of customers and the overall market.



The distinction between software and hardware products is rarely relevant in the disclosure of vulnerabilities.

- **Developing a legal position for discoverers:** This entails a statement articulating an organisation's position with regard to the prosecution of vulnerability finders and researchers who act in good faith. This statement should unambiguously clarify which vulnerability research activities would lead to legal action, and which are accepted.
- **Developing the capacity to receive and disseminate vulnerability information:** A vendor should have the requisite capacity to receive and disseminate vulnerability information. A point of contact (POC) should be appointed within a vendor organisation to action this process.
- **Receiving vulnerability reports from either an internal or external source:** Internal and external actors should be able to engage with the vulnerability POC.



A range of options are available for enabling the submission of vulnerability reports. Some organisations provide a secure web form, while others encourage submission via email using suitable security precautions (e.g. PGP encryption).

- **Acknowledging receipt of the report:** The POC should issue an acknowledgement of the vulnerability in the form of a report to the discoverer.

## D5.7 - Responsible disclosure



Make sure that a confirmation of receipt email is issued once a vulnerability report has been issued. This will assure discoverers that their submissions have been received and will enhance transparency of communication, as well as ensuring adherence to specified vulnerability disclosure timelines.

- **Internally verifying the vulnerability with a proof of concept:** Internal developers and engineers should liaise with the POC to verify the vulnerability in the stated system by demonstrating a proof of concept.
- **Developing a resolution:** Developers and engineers should then fix, patch and update the vulnerable system to ensure its proper functioning for users.
- **Disseminating information on vulnerabilities and advice on addressing these:** Vendors should publicly disclose the vulnerability and offer a fix, patch or update to the affected system. Depending on the vendor and products offered, they may or may not have accurate lists of users to notify of the vulnerability.
- **Engaging in post-resolution activities:** The vendor should collect feedback from users about the update, patch or fix and its ability to remediate the vulnerability.



### Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: base, temporal and environmental. The base group represents the intrinsic qualities of a vulnerability, the temporal group reflects the characteristics of a vulnerability that change over time, and the environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The base metrics produce a score ranging from 0.0 to 10.0, which can then be modified by scoring the temporal and environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides a collection of examples of vulnerabilities scored using CVSS v3.0.

CVSS is owned and managed by FIRST.Org, Inc., a US-based non-profit organisation whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all rights and interest in CVSS, it licenses it to the public for free use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST does, however, require that any individual or entity using CVSS give proper attribution by stating, where applicable, that CVSS is owned by FIRST and used with permission. Furthermore, FIRST requires as a condition of use that any individual or entity which publishes scores conforms to the guidelines described in this document and provides both the score and the scoring vector so others can understand how the score was derived.



- Ensure that responsible disclosure processes are set for all stakeholders involved (i.e. product vendors, discoverers, users and the public).

The range of stakeholders potentially involved in vulnerability disclosures is particularly complex and characterised by stakeholder groups that may have diverging goals.<sup>702</sup> In the absence of clear procedures and processes, this may result in vulnerability disclosures that are highly inconsistent and reflect the perspective of those parties that have the best ability and resources to control the process. The main stakeholder groups to be considered when focusing on vulnerabilities are:

- **Discoverers:** Less frequently, these actors are referred to as 'reporters'. These are typically technical security researchers who investigate and identify vulnerabilities. Discoverers may also have malicious intent and seek to exploit or make profit from identified vulnerabilities.
- **Vendors:** These are the producers or suppliers of products that potentially contain vulnerabilities. Vendors may be also discoverers.

## D5.7 - Responsible disclosure

- **Users:** These are individuals and organisations using products with vulnerabilities.
- **Mediators:** These are organisations that may help facilitate a disclosure process between the discoverer and the vendor.

In addition, other actors involved in the field of vulnerability disclosures are:

- **Government:** Governmental agencies may play a role as a discoverer, vendor, user or mediator. In addition to this, the government is also in charge of designing the national legal framework regulating disclosure issues.
- **Media:** Media outlets may report and disclose information on vulnerabilities.

While the adoption of frameworks for coordinated vulnerability disclosure pertains primarily to private sector actors, a country's government and its agencies have a significant role to play in the field of responsible disclosure. Government departments, agencies and institutions often run their own vulnerability disclosure programmes. Governments may focus their efforts on:

- Regulating the legal landscape to encourage vulnerability reporting;
- Regulating the government's internal decision-making process with regard to vulnerabilities discovered by governmental agencies and contractors.

When a government agency or one of its contractors discovers or purchases a so-called zero-day vulnerability (i.e. a vulnerability unknown to the general public and software developers), they are faced with a choice. The government may responsibly disclose the vulnerability and contribute to the securing of cyberspace, or it may decide to withhold this information for reasons of national security. Furthermore, governments may opt to use zero-day vulnerabilities to their advantage, for example to undertake law enforcement, intelligence or military operations.

No consensus best practice yet exists as to how a government can regulate this. The experience of the US presented below suggests that governments may wish to establish a clearly defined decision-making process accompanied by clear decision-making criteria to be used for assessing on a case-by-case basis the preferred approach to handling vulnerabilities. This process should require government-wide compliance and be subject to periodic reviews. Once such a process has been established, publicly disclosing its high-level structure and the criteria used to inform the decision-making process could enhance transparency and foster trust in the mechanisms set in place among vendors, researchers and the general public.



### The US Vulnerability Equities Process<sup>703</sup>

The US government has established a process to determine whether information about zero-day vulnerabilities discovered by the government and its contractors should be disclosed or withheld. The US Vulnerability Equities Process (VEP) was established across 2008 and 2009 by a working group with representatives of the US intelligence community, Attorney General, Federal Bureau of Investigation, DoD, Department of State, Department of Energy, and DHS.

According to information available in the public domain, the US VEP does not establish any hard and fast rule for determining which approach to take, but rather prescribes a high-level, interagency decision-making process. Commenting on the criteria used to inform the decision-making process, the then-White House Cybersecurity Coordinator, Michael Daniel, stated that a number of questions were investigated each time a zero-day vulnerability was being assessed. These questions focus on identifying:

- The extent to which a vulnerable system is in use in the Internet infrastructure;
- The threat associated with leaving a vulnerability unpatched;
- The extent to which the vulnerability is needed to obtain intelligence;
- The likelihood of other parties discovering the vulnerability and whether other parties may be aware of or exploiting this information;
- The extent to which the government may use the vulnerability to its advantage for a limited amount of time;
- The extent to which the vulnerability may be patched or mitigated.

In addition to the above government-specific roles, government agencies and vendors may also stimulate a controlled investigation of vulnerabilities in their systems through bug bounty programmes, vulnerability purchase programmes and vulnerability rewards programmes. Through these initiatives, vendors or governmental agencies assign financial rewards to researchers who successfully identify vulnerabilities within their systems or products.



- Encourage vendors and service providers to commit to refrain from legal action against parties disclosing vulnerabilities.

In any vulnerability disclosure framework, a statement should be included to reassure vulnerability discoverers acting in good faith that they will not face legal action. In addition to goodwill on the side of software developers and vendors, the national legal framework should also ensure adequate protection and transparency rules on this matter.

Legal frameworks may present several challenges hindering the investigation, responsible disclosure and subsequent resolution of software vulnerabilities. A 2015 study by ENISA suggests that legal frameworks across EU Member States and the US have either established or left unaddressed several grey areas concerning the legal liability of discoverers of software vulnerabilities. These grey areas may then be used by vendors against vulnerability researchers, often on the grounds of abuse of intellectual property rights

## D5.7 - Responsible disclosure

and breach of licensing. While no established guideline exists as to how a legal balance could be established, a solution may be found in the adoption of exemptions from laws regulating licensing and copyright for security researchers acting in good faith.



If no specific legislation on vulnerability disclosure has been adopted, case law and the interpretation of the existing legal framework will influence the practice of vulnerability disclosure within a country. To ensure transparency and provide the researcher community and general public with clarity as to how this matter is being handled by the judiciary, prosecution guidelines or jurisprudence overviews should be published. The publication of these documents could also encourage a homogeneous approach to the issue of legal prosecution for vulnerability disclosure within the country.



### DMCA Research Exemptions

The United States Digital Millennium Copyright Act (DMCA) prohibits any circumvention of controls protecting copyrighted materials. This legal provision would effectively prohibit any vulnerability research activity entailing reverse engineering, access to obfuscated code, etc.

In October 2016, the Librarian of Congress authorised an exemption to the DMCA which effectively grants researchers a right to investigate vulnerabilities in consumer devices, so long as this is done within the boundaries of other laws (e.g. Computer Fraud and Abuse Act) and through a suitable setup and testing environment. The exemption currently covers all user devices 'primarily designed for use by individual consumers'.



- Ensure that technical details of vulnerabilities are published and advisory information is disseminated according to individual roles and responsibilities.

The technical details of a vulnerability and its remediation and mitigation strategies are typically published as an advisory communication. The advisory communication describes the vulnerability and includes information about the systems affected. The audience for the advisory is generally users who are affected and require sufficient information to make informed risk decisions about the product or online service, and how to remediate or mitigate the vulnerability. Advisories can also be issued more widely (e.g. to the public and other vendors).

A consistent format for an advisory issued by vendors should become a convention in order to improve understanding of the advisory. When creating an advisory, affected vendors should consider providing both human and machine-readable formats (e.g. a CSV file). These can be issued to other vendors and mediators (e.g. national CERTs). Further, the use of cryptographic verification is important for security patches and updates to software systems to enable users to validate their authenticity. Accepting a

counterfeit advisory may introduce a vulnerability into a system, compromise a product's security measures and potentially harm users.



### Interdependency of systems

Many vulnerable components are part of complex systems that interact with other products in some way. Online services and digital products can often share underlying source code with other products, as well as similar software libraries, and the same network protocols or file formats. This interdependency between products is essential to understanding the extent of a vulnerability which may persist in many vendors' products. Moreover, vendors or users may be uncertain as to which products are affected.

Vendors may need to work closely with a coordinator to release the advisory to other relevant vendors. These vendors might use interdependent systems and suffer from the same underlying vulnerability. Other vendors then may undergo their own internal assessment to verify the vulnerability with a proof of concept. If the vulnerability is found to exist in their interdependent systems, then users will receive additional advisory information.



- Continuously review responsible disclosure policies on the basis of the needs of stakeholders affected.

Vulnerability disclosure policies should be reviewed on a regular basis. Vendors can review their internal and public-facing policies after the remediation of a vulnerability and the publication of an advisory to users and other vendors. Vendors should review current industry standards on vulnerability disclosure practices and handling techniques (e.g. ISO/IEC 29147 and ISO/IEC 30111) as well as considering any new publications on international good practices based on lessons learned and key stakeholder consultations. Reviews might consider challenges in the following areas, which are flagged in prior studies as particular areas vendors have found challenging in the past:<sup>704</sup>

- **Vendor disclosure policies:** The vendor should review how it would like to be contacted (e.g. email, phone or web form), the secure communications it offers, how it sets communication expectations, valuable information to collect about a vulnerability, out-of-scope services and the tracking of reports.
- **Formalised coordinator support:** When there is a major vulnerability affecting multiple vendors, a coordinator should attempt to coordinate their release with multiple vendors. If vendors nominate more than one coordinator to be involved, then this relationship should be clarified by nominating a leader in order to reduce confusion and duplication of effort.
- **Post-resolution activities:** By engaging in post-resolution activities, vendors can seek feedback from users about remediation strategies and check whether

## D5.7 - Responsible disclosure

these worked well, or were found to be incomplete or have unintended consequences. If this process is ineffective, vendors should formalise this process by allowing users to contact the vendor (i.e. implement an online feedback form, email template or phone contact line to evaluate a specific mitigation strategy).



- Share responsible disclosure frameworks internationally and contribute to the development of best practices in this area.

Good practices in the area of vulnerability disclosure have been outlined in the literature on the topic (e.g. ENISA's framework and ISO/IEC standards listed above). The following good practices may assist vendors in their interactions with discoverers.

- **Use existing documentation.** To avoid having to develop capability from scratch, existing documents on good practices should be consulted by various stakeholders to implement new or existing initiatives (e.g. ISO/IEC standards).
- **Ensure good communication.** Vendors should appoint a liaison officer to act as a conduit for discoverers to report vulnerabilities.
- **Maintain a policy on vulnerability disclosure.** Vendors should have a policy in place that sets out the process for responding to and resolving vulnerability reports. The policy should indicate to reporters what information they need to provide.
- **Issue confirmation receipts.** As mentioned above, vendors should acknowledge receipt of vulnerability reports and provide the discoverer with indicative timelines for their resolution.
- **Disseminate information to users.** Users should be informed about how to best protect themselves in light of the disclosure of a vulnerability.
- **Issue timelines.** Vendors should issue an indicative timeline for resolving vulnerabilities on a case-by-case basis.
- **Allow for flexibility in reporting and disclosure.** There is no one-size-fits-all solution. It is therefore imperative to tailor the vulnerability report to specific details that pose risks.

In order to contribute to these good practice guides and disclosure frameworks, governments, large vendors and businesses should allocate funding for research and participating in the development of standards (see Dimension 5.1 – Adherence to standards). In order to share these standards internationally, they should be released to the public in order to drive adoption, increase impact and enable small businesses and start-ups with limited resources to implement good practices.

## Additional resources



- ENISA. 2015. Good Practice Guide on Vulnerability Disclosure: From challenges to recommendations. Heraklion, Greece: ENISA.
- ISO. 2014. ISO/IEC 29147:2014. Information technology, security techniques, vulnerability disclosure. Geneva, Switzerland: ISO.
- ISO. 2013. ISO/IEC 30111:2013. Information technology, security techniques, vulnerability handling processes. Geneva, Switzerland: ISO.
- EPIC. 2017. Vulnerabilities Equities Process. Washington, DC: Electronic Privacy Information Center.



## Resources and publications

---

This section presents references to publications and resources that may be consulted or used to further knowledge and understanding of cybersecurity capacity building in a given issue area. Resources and publications are presented according to the 5 dimensions of the GCSCC CMM model upon which this guide builds:

- D1 – Strategy and resilience
- D2 – Society and culture
- D3 – Cybersecurity education, training and skills
- D4 – Law and regulation
- D5 – Standards, controls and technologies.

Factor-specific publications and resources are listed at the end of each of the factor-specific sections contained in the previous chapters of this document.

## D1. Cybersecurity policy and strategy

(ISC)<sup>2</sup> (International Information System Security Certification Consortium). 2017. 'Certified Cyber Forensics Professional.' As of 13 November 2017: <https://www.isc2.org/Certifications/CCFP>

AfricaCERT. N.d. 'About Us.' As of 9 November 2017: <https://www.africacert.org/home/about-us/>

APCERT (Asia Pacific Computer Emergency Response Team). 2017a. 'Event Calendar.' As of 1 November 2017: <http://www.apcert.org/events/calendar/index.html>

\_\_\_\_\_. 2017b. 'Mission Statement.' As of 9 November 2017: <https://www.apcert.org/about/mission/index.html>

Bada, Maria, & Sadie Creese. 2014. *Cyber security awareness campaigns: Why do they fail to change behavior?* Oxford: Global Cyber Security Capacity Centre. As of 17 July 2017: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf>

Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell & Elizabeth Phillips. 2014. *Computer Security Incident Response Teams (CSIRTs): An Overview.* Oxford: Global Cyber Security Capacity Centre. As of 17 July 2017: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf>

Bandos, Tim. 2017. 'The Five Steps of Incident Response.' *DigitalGuardian*, 27 July. As of 13 November 2017: <https://digitalguardian.com/blog/five-steps-incident-response>

Brown, Cameron SD. 2015. 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice.' *International Journal of Cyber Criminology* 9(1): 55.

Cichonski, Paul, Tom Millar, Tim Grance & Karen Scarfone. 2012. *Computer security incident handling guide.* NIST. 800-61. As of 13 November 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Cole, Jennifer, & Edward Hawker. 2014. 'Emergency Services Communications: Resilience for the Twenty-First Century.' As of 17 July 2017: [https://rusi.org/sites/default/files/201405\\_op\\_emergency\\_services\\_communications.pdf](https://rusi.org/sites/default/files/201405_op_emergency_services_communications.pdf)

Creasey, Jason. 2013. *Cyber Security Incident Response Guide.* CREST. As of 13 November 2017: <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>

CSIS (Center for Strategic & International Studies). 2017. 'Analysis.' As of 1 November 2017: <https://www.csis.org/analysis/securing-cyberspace-through-publicprivatepartnerships>

CTO (Commonwealth Telecommunications Organisation). 2015. *Commonwealth approach for developing national cybersecurity strategies.* As of 1 November 2017: <http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf>

CyberGreen. 2017. 'Home page.' As of 1 November 2017: [www.cybergreen.net](http://www.cybergreen.net)

Davis, John II, Martin C Libicki, Stuart E Johnson, Jason Kumar, Michael Watson & Andrew Karode. 2016. *A framework for programming and budgeting for cybersecurity*. Santa Monica, Calif.: RAND Corporation. TL-186. As of 1 November 2017: <https://www.rand.org/pubs/tools/TL186.html>

Defence Academy of the United Kingdom. 2017. 'Defence Cyber School.' As of 9 November 2017: <https://www.da.mod.uk/colleges-schools/technology-school/defence-cyber-school>

DLA Piper. 2017. 'Data protection laws around the world.' As of 17 July 2017: <https://www.dlapiperdataprotection.com/index.html>

Dutch Ministry of Defence. 2012. 'The Defence Cyber Strategy.' As of 10 November 2017: [https://ccdcoc.org/strategies/Defence\\_Cyber\\_Strategy\\_NDL.pdf](https://ccdcoc.org/strategies/Defence_Cyber_Strategy_NDL.pdf)

EC-Council. 2017a. 'About Us.' As of 13 November 2017: <https://www.eccouncil.org/about/>

\_\_\_\_\_. 2017b. 'Handle Security Incidents: Become an ECIH.' As of 13 November 2017: <https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/>

Emergency Communications Preparedness Centre. 2016. 'Federal Financial Assistance Reference Guide.' As of 17 July 2017: [https://www.911.gov/pdf/2016\\_ECPC\\_Reference\\_Guide.pdf](https://www.911.gov/pdf/2016_ECPC_Reference_Guide.pdf)

ENISA (European Union Agency for Network and Information Security). 2006. 'A step-by-step approach on how to set up a CSIRT.' As of 17 June 2017: [https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at\\_download/fullReport](https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport)

\_\_\_\_\_. 2009. 'National Exercise - Good Practice Guide.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide>

\_\_\_\_\_. 2012. 'National Cyber Security Strategies: An Implementation Guide.' As of 17 July 2017: <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>

\_\_\_\_\_. 2014a. 'An evaluation Framework for National Cyber Security Strategies.' As of 17 June 2017: [https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at\\_download/fullReport](https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport)

\_\_\_\_\_. 2014b. 'National/governmental CERTs: ENISA's recommendations on baseline capabilities.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities>

\_\_\_\_\_. 2014c. 'Report on Cyber Crisis Cooperation and Management.' 6 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/ccc-study>

\_\_\_\_\_. 2014d. 'Study on cryptographic protocols.' 21 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols>

\_\_\_\_\_. 2015. 'Critical Information Infrastructures Protection approaches in EU.' July. As of 17 June 2017: <https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf>

- \_\_\_\_\_. 2016a. 'Good Practice Guide on National Cyber Security Strategies.' As of 17 June 2017: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/good-practice-guide-on-national-cyber-security-strategies>
- \_\_\_\_\_. 2016b. 'Strategies for incident response and cyber crisis cooperation.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation>
- \_\_\_\_\_. 2017. 'ENISA Threat Landscape Report 2016.' 8 February. As of 17 June 2017: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>
- EU Council. 2008. 'On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.' 23 December. As of 17 July 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>
- European Commission. 2010. 'European Programme for Critical Infrastructure Protection.' 17 August. As of 1 November 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260>
- \_\_\_\_\_. 2015. 'Risk Management Capability Assessment Guidelines.' As of 17 July 2017: [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)&from=EN)
- Federal Emergency Management Agency. 2015. 'Fact sheet: Disaster emergency communications.' As of 17 July 2017: <https://www.fema.gov/media-library-data/1440617086804-f6489d2de59dddeba8bebcb9b4d419009/DEC%20June%2015.pdf>
- FIRST (Forum of Incident Response and Security Teams). 2017a. 'Home page.' As of 1 November 2017: [www.first.org](http://www.first.org)
- \_\_\_\_\_. 2017b. 'Mission Statement.' As of 9 November 2017: <https://www.first.org/about/mission>
- Fischer, Eric A. 2014. 'Cybersecurity Issues and challenges: in brief.' 12 August. As of 17 July 2017: <https://fas.org/sgp/crs/misc/R43831.pdf>
- Friedland, Carsten, & Monika Muylkens, eds. 2009. *ITU e-Government Implementation Toolkit*. Geneva: ITU. As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/app/e-gov.html>
- GCSCC (Global Cyber Security Capacity Centre). 2014. 'Cyber security capability maturity model (CMM) - V1.2.' Oxford, 15 December. As of 17 July 2017: [https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201\\_2\\_0.pdf](https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf)
- \_\_\_\_\_. (Global Cyber Security Capacity Centre). 2017. *Cyber security capability maturity model for Nations (CMM): Revised Edition*. Oxford: University of Oxford. As of 13 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition\\_09022017\\_1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf)
- GIAC Certifications (Global Information Assurance Certification). 2017a. 'GIAC Certified Handler (GCIH).' As of 13 November 2017: <https://www.giac.org/certification/certified-incident-handler-gcih>

- \_\_\_\_\_. 2017b. 'GIAC Information Security Certification - Program Overview.' As of 13 November 2017: <https://www.giac.org/about/program-overview>
- \_\_\_\_\_. 2017c. 'GIAC Response and Industrial Defense (GRID).' As of 13 November 2017: <https://www.giac.org/certification/response-industrial-defense-grid>
- Goodwin, Cristin Flynn, & J Paul Nicholas. 2013. *Developing a National Strategy for Cybersecurity*. Microsoft. As of 1 November 2017: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi>
- Government of Japan. 2015. *The Basic Policy of Critical Infrastructure Protection*. Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)
- Government of the Netherlands. 2013. *International Security Strategy*. As of 9 November 2017: <https://www.government.nl/documents/policy-notes/2013/06/21/international-security-strategy>
- ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). N.d. 'Training Available Through ICS-CERT.' As of 1 November 2017: <https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT>
- Intel. 2015. 'Understanding cyberthreat motivations to improve defences.' As of 17 July 2017: <https://www.mcafee.com/us/resources/deflect-targeted-attacks/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf>
- ITU. 2009. 'Cybersecurity Guide for Developing Countries.' As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf>
- \_\_\_\_\_. 2011. *ITU National Cybersecurity Strategy Guide*. Geneva, Switzerland: ITU. As of 1 November 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>
- Joint Forces Command. N.d. 'About Us.' UK Government. As of 9 November 2017: <https://www.gov.uk/government/organisations/joint-forces-command/about>
- Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. Gaithersburg, MD: NIST. As of 1 November 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- Klimberg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication. As of 17 July 2017: <https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>
- Minářík, Tomáš. 2016. *National cyber security organisation: Czech Republic*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdcoe.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_CZE\\_032016.pdf](https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf)
- Mitchell, Ronald K, Bradley R Agle & Donna J Wood. 1997. 'Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts.' *Academy of management review* 22(4): 853-86.

MITRE. 2017. 'Cybersecurity Resources.' As of 1 November 2017:  
<https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources>

NATO (North Atlantic Treaty Organization). 2017. 'NATO Cyber Defence Fact Sheet.' As of 9 November 2017:  
[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2017\\_05/20170515\\_1705-factsheet-cyber-defence-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/20170515_1705-factsheet-cyber-defence-en.pdf)

NATO Industry Cyber Partnership. 2016. 'Objectives and Principles.' As of 9 November 2017:  
<http://www.nicp.nato.int/objectives-and-principles/index.html>

Natural Resource Governance Institute. 2015. 'Legal Framework: Navigating the Web of Laws and Contracts Governing Extractive Industries.' March. As of 17 July 2017:  
[https://resourcegovernance.org/sites/default/files/nrgi\\_Legal-Framework.pdf](https://resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf)

NCSC (National Cyber Security Centrum). 2015. 'GCCS CSIRT Maturity Quick Scan.' As of 1 November 2017: <https://check.ncsc.nl/>

\_\_\_\_\_. 2016. *Common cyber attacks: reducing the impact.* As of 13 November 2017:  
[https://www.ncsc.gov.uk/content/files/protected\\_files/guidance\\_files/common\\_cyber\\_attacks\\_ncsc.pdf](https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf)

\_\_\_\_\_. 2017. 'Public Private Partnerships.' 9 June 2017. As of 9 November 2017:  
<https://www.ncsc.nl/english/Cooperation/public-private-partnership.html>

NISC (National Center of Incident readiness and Strategy for Cybersecurity). 2014. 'The Basic Policy of Critical Information Infrastructure Protection.' 19 May. As of 17 July 2017:  
[http://www.nisc.go.jp/eng/pdf/actionplan\\_ci\\_eng\\_v3.pdf](http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf)

NIST. 2011. *Information Security.* NIST Special Publication 800-39. As of 17 July 2017:  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

\_\_\_\_\_. 2014. 'Framework for Improving Critical Infrastructure Cybersecurity.' 12 February. As of 17 July 2017:  
[https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-0212\\_14.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-0212_14.pdf)

OAS (Organization of American States). 2015. 'Best Practices for Establishing a National CSIRT.' April. As of 17 July 2017:  
<https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>

\_\_\_\_\_. 2016. *Best Practices for Establishing a National CSIRT.* As of 10 November 2017:  
<https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>

OECD. 2012a. *Cybersecurity policy making at a turning point.* As of 1 November 2017:  
<http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>

\_\_\_\_\_. 2012b. 'High Level Risk Forum: Strategic Crisis Management.' 13-14 December. As of 17 July 2017:  
[http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/HLRF\(2012\)3&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/HLRF(2012)3&docLanguage=En)

- \_\_\_\_\_. 2013. 'The OECD Privacy Framework.' As of 17 July 2017: [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
- \_\_\_\_\_. 2014. *OECD Recommendation on Digital Government Strategies*. As of 1 November 2017: <http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm>
- Oliker, Olga, Lynn E Davis, Keith Crane, Andrew Radin, Celeste Ward Gventer, Susanne Sondergaard, James T Quinlivan, Stephan B Seabrook, Jacopo Bellasio & Bryan Frederick. 2016. *Security Sector Reform in Ukraine*. Rand Corporation.
- Osula, Anna-Maria. 2015. *National cyber security organisation: United Kingdom*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdcoe.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_UK\\_032015\\_0.pdf](https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf)
- Osula, Anna-Maria, & Kadri Kaska. 2013. *National Cyber Security Strategy Guidelines*. Tallinn: NATO CCD COE Publication. As of 17 July 2017: [https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSS%20Guidelines\\_2013.PDF](https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSS%20Guidelines_2013.PDF)
- Pernik, Piret, Jesse Wojtkowiak & Alexander Verschoor-Kirss. 2016. *National cyber security organisation: United States*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdcoe.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_USA\\_122015.pdf](https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf)
- RAND Corporation. 2017. 'Military Doctrine.' As of 9 November 2017: <https://www.rand.org/topics/military-doctrine.html>
- Ready. N.d. 'Risk Assessment.' As of 1 November 2017: <https://www.ready.gov/risk-assessment>
- Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle & Pablo Rodriguez. 2013. *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) : unclassified summary*. Santa Monica, Calif.: RAND Corporation. RR-286. [http://www.rand.org/pubs/research\\_reports/RR286.html](http://www.rand.org/pubs/research_reports/RR286.html)
- Robles, Rosslyn John, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park & J Lee. 2008. 'Common threats and vulnerabilities of critical infrastructures.' *International journal of control and automation* 1(1): 17-22.
- SANS Digital Forensics and Incident Response. 2017. 'GIAC Computer Forensics Certifications.' As of 13 November 2017: <https://digital-forensics.sans.org/certification>
- Simon, Tobby. 2017. 'Critical Infrastructure and the Internet of Things.' January. As of 17 July 2017: [https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46\\_0.pdf](https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf)
- Suter, Manuel. 2007. 'A Generic National Framework For Critical Information Infrastructure Protection (CIIP).' August. As of 27 July 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>
- UK Cabinet Office. 2010. 'Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.' March. As of 17 July 2017:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/62504/strategic-framework.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf)

UK Centre for the Protection on National Infrastructure. 2017. 'Critical National Infrastructure.' As of 17 July 2017: <https://www.cpni.gov.uk/critical-national-infrastructure-0>

UK Government. 2015. *National Security Strategy and Strategic Defence and Security Review 2015*. Cm 9161. As of 1 November 2017: <https://www.eda.europa.eu/docs/default-source/procurement/uk-national-security-strategy-and-strategic-defence-security-review-2015.pdf>

\_\_\_\_\_. 2016. 'National Cyber Security Strategy 2016 to 2021.' 11 September 2017. As of 10 November 2017: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

\_\_\_\_\_. N.d.-a. 'The Defence Science and Technology Laboratory (Dstl).' As of 9 November 2017: <https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory>

\_\_\_\_\_. N.d.-b. 'More about R-Cloud.' As of 9 November 2017: <https://rcloud.dstl.gov.uk/about>

UK Government House of Commons Defence Committee. 2012. 'Defence and Cyber-Security: Sixth Report of Session 2012-13.' As of 10 November 2017: <https://publications.parliament.uk/pa/cm201213/cmselect/cmdefence/106/106.pdf>

UK Ministry of Defence. 2017a. 'Defence Cyber Protection Partnership.' 26 October. As of 9 November 2017: <https://www.gov.uk/government/collections/defence-cyber-protection-partnership>

\_\_\_\_\_. 2017b. 'Single departmental plan: 2015 to 2020.' As of 9 November 2017: <https://www.gov.uk/government/publications/mod-single-departmental-plan-2015-to-2020/single-departmental-plan-2015-to-2020>

UK National Cyber Security Centre. 2016. 'We work for government and the Critical National Infrastructure.' 2 October. As of 17 July 2017: <https://www.ncsc.gov.uk/information/we-work-government-and-critical-national-infrastructure>

UNCTAD. 2015. 'Information Economy Report.' As of 17 July 2017: [http://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf)

United Nations General Assembly. 2010. '64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures' *Resolution adopted by the General Assembly on 21 December 2009 64(5)*. As of 1 November 2017: [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=A/RES/64/211](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211)

US Department of Defence. 2015. 'The DOD Cyber Strategy.' As of 10 November 2017: [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

US Department of Homeland Security. 2013. 'Information Technology Sector-Specific Plan: An Annex to the NIPP 2013'. As of 17 July 2017: <https://www.dhs.gov/publication/nipp-ssp-information-technology-2016>

- \_\_\_\_\_. 2014. *National Emergency Communications Plan*. As of 13 November 2017: [https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan\\_October%2029%202014.pdf](https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf)
- \_\_\_\_\_. 2017. 'Cyber Storm: Securing Cyber Space.' 21 July. As of 9 November 2017: <https://www.dhs.gov/cyber-storm>
- Wamala, Frederick. 2009. *ITU National Cybersecurity/CIIP Self-Assessment Tool*. Geneva, Switzerland: ITU. As of 1 November 2017: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf>
- \_\_\_\_\_. 2011. *ITU National Cybersecurity Strategy Guide*. Geneva: ITU Publication. As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs//ITUNationalCybersecurityStrategyGuide.pdf>
- Yang, Jing, Geoffrey Qiping Shen, Lynda Bourne, Christabel Man-Fong Ho & Xiaolong Xue. 2011. 'A typology of operational approaches for stakeholder analysis and engagement.' *Construction management and economics* 29(2): 145-62.

## D2. Cyber culture and society

Action Fraud. N.d. 'About Us.' As of 9 November 2017:  
<https://www.actionfraud.police.uk/about-us/who-we-are>

APWG (Anti-Phishing Working Group). 2017. 'About APWG.' As of 9 November 2017:  
<https://www.antiphishing.org/about-APWG/>

Ball, James, Julian Borger & Glenn Greenwald. 2013. 'Revealed: how US and UK spy agencies defeat internet privacy and security.' 21 June. As of 7 July 2017:  
<https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

Berejka, Marc, & Ari M Schwartz. 2011. 'Cybersecurity, Innovation and the Internet Economy.' As of 17 July 2017: [http://www.nisc.go.jp/eng/pdf/actionplan\\_ci\\_eng\\_v3.pdf](http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf)

Bertot, John Carlo, Paul T Jaeger & Derek Hansen. 2012. 'The impact of polices on government social media usage: Issues, challenges, and recommendations.' *Government information quarterly* 29(1): 30-40.

Better Internet for Kids. N.d. 'Home page.' As of 1 November 2017:  
<https://www.betterinternetforkids.eu/>

CERT. 2017. 'STEPfwd.' As of 1 November 2017: <https://stepfwd.cert.org/lms>

Correia, John, & Deborah Compeau. 2017. 'Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA.' *Proceedings of the 50th Hawaii International Conference on System Sciences*.

CSIAC (Cyber Security & Information Systems Information Analysis Center). 2017. 'Cyber Awareness Videos.' As of 1 November 2017: <https://www.csiac.org/series/cyber-awareness-videos/>

CyberSecurity Malaysia. 2017. 'CyberSAFE.' As of 31 October 2017: <http://www.cybersafe.my/en/>

ENISA. 2007. *Information security awareness initiatives: Current proactive and the measurement tools*.

\_\_\_\_\_. 2013. 'National-level Risk Assessments: An Analysis Report.' As of 17 June 2017:  
<https://www.enisa.europa.eu/publications/nlra-analysis-report>

\_\_\_\_\_. 2014a. 'An evaluation Framework for National Cyber Security Strategies.' As of 17 June 2017:  
[https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at\\_download/fullReport](https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport)

\_\_\_\_\_. 2014b. 'Methodologies for the identification of Critical Information Infrastructure assets and services.' As of 17 June 2017:  
<https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis>

\_\_\_\_\_. 2015a. 'Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches.' December. As of 17 June 2017:  
<https://www.enisa.europa.eu/publications/cybersecurity-information-sharing>

- \_\_\_\_\_. 2015b. 'Security and Resilience in eHealth Infrastructures and Services.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services>
- \_\_\_\_\_. 2017. 'ENISA Cyber Security Month.' As of 1 November 2017: <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month>
- European Commission. 2014. 'Working Document on surveillance of electronic communications for intelligence and national security purposes.' As of 17 July 2017: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf)
- \_\_\_\_\_. N.d.-a. 'Misleading advertising.' As of 17 July 2017: [http://ec.europa.eu/consumers/consumer\\_rights/unfair-trade/false-advertising/index\\_en.htm](http://ec.europa.eu/consumers/consumer_rights/unfair-trade/false-advertising/index_en.htm)
- \_\_\_\_\_. N.d.-b. 'Overview on Binding Corporate rules.' As of 9 November 2017: [http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm)
- European Cyber Security Month. N.d. 'Home page.' As of 9 November 2017: <https://cybersecuritymonth.eu/>
- European Parliament. 2016a. 'General Data Protection Regulation.' As of 17 July 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en>
- \_\_\_\_\_. 2016b. 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46.' *Official Journal of the European Union (OJ)* 59: 1-88. As of 9 November 2017: [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)
- FBI (Federal Bureau of Investigation). N.d. 'Safe Online Surfing.' As of 1 November 2017: <https://sos.fbi.gov/>
- FBI IC3 (Federal Bureau of Investigation Internet Crime Complaint Center). N.d. 'Home page.' As of 9 November 2017: <https://www.ic3.gov/about/default.aspx>
- Financial Industry Regulatory Authority. 2015. 'Report on Cybersecurity Practices.' As of 17 July 2017: <https://www.finra.org/file/report-cybersecurity-practices>
- FOSI (Family Online Safety Institute). 2017. 'Home page.' As of 1 November 2017: [www.fosi.org](http://www.fosi.org)
- FTC (Federal Trade Commission). N.d. 'OnGuardOnline.' As of 1 November 2017: <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>
- G7 Cyber Expert Group. 2016. 'G7 fundamental elements for cyber security.' As of 1 July 2017: <https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security>
- Gant, Jon P., ed. 2008. *Electronic government for developing countries*. Geneva: ITU. As of 17 July 2017: [http://www.itu.int/ITU-D/cyb/app/docs/e-gov\\_for\\_dev\\_countries-report.pdf](http://www.itu.int/ITU-D/cyb/app/docs/e-gov_for_dev_countries-report.pdf)

Gasser, Urs, Nancy Gertner, Jack L Goldsmith, Susan Landau, Joseph S Nye, David O'Brien, Matthew G Olsen, Daphna Renan, Julian Sanchez & Bruce Schneider. 2016. *Don't Panic: Making Progress on the "Going Dark" Debate*. Harvard University: The Berkman Center for Internet & Society. As of 9 November 2017: <https://cyber.harvard.edu/pubrelease/dont-panic/Dont%20Panic%20Making%20Progress%20on%20Going%20Dark%20Debate.pdf>

GLACY (Global Action on Cybercrime). 2014. 'Good practice study: Cybercrime reporting mechanisms.' September. As of 17 July 2017: <https://rm.coe.int/168030287c>

Goolsby, Rebecca. 2013. 'On Cybersecurity, Crowdsourcing, and Social Cyber-Attack.' 4 March. As of 17 July 2017: <https://www.wilsoncenter.org/publication/cybersecurity-crowdsourcing-and-social-cyber-attack>

Government of Canada. 2017. 'Get Cyber Safe.' 17 October. As of 1 November 2017: <https://www.getcybersafe.gc.ca/index-eng.aspx>

Government of Japan. 2015. *The Basic Policy of Critical Infrastructure Protection*. Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)

Hodge, Neil. 2012. 'The EU: Privacy by Default.' *In-House Persp.* 8: 19. As of 17 July 2017: <https://www.ibanet.org/Document/Default.aspx?DocumentUid=83F52EA7-E19A-4E4B-A2E5-A77EDC535F6B>

ICC (International Chamber of Commerce). 2015. 'ICC Cyber Security Guide for Business.' As of 17 July 2017: <https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/>

iKeepSafe. 2017. 'Home page.' As of 1 November 2017: [www.ikeepsafe.org](http://www.ikeepsafe.org)

Interpol. 2017. 'Cybercrime.' As of 1 November 2017: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>

ITU. 2009. 'Guidelines for Policy Makers on Child Online Protection.' As of 17 July 2017: <http://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf>

\_\_\_\_\_. 2014. 'The quest for cyber confidence.' As of 17 July 2017: <http://handle.itu.int/11.1002/pub/80b7079c-en>

IWF (International Watch Foundation). 2017. 'Home page.' As of 1 November 2017: [www.iwf.org.uk](http://www.iwf.org.uk)

Kick, Jason. 2014. 'Cyber Exercise Playbook.' November. As of 17 July 2017: [http://www.mitre.org/sites/default/files/publications/pr\\_14-3929-cyber-exercise-playbook.pdf](http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)

Microsoft. 2013. 'Privacy by Default.' As of 17 July 2017: [http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy\\_by\\_default.pdf](http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy_by_default.pdf)

Ministère de l'Intérieur. N.d. 'Portail officiel de signalement des contenus illicites de l'Internet.' As of 9 November 2017: <https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil/input.action>

National Center for Missing & Exploited Children. 2017. 'Educators.' As of 1 November 2017: <http://www.netsmartz.org/Educators>

NICCS. N.d. 'Home page.' As of 31 October 2017: <http://niccs.us-cert.gov>

NIST. 2017. 'NICE Cybersecurity Workforce Framework.' 19 October. As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

\_\_\_\_\_. N.d. 'National initiative for cybersecurity education (NICE).' As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice>

NOVA Labs. 2017. 'Cybersecurity 101.' As of 1 November 2017: [www.pbs.org/wgbh/nova/labs/lab/cyber/1/1](http://www.pbs.org/wgbh/nova/labs/lab/cyber/1/1)

Nye, Joseph S. 2014. 'The regime complex for managing global cyber activities.'

OECD (Organisation for Economic Co-operation and Development). 2007. 'OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.' As of 9 November 2017: <http://www.oecd.org/internet/ieconomy/38770483.pdf>

\_\_\_\_\_. 2008. 'OECD Recommendations on the Protection of Critical Information Infrastructures.' As of 17 July 2017: <http://www.oecd.org/sti/ieconomy/ciip.htm>

\_\_\_\_\_. 2013. 'The OECD Privacy Framework.' As of 17 July 2017: [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

\_\_\_\_\_. 2017. 'Key issues for digital transformation in the G20.' 12 January. As of 17 July 2017: <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>

Oxley, Alan. 2011. 'A best practices guide for mitigating risk in the use of social media.' As of 17 July 2017: [https://ofti.org/wp-content/uploads/2012/07/71490\\_riskuseofsocialmedia.pdf](https://ofti.org/wp-content/uploads/2012/07/71490_riskuseofsocialmedia.pdf)

Proteccion Online. N.d. 'Home page.' As of 1 November 2017: [www.protecciononline.com](http://www.protecciononline.com)

Robinson, Neil, Veronika Horvath, Jonathan Cave, Arnold PC Roosendaal & Marieke Klaver. 2013. 'Data and security breaches and cyber-security strategies in the EU and its international counterparts.' As of 17 July 2017: [http://www.rand.org/pubs/external\\_publications/EP50395.html](http://www.rand.org/pubs/external_publications/EP50395.html)

Stay Safe Online. 2017. 'Home page.' As of 17 July 2017: <https://staysafeonline.org>

Stop Think Connect. 2017. 'Home Page.' As of 17 July 2017: <https://www.stophinkconnect.org/>

Trend Micro, & Organization of American States. 2015. *Cyber Security and Critical Infrastructure in the Americas.* Trend Micro Publication. As of 17 July 2017: [https://www.sites.oas.org/cyber/Certs\\_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf](https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf)

UK Government. 2016a. 'Cyber Essentials.' As of 9 November 2017: <https://www.cyberaware.gov.uk/cyberessentials/faq.html>

- \_\_\_\_\_. 2016b. 'Protect your business against cyber threats.' As of 1 November 2017: [www.cyberstreetwise.com/cyberessentials/](http://www.cyberstreetwise.com/cyberessentials/)
- UNCTAD. 2015. 'Information Economy Report.' As of 17 July 2017: [http://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf)
- \_\_\_\_\_. 2016. 'Data protection regulations and international data flows: Implications for trade and development.' As of 17 July 2017: [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)
- US Department of Homeland Security. N.d.-a. *Cybersecurity Questions for CEOs*. As of 1 November 2017: <https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf>
- \_\_\_\_\_. N.d.-b. 'Five ways to be cyber secure at work.' As of 1 November 2017: <https://www.dhs.gov/sites/default/files/publications/Week2TipCard-%20508%20compliant.pdf>
- \_\_\_\_\_. N.d.-c. 'Stop. Think. Connect.' As of 31 October 2017: <https://www.dhs.gov/stopthinkconnect>
- US Department of Justice. N.d. *24/7 High Tech Crime Network*. Computer Crime & Intellectual Property Section. As of 1 November 2017: [http://www.oas.org/juridico/english/cyb20\\_network\\_en.pdf](http://www.oas.org/juridico/english/cyb20_network_en.pdf)
- VFAC (Virtual Forum Against Cybercrime). 2012. 'Home page.' As of 1 November 2017: <https://www.cybercrimeforum.org/index.jsp>
- Ward, Dan, & Robert Morgus. 2016. *Professor Cy Burr's Graphic Guide to: International Cyber Norms*. New America. As of 1 November 2017: <https://na-production.s3.amazonaws.com/documents/CyberNorms11.14.pdf>
- WePROTECT Global Alliance. 2015. 'Home page.' As of 1 November 2017: [www.weprotect.org](http://www.weprotect.org)
- World Bank. 2016. 'World Development Report 2016: Digital Dividends.' Washington, DC. As of 17 July 2017: <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>

## D3. Cyber security education, training and skills

APMG International. 2017. 'Accreditation.' As of 31 October 2017: <https://apmg-international.com/our-services/accreditation>

APNIC (Asia Pacific Network Information Centre). 2017. 'Courses.' As of 1 November 2017: <https://training.apnic.net/courses>

AXELOS. N.d. 'Global Best Practice Solutions.' As of 31 October 2017: <https://www.axelos.com/>

Bada, Maria, & Sadie Creese. 2014. *Cyber security awareness campaigns: Why do they fail to change behavior?* Oxford: Global Cyber Security Capacity Centre. As of 17 July 2017: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf>

Bada, Maria, Angela Sasse & Jason Nurse. 2014. 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?' *Global Cyber Security Capacity Centre*. As of 31 October 2017: <http://discovery.ucl.ac.uk/1468954/>

Bayuk, Jennifer L, Jason Healey, Paul Rohmeyer, Marcus H Sachs, Jeffrey Schmidt & Joseph Weiss. 2012. *Cyber security policy guidebook*. John Wiley & Sons.

Bennett, Alex. 2017. 'Cybersecurity in 2025: the skills we'll need to tackle threats of the future.' *Wired*, 4 April. As of 31 October 2017: <http://www.wired.co.uk/article/cybersecurity-2025-skills-risks>

BLS (United States Bureau of Labor Statistics). 2015. 'Labor force characteristics by race and ethnicity, 2014.' *US Bureau of Labor Statistics* November(Report 1057). As of 31 October 2017: <https://www.bls.gov/opub/reports/race-and-ethnicity/archive/labor-force-characteristics-by-race-and-ethnicity-2014.pdf>

BSA. 2015. *Asia-Pacific Cybersecurity Dashboard. A Path to a Secure Global Cyberspace*. Washington, DC: BSA Worldwide. As of 31 October 2017: [http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study\\_apac\\_cybersecurity\\_en.pdf](http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf)

Carr, Madeline. 2016. 'Public–private partnerships in national cyber-security strategies.' *International Affairs* 92(1): 43-62. As of 31 October 2017: [https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92\\_1\\_03\\_Carr.pdf](https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf)

Cătălui, Daria. 2014. *Public Private Partnerships in Network and Information Security Education*. ENISA. As of 31 October 2017: <https://www.enisa.europa.eu/publications/public-private-partnerships-in-network-and-information-security-education>

Central District of California United States Attorney's Office. 2017. 'The Cybersecurity Program.' 18 October. As of 31 October 2017: <https://www.justice.gov/usao-cdca/cybersecurity-program>

Centres of Academic Excellence in Cybersecurity Community. 2017. 'Home page.' As of 31 October 2017: <https://www.caecommunity.org/>

Cyber Security Challenge UK. 2017. 'Novice Toolkit.' As of 31 October 2017: <https://cybersecuritychallenge.org.uk/novice-toolkit>

- CyberSecurity Malaysia. 2017. 'CyberSAFE.' As of 31 October 2017: <http://www.cybersafe.my/en/>
- CyberSeek. N.d. 'Hack the Gap: Close the cybersecurity talent gap with interactive tools and data.' As of 31 October 2017: <http://cyberseek.org/index.html>
- EC-Council. 2017. 'Accreditations.' As of 31 October 2017: <https://www.eccouncil.org/accreditations/>
- ENISA. 2007. *Information security awareness initiatives: Current proactive and the measurement tools.*
- . 2009. 'National Exercise - Good Practice Guide.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide>
- . 2012a. *Collaborative Solutions for Network Information Security in Education.* As of 10 November 2017: <https://www.enisa.europa.eu/publications/collaborative-solutions-for-network-information-security-in-education>
- . 2012b. 'Good Practices in Resilient Internet Interconnections.' June 2012. As of 17 July 2017: <https://www.enisa.europa.eu/publications/enisa-report-on-resilient-internet-interconnections>
- . 2012c. *Network Information Security in Education.* As of 10 November 2017: <https://www.enisa.europa.eu/publications/collaborative-solutions-for-network-information-security-in-education>
- . 2013. *Brokerage model for NIS in Education.* As of 10 November 2017: <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/nis-brokerage-1/NetworkInformationSecurityinEducation.pdf>
- . 2014a. *An evaluation framework for Cyber Security Strategies.* As of 31 October 2017: <https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies>
- . 2014b. *PPPs and their role in NIS Education.* As of 31 October 2017: <https://www.enisa.europa.eu/publications/public-private-partnerships-in-network-and-information-security-education>
- . 2014c. *Roadmap for NHS education programmes in Europe.* As of 31 October 2017: [https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe/at\\_download/fullReport](https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe/at_download/fullReport)
- . 2015a. 'Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/cybersecurity-information-sharing>
- . 2015b. *Status of privacy and NIS course curricula in EU Member States.* As of 31 October 2017: <https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states>
- . 2016. 'Governance framework for European standardisation.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/policy-industry-research>
- . 2017a. 'Education Map.' As of 31 October 2017: <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities>

- \_\_\_\_\_. 2017b. 'National cyber security strategies training tool.' As of 17 June 2017: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool>
- EPSRC (Engineering and Physical Sciences Research Council). 2017. 'Academic Centres of Excellence in Cyber Security Research.' As of 31 October 2017: <https://www.epsrc.ac.uk/research/centres/acecybersecurity/>
- European Commission. 2012. 'EU High level group of experts on literacy.' Luxembourg. As of 1 November 2017: [http://ec.europa.eu/dgs/education\\_culture/repository/education/policy/school/doc/literacy-report\\_en.pdf](http://ec.europa.eu/dgs/education_culture/repository/education/policy/school/doc/literacy-report_en.pdf)
- Fraunhofer Academy. 2017. 'Structure and Organization of Fraunhofer-Gesellschaft.' As of 31 October 2017: <https://www.fraunhofer.de/en/about-fraunhofer/profile-structure/structure-organization.html>
- \_\_\_\_\_. N.d. *Cybersecurity Training Lab.* As of 31 October 2017: <https://www.academy.fraunhofer.de/content/dam/academy/en/documents/Information%20und%20Kommunikation/en/Cybersecurity Info Brochure 2017 web.pdf>
- GCHQ. 2016. *GCHQ Certification of Cyber Security Training Courses.* NCSC. As of 10 November 2017: [https://www.ncsc.gov.uk/content/files/protected\\_files/document\\_files/GCT%20scheme%20-%20Course%20Content%20Criteria%20v2%200.pdf](https://www.ncsc.gov.uk/content/files/protected_files/document_files/GCT%20scheme%20-%20Course%20Content%20Criteria%20v2%200.pdf)
- \_\_\_\_\_. N.d. 'CyberFirst.' As of 31 October 2017: <https://www.gchq-careers.co.uk/early-careers/cyberfirst.html>
- GCS SCC (Global Cyber Security Capacity Centre). 2014. 'Cyber security capability maturity model (CMM) - V1.2.' Oxford, 15 December. As of 17 July 2017: [https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201\\_2\\_0.pdf](https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf)
- GenCyber. N.d.-a. 'GenCyber: Girls in CybHER Security.' As of 31 October 2017: <http://www.gencybergirls.camp/about-us.html>
- \_\_\_\_\_. N.d.-b. 'Inspiring the Next Generation of Cyber Stars.' As of 31 October 2017: <https://www.gen-cyber.com/about/>
- Government of Japan. 2015. *The Basic Policy of Critical Infrastructure Protection.* Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)
- Hall, Suzanne, Sloane Menkes & Emily Stapf. 2017. 'Women in Cybersecurity: Underrepresented, untapped potential.' PwC, 31 October, 07:14 EDT. As of 31 October 2017: <https://www.pwc.com/us/en/cybersecurity/women-in-cybersecurity.html>
- IAPP (International Association of Privacy Professionals). 2017. 'About the IAPP.' As of 31 October 2017: <https://iapp.org/about/>
- ICC (International Chamber of Commerce). 2015. 'ICC Cyber Security Guide for Business.' As of 17 July 2017: <https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/>

ICMCP (International Consortium of Minority Cybersecurity Professionals). 2017. 'Home page.' As of 31 October 2017: <https://icmcp.org/>

IISP. 2010. 'Information Security Skills Framework.' As of 10 November 2017: <https://www.iisp.org/imis15/CMDDownload.aspx?ContentKey=1c057e3e-05f0-4e65-9274-48722282033b&ContentItemKey=4952be86-df54-47f4-ada6-b89c3b81da41>

Insafe. N.d. 'About Safer Internet Day.' As of 31 October 2017: <https://www.saferinternetday.org/web/sid/about>

Jagasia, Arnav. 2017. 'A look into public private partnerships for cybersecurity.' *Public Policy Initiative, Penn Wharton University of Pennsylvania*, 18 April. As of 31 October 2017: <https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for>

Johnson, Craig L. 2008. 'A framework for pricing government e-services.' *Electronic Commerce Research and Applications* 6(4): 484-9.

Lewis, James Andrew, & Götz Neuneck. 2013. *The Cyber Index: International Security Trends and Realities*. Vol. 3. United Nations Publications. As of 1 November 2017: <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>

Libicki, Martin C, David Senty & Julia Pollak. 2014. *Hackers Wanted: an examination of the cybersecurity labor market*. Santa Monica, Calif.: Rand Corporation. RR-430. As of 31 October 2017: [https://www.rand.org/pubs/research\\_reports/RR430.html](https://www.rand.org/pubs/research_reports/RR430.html)

Lord, Nate. 2017. 'Cybersecurity higher education: The top cybersecurity colleges and degrees.' *Digital Guardian*, 18 August. As of 31 October 2017: <https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees>

Luijif, Eric, Tom van Schie, Theo van Ruijven & Auke Huistra. 2016. 'The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.' As of 17 July 2017: <https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf>

Malmedal, Bjarte, & Hanne Eggen Røislien. 2016. *The Norwegian Cyber Security Culture*. NorSIS. As of 10 November 2017: <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>

National Cyber Security Alliance. 2017. 'StaySafeOnline.' As of 31 October 2017: <https://staysafeonline.org/about/>

NATO Cooperative Cyber Defence Centre of Excellence. N.d. 'Cyber Defence Training.' As of 31 October 2017: <https://ccdcoc.org/training.html>

NCSC. 2015. 'GCHQ Certified Training.' 1 August 2016. As of 31 October 2017: <https://www.ncsc.gov.uk/scheme/gchq-certified-training>

\_\_\_\_\_. 2017. 'About the NCSC.' 9 June. As of 31 October 2017:  
<https://www.ncsc.gov.uk/information/about-ncsc>

Newhouse, William, Stephanie Keith, Benjamin Scribner & Greg Witte. 2017. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* NIST. 800-181. As of 10 November 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

NICCS (National Initiative for Cybersecurity Careers and Studies). 2017. 'Cybersecurity.' 8 September 2017. As of 31 October 2017: <https://niccs.us-cert.gov/cybersecurity>

NICE (National Initiative for Cybersecurity Education). 2013. *2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report*. US Department of Homeland Security. As of 31 October 2017: <https://www.dhs.gov/cybersecurity-workforce-development-resources>

\_\_\_\_\_. 2017. *Cyber Ranges*. National Institute of Standards Technology. As of 31 October 2017: [https://www.nist.gov/sites/default/files/documents/2017/05/23/cyber\\_ranges\\_2017.pdf](https://www.nist.gov/sites/default/files/documents/2017/05/23/cyber_ranges_2017.pdf)

NIST. 2017. 'NICE Cybersecurity Workforce Framework.' 19 October. As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

\_\_\_\_\_. N.d.-a. 'Home page.' As of 31 October 2017: <https://www.nist.gov/>

\_\_\_\_\_. N.d.-b. 'Information Technology Laboratory: Applied Cybersecurity Division.' As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity>

Norwegian Ministries. 2012. *Cyber Security Strategy for Norway*. As of 31 October 2017: [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway\\_Cyber\\_Security\\_StrategyNO.pdf](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway_Cyber_Security_StrategyNO.pdf)

OAS (Organization of American States). 2015a. 'Best Practices for Establishing a National CSIRT.' April. As of 17 July 2017: <https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>

\_\_\_\_\_. 2015b. *Cybersecurity awareness campaign toolkit*. As of 31 October 2017: [https://www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20\(English\).pdf](https://www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20(English).pdf)

OECD. 2017. 'Key issues for digital transformation in the G20.' 12 January. As of 17 July 2017: <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>

Pârvu, Daniela, & Cristina Voicu-Olteanu. 2009. 'Advantages and limitations of the public private partnerships and the possibility of using them in Romania.' *Transylvanian Review of Administrative Sciences* 5(27): 189-98. As of 31 October 2017: [http://www.ucv.ro/pdf/invatamant/educatie/scoala\\_doctorala/pirvu\\_daniela/portofoliu/2.pdf](http://www.ucv.ro/pdf/invatamant/educatie/scoala_doctorala/pirvu_daniela/portofoliu/2.pdf)

Ponemon Institute. 2014. *2014 Best Schools for Cybersecurity*. Sponsored by HP Enterprise Security. As of 31 October 2017: [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_2014\\_Best\\_Schools\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf)

- Purser, Steve. 2014. *Standards for Cyber Security*. IOS Press: ENISA. As of 31 October 2017: <https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security>
- Raguseo, Domenico. 2017. 'The Future of Cybersecurity.' *SecurityIntelligence*, 10 February. As of 31 October 2017: <https://securityintelligence.com/the-future-of-cybersecurity/>
- SANS. 2017. 'World Leading Cyber Security Training.' As of 31 October 2017: <https://uk.sans.org/>
- Security Awareness Program Special Interest Group PCI Security Standards Council. 2014. *Information Supplement: Best Practices for Implementing a Security Awareness Program*. PCI Security Standards Council. As of 10 November 2017: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_V1.0\\_Best\\_Practices\\_for\\_Implementing\\_Security\\_Awareness\\_Program.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf)
- Singapore Institute of Technology. 2017. 'Information and Communications Technology (Information Security), BEng (Hons).' As of 31 October 2017: <https://www.singaporettech.edu.sg/undergraduate-programmes/ict-information-security>
- The Guardian. 2012. 'IT Governance Ltd.' *The Guardian*, 21 February. As of 31 October 2017: <https://www.theguardian.com/guardian-professional/2012/feb/21/it-governance-ltd>
- The White House. 2016. 'FACT SHEET: Cybersecurity National Action Plan.' 9 February. As of 17 July 2017: <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
- Tirrell, William K. 2012. *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?* : Army Command And General Staff Coll Fort Leavenworth Ks. As of 31 October 2017: <https://www.hSDL.org/?view&did=729810>
- UK Cabinet Office. N.d. 'About Us.' As of 31 October 2017: <https://www.gov.uk/government/organisations/cabinet-office/about>
- UK Government. 2014. 'Accreditation and conformity assessment: guidance for business and government departments.' As of 31 October 2017: <https://www.gov.uk/government/publications/accreditation-and-conformity-assessment-guidance-for-business-and-government-departments/>
- \_\_\_\_\_. 2016a. 'Cyber security training for business.' As of 31 October 2017: <https://www.gov.uk/government/collections/cyber-security-training-for-business>
- \_\_\_\_\_. 2016b. 'Millions invested in degree apprenticeships.' As of 31 October 2017: <https://www.gov.uk/government/news/millions-invested-in-degree-apprenticeships>
- \_\_\_\_\_. 2017a. 'Extracurricular cyber clubs to inspire and identify tomorrow's cyber security professionals.' As of 31 October 2017: <https://www.gov.uk/government/news/extracurricular-cyber-clubs-to-inspire-and-identify-tomorrows-cyber-security-professionals>
- \_\_\_\_\_. 2017b. 'Students urged to apply for pioneering Cyber Schools Programme.' As of 31 October 2017:

<https://www.gov.uk/government/news/students-urged-to-apply-for-pioneering-cyber-schools-programme>

\_\_\_\_\_. N.d. 'Office of Cyber Security and Information Assurance.' As of 31 October 2017: <https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance>

UK Ministry of Defence. 2017. 'JSP 822: Defence Direction and Guidance for Training and Education.' As of 17 July 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/600177/20170317-JSP\\_822\\_Part\\_1-Final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/600177/20170317-JSP_822_Part_1-Final.pdf)

UK National Cyber Security Centre. 2015. '10 Steps: User education and awareness.' 8 August 2016. As of 17 July 2017: <https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness>

United States Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense. As of 31 October 2017: [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final%202015%20DoD%20CYBER%20STRATEGY%20for%20web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final%202015%20DoD%20CYBER%20STRATEGY%20for%20web.pdf)

US Department of Homeland Security. 2017a. 'About Stop. Think. Connect.' As of 31 October 2017: <https://www.stopthinkconnect.org/about>

\_\_\_\_\_. 2017b. 'Cybersecurity Workforce Development Resources.' 17 October. As of 31 October 2017: <https://www.dhs.gov/cybersecurity-workforce-development-resources>

\_\_\_\_\_. N.d. 'Stop. Think. Connect.' As of 31 October 2017: <https://www.dhs.gov/stopthinkconnect>

USTTI (United States Telecommunications Training Institute ). 2017. 'Home page.' As of 1 November 2017: <http://www.ustti.org/>

Wilson, Mark, Dorothea E de Zafra, Sadie I Pitcher, John D Tressler & John B Ippolito. 1998. 'Information technology security training requirements: A role-and performance-based model.' As of 17 July 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf>

Wilson, Mark, & Joan Hash. 2003. 'Building an information technology security awareness and training program.' *NIST Special publication 800(50)*: 1-39.

Yampolskiy, Roman. 2017. 'Ai is the future of cybersecurity, for better and for worse.' *Harvard Business Review*, 8 March. As of 31 October 2017: <https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse>

## D4. Legal and regulatory frameworks

Brown, Cameron SD. 2015. 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice.' *International Journal of Cyber Criminology* 9(1): 55.

College of Policing. N.d. 'Digital and cyber crime.' As of 10 November 2017: [http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber\\_crime.aspx](http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx)

Constantin, Lucian. 2014. '5 things you need to know about cybersecurity insurance.' 25 April. As of 17 July 2017: <http://www.cio.com/article/2376802/security/5-things-you-need-to-know-about-cybersecurity-insurance.html>

Council of Europe. 2008a. 'Convention on Cybercrime.' *European Treaty Series* 185. As of 10 November 2017: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf)

\_\_\_\_\_. 2008b. 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime.' 2 April. As of 17 July 2017: <https://rm.coe.int/16802fa3ba>

\_\_\_\_\_. 2017a. 'International Cooperation against Cybercrime.' As of 17 July 2017: <https://www.coe.int/en/web/cybercrime/international-cooperation>

\_\_\_\_\_. 2017b. 'Law enforcement - Internet service provider Cooperation.' As of 17 July 2017: <https://www.coe.int/en/web/cybercrime/lea-/isp-cooperation>

CPS (The Crown Prosecution Service). N.d. 'Cybercrime - Legal Guidance.' As of 10 November 2017: [http://www.cps.gov.uk/legal/a\\_to\\_c/cybercrime/](http://www.cps.gov.uk/legal/a_to_c/cybercrime/)

Craiger, J Philip. 2005. 'Computer forensics procedures and methods.' In *Handbook of Information Security*, Edited by H. Bigdoli. New York: John Wiley & Sons. As of 10 November 2017: <http://www.cyberace.org/Publications/craiger.forensics.methods.procedures.DRAFT.pdf>

Daly, Kathleen, & Rick Sarre. 2017. 'Criminal justice system: Aims and processes.' In *Crime and Justice: A Guide to Criminology*, Edited by Darren Palmer, Williem de Lint & Derek Dalton. Sydney: Lawbook Co. As of 10 November 2017: [https://www.griffith.edu.au/\\_data/assets/pdf\\_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf](https://www.griffith.edu.au/_data/assets/pdf_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf)

Deloitte. 2015. *The Deloitte Consumer Review: Consumer data under attack: The growing threat of cyber crime.* As of 10 November 2017: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf>

ENISA. 2016a. 'Governance framework for European standardisation.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/policy-industry-research>

- \_\_\_\_\_. 2016b. 'Strategies for incident response and cyber crisis cooperation.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation>
- European Council. 2014. 'EU Human Rights Guidelines on Freedom of Expression Online and Offline.' As of 17 July 2017: [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/EN/foraff/142549.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf)
- European Union, & Council of Europe. 2011. *Specialised cybercrime units: Good practice study*. Strasbourg, France: Directorate General of Human Rights and Rule of Law. As of 10 November 2017: <https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33>
- Europol. 2016. 'The relentless growth of cybercrime.' As of 17 July 2017: <https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime>
- \_\_\_\_\_. 2017. 'European cybercrime centre - EC3.' As of 10 November 2017: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
- \_\_\_\_\_. N.d. 'Training and Capacity Building.' As of 10 November 2017: <https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building>
- Forensic Science Regulator. 2015. 'Newsletter.' October(26). As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/470526/FSR\\_Newsletter\\_26\\_October\\_2015.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470526/FSR_Newsletter_26_October_2015.pdf)
- Forensic Science Simplified. N.d. *A Simplified Guide To Digital Evidence*. NFSTC. As of 10 November 2017: <http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf>
- GCSCC (Global Cyber Security Capacity Centre). 2014. 'Cyber security capability maturity model (CMM) - V1.2.' Oxford, 15 December. As of 17 July 2017: [https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201\\_2\\_0.pdf](https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf)
- GLACY (Global Action on Cybercrime). 2014. 'Good practice study: Cybercrime reporting mechanisms.' September. As of 17 July 2017: <https://rm.coe.int/168030287c>
- Gordon, Sarah, & Richard Ford. 2006. 'On the definition and classification of cybercrime.' *Journal in Computer Virology* 2(1): 13-20. As of 10 November 2017: [https://www.griffith.edu.au/\\_data/assets/pdf\\_file/0011/924878/2017-Daly-and-Sarre-Criminal-J ustice-System-FINAL-23-Oct-2016.pdf](https://www.griffith.edu.au/_data/assets/pdf_file/0011/924878/2017-Daly-and-Sarre-Criminal-J ustice-System-FINAL-23-Oct-2016.pdf)
- Government of Japan. 2015. *The Basic Policy of Critical Information Infrastructure Protection*. Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)
- Home Office. 2010. *Cyber Crime Strategy*. London: UK Parliament. Cm 7842. As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228826/7842.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf)
- Interpol. 2017a. 'Activities.' As of 10 November 2017: <https://www.interpol.int/Crime-areas/Cybercrime/Activities/Digital-forensics>

- \_\_\_\_\_. 2017b. 'ASEAN Cyber Forensic Investigation Capability Project – first training course.' As of 10 November 2017:  
<https://www.interpol.int/News-and-media/Events/2015/ASEAN-Cyber-Forensic-Investigation-Capability-Project/ASEAN-Cyber-Forensic-Investigation-Capability-Project-%E2%80%93-first-training-course>
- \_\_\_\_\_. 2017c. 'The INTERPOL Global Complex for Innovation.' As of 10 November 2017:  
<https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI>
- ITU. 2010. 'ITU Toolkit for Cybercrime Legislation.' As of 17 July 2017:  
<http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf>
- \_\_\_\_\_. 2012a. *HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts*. Geneva, Switzerland: ITU. As of 10 November 2017:  
<https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf>
- \_\_\_\_\_. 2012b. *Understanding cybercrime: Phenomena, challenges and legal response*. As of 17 July 2017:  
<http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html>
- \_\_\_\_\_. 2014. 'The quest for cyber confidence.' As of 17 July 2017:  
<http://handle.itu.int/11.1002/pub/80b7079c-en>
- Kornblum, Jesse. 2002. *Preservation of Fragile Digital Evidence by First Responders*. As of 10 November 2017:  
[http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/Jesse\\_Kornblum.pdf](http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/Jesse_Kornblum.pdf)
- Ling, Tom, & Lidia Villalba van Dijk. 2009. *Performance Audit Handbook: Routes to effective evaluation*. TR-788-RE ed. Santa Monica, Calif.: RAND Corporation. As of 1 November 2017:  
[https://www.rand.org/pubs/technical\\_reports/TR788.html](https://www.rand.org/pubs/technical_reports/TR788.html)
- Mendel, Toby, Andrew Puddephatt, Ben Wagner, Dixie Hawtin & Natalia Torres. 2012. 'Global survey on internet privacy and freedom of expression.' As of 17 July 2017:  
<http://unesdoc.unesco.org/images/0021/002182/218273e.pdf>
- Microsoft Digital Crimes Unit. 2015. *Digital Crimes Unit Fact Sheet*. As of 10 November 2017:  
[https://news.microsoft.com/download/presskits/DCU/docs/dcufS\\_160115.pdf](https://news.microsoft.com/download/presskits/DCU/docs/dcufS_160115.pdf)
- National Crime Agency. N.d. 'National Cyber Crime Unit.' As of 10 November 2017:  
<http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>
- NCSC. 2017a. 'Cyber Security Information Sharing Partnership (CiSP).' 27 September 2016. As of 10 November 2017: <https://www.ncsc.gov.uk/cisp>
- \_\_\_\_\_. 2017b. 'NCSC-certified degrees.' 12 August. As of 31 October 2017:  
<https://www.ncsc.gov.uk/information/ncsc-certified-degrees>

- Odinot, G, MA Verhoeven, RLD Pool & CJ de Poot. 2017. 'Organised Cybercrime in the Netherlands.' As of 17 July 2017: [https://www.wodc.nl/binaries/Cahier%202017-1\\_Full%20text\\_tcm28-244615.pdf](https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf)
- PCI Security Standards Council. 2014. 'Best Practices for Implementing a Security Awareness Program.' October. As of 17 July 2017: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_V1.0\\_Best\\_Practices\\_for\\_Implementing\\_Security\\_Awareness\\_Program.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf)
- Posner, Richard A. 1998. 'Creating a legal framework for economic development.' *The World Bank Research Observer* 13(1): 1-11.
- Prasanthi, Lakshmi, & Tata A S K Ishwarya. 2015. 'Cyber Crime: Prevention & Detection.' *International Journal of Advanced Research in Computer and Communication Engineering* 4(3). As of 10 November 2017: <https://www.ijarcce.com/upload/2015/march-15/IJARCCE%2011.pdf>
- Prayudi, Yudi, Ahmad Ashari & Tri K Priyambodo. 2014. 'Digital evidence cabinets: A proposed framework for handling digital chain of custody.' *International Journal of Computer Applications* 107(9). As of 10 November 2017: [https://www.researchgate.net/profile/Yudi\\_Prayudi/publication/273131361\\_Digital\\_Evidence\\_Cabinets\\_A\\_Proposed\\_Framework\\_for\\_Handling\\_Digital\\_Chain\\_of\\_Custody/links/54f880130cf210398e96b370/Digital-Evidence-Cabinets-A-Proposed-Framework-for-Handling-Digital-Chain-of-Custody.pdf](https://www.researchgate.net/profile/Yudi_Prayudi/publication/273131361_Digital_Evidence_Cabinets_A_Proposed_Framework_for_Handling_Digital_Chain_of_Custody/links/54f880130cf210398e96b370/Digital-Evidence-Cabinets-A-Proposed-Framework-for-Handling-Digital-Chain-of-Custody.pdf)
- Prayudi, Yudi, & Azhari Sn. 2015. 'Digital chain of custody: State of the art.' *International Journal of Computer Applications* 114(5). As of 10 November 2017: [https://www.researchgate.net/profile/Yudi\\_Prayudi/publication/273694917\\_Digital\\_Chain\\_of\\_Custody\\_State\\_of\\_The\\_Art/links/5508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf](https://www.researchgate.net/profile/Yudi_Prayudi/publication/273694917_Digital_Chain_of_Custody_State_of_The_Art/links/5508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf)
- Queensland Government. 2016. 'Criminal Justice Framework: Guidelines for evaluating criminal justice initiatives.' As of 10 November 2017: <https://www.premiers.qld.gov.au/publications/categories/guides/assets/criminal-justice-evaluation-framework.pdf>
- Sales, Nathan Alexander. 2012. 'Regulating cyber-security.' As of 1 November 2017: <http://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1/>
- Staro, Sergio. 2010. *The G8 24/7 Network*. Italian delegation at the G8 Rome/Lyon Group (Subgroup on High Tech Crime). As of 10 November 2017: <https://rm.coe.int/16802fa06e>
- Tikk-Ringas, Eneken. 2015. *Legal Framework of Cyber Security*. In *Cyber Security: Analytics, Technology and Automation*. Springer. As of 1 November 2017: [https://link.springer.com/chapter/10.1007/978-3-319-18302-2\\_8](https://link.springer.com/chapter/10.1007/978-3-319-18302-2_8)
- UK Government. 2010. *Cyber Crime Strategy*. Cm 7842. As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228826/7842.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf)
- \_\_\_\_\_. 2014. *Serious and organised crime strategy*. As of 10 November 2017: <https://www.gov.uk/government/publications/serious-organised-crime-strategy>

- \_\_\_\_\_. 2015. 'Cyber security insurance: new steps to make UK world centre.' 23 March. As of 17 July 2017:  
<https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre>
- \_\_\_\_\_. 2016. 'National Cyber Security Strategy 2016 to 2021.' 11 September 2017. As of 10 November 2017: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>
- \_\_\_\_\_. N.d. 'Home Office: About Us.' As of 10 November 2017:  
<https://www.gov.uk/government/organisations/home-office/about>
- UK Ministry of Justice. 2014. *Transforming the Criminal Justice System Strategy and Action Plan – Implementation Update.* As of 10 November 2017:  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/330690/cjs-strategy-action-plan.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330690/cjs-strategy-action-plan.pdf)
- UK Parliament. 2014a. 'Chapter 2: Social media and the law.' As of 17 July 2017:  
<https://publications.parliament.uk/pa/l201415/ldselect/lcomuni/37/3704.htm#note2>
- \_\_\_\_\_. 2014b. 'How laws are made.' As of 10 November 2017:  
<http://www.parliament.uk/education/about-your-parliament/how-laws-are-made/>
- \_\_\_\_\_. 2016. 'Digital Forensics and Crime.' As of 10 November 2017:  
<http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0520>
- UNODC. 2013. 'Comprehensive Study on Cybercrime.' February. As of 17 July 2017:  
[https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf)
- US Department of Homeland Security. 2017. 'Cybersecurity Insurance.' As of 17 July 2017:  
<https://www.dhs.gov/cybersecurity-insurance>
- Vandeven, Sally. 2014. *Forensic Images: For Your Viewing Pleasure.* InfoSec Reading Room: SANS Institute. As of 10 November 2017:  
<https://uk.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447>
- Wainwright, Robert, & Frank J. Cilluffo. 2017. 'Responding to Cybercrime at Scale: Operation Avalanche - A cast-study.' As of 17 July 2017:  
<https://cchs.gwu.edu/sites/cchs.gwu.edu/files/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf>
- WEF (World Economic Forum). 2017. *Guidance on Public-Private Information Sharing against Cybercrime.* As of 10 November 2017:  
[http://www3.weforum.org/docs/WEF\\_Guidance\\_Cybercrime\\_report\\_2017.pdf](http://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf)
- World Bank. 2016. *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies.* Washington, DC: The World Bank. As of 10 November 2017:  
<http://www.combattingcybercrime.org/>

## D5. Standards, organisations and technologies

Acar, Yasemin, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek & Christian Stransky. 2017. 'How Internet Resources Might Be Helping You Develop Faster but Less Securely.' *IEEE Security & Privacy* 15(2): 50-60.

ACORN (Australian Cybercrime Online Reporting Network). N.d. 'Home page.' As of 10 November 2017: <https://www.acorn.gov.au/>

ARIN (American Registry for Internet Numbers). 2017. 'Regional Internet Registries.' As of 31 October 2017: <https://www.arin.net/knowledge/rirs.html>

Australia, Code Club. 2016. '#GETKIDSCODING.' As of 10 November 2017: <https://codeclubau.org/>

Australian Department of Defence. 2013. 'Top 4 strategies to mitigate targeted cyber intrusions: Mandatory requirements explained.' 2017. As of 17 July 2017: <https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>

Ball, James, Julian Borger & Glenn Greenwald. 2013. 'Revealed: how US and UK spy agencies defeat internet privacy and security.' 21 June. As of 7 July 2017: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

BBC. 2014. 'GCHQ accredits UK master's degrees for 'cyber spies'.' BBC, 2 August. As of 10 November 2017: <http://www.bbc.com/news/uk-28623365>

\_\_\_\_\_. 2017. 'Russian arrested in Spain 'over mass hacking'.' 10 April. As of 17 July 2017: <http://www.bbc.com/news/technology-39553250>

Black, Paul E, Lee Badger, Barbara Guttman & Elizabeth Fong. 2016. *Dramatically Reducing Software Vulnerabilities*. NIST. NISTIR 8151. As of 10 November 2017: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf>

Brown, Cameron SD. 2015. 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice.' *International Journal of Cyber Criminology* 9(1): 55.

Casson, Tony, & Patrick S Ryan. 2006. 'Open standards, open source adoption in the public sector, and their relationship to Microsoft's market dominance.' In *Standards Edge: Unifier or Divider?*, Edited by Sherrie Bolin. Sheridan Books. As of 31 October 2017: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1656616](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1656616)

CERT (Computer Emergency Response Team). 2017a. 'Create a CSIRT.' As of 17 July 2017: <http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm?>

\_\_\_\_\_. 2017b. 'SEI CERT Coding Standards.' As of 10 November 2017: <https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards>

Constantin, Lucian. 2014. '5 things you need to know about cybersecurity insurance.' 25 April. As of 17 July 2017: <http://www.cio.com/article/2376802/security/5-things-you-need-to-know-about-cybersecurity-insurance.html>

CPNI (Centre for the Protection of National Infrastructure). 2017. 'Supply Chain.' As of 31 October 2017: <https://www.cpni.gov.uk/supply-chain>

CSIS (Center for Strategic & International Studies). 2017. 'Analysis.' As of 1 November 2017: <https://www.csis.org/analysis/securing-cyberspacethrough-publicprivatepartnerships>

CYLON. 2017. 'Home page.' As of 10 November 2017: <https://cylonlab.com/>

Dredge, Stuart. 2014. 'Coding at school: a parent's guide to England's new computing curriculum.' *The Guardian*, 4 September. As of 10 November 2017: <https://www.theguardian.com/technology/2014/sep/04/coding-school-computing-children-programming>

e-Estonia. 2017. 'Estonia to open the world's first data embassy in Luxembourg.' *e-estonia*, June. As of 10 November 2017: <https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/>

EFF. N.d.-a. 'How to Deploy HTTPS Correctly.' As of 10 November 2017: <https://www.eff.org/https-everywhere/deploying-https>

\_\_\_\_\_. N.d.-b. 'HTTPS Everywhere.' As of 10 November 2017: <https://www.eff.org/https-everywhere/>

\_\_\_\_\_. N.d.-c. 'HTTPS Everywhere FAQ.' As of 10 November 2017: <https://www.eff.org/https-everywhere/faq>

ENISA. 2010. 'Report on secure routing technologies.' As of 17 June 2017: [https://www.enisa.europa.eu/publications/archive/report-on-secure-routing-technologies/at\\_download/fullReport](https://www.enisa.europa.eu/publications/archive/report-on-secure-routing-technologies/at_download/fullReport)

\_\_\_\_\_. 2011a. *Desktop Research on Public Private Partnerships*. As of 1 November 2017: [https://www.enisa.europa.eu/publications/copy\\_of\\_desktop-researach-on-public-private-partnerships](https://www.enisa.europa.eu/publications/copy_of_desktop-researach-on-public-private-partnerships)

\_\_\_\_\_. 2011b. *Good Practice Guide on Cooperative Models for Effective PPPs*. As of 1 November 2017: <https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperative-models-for-effective-ppps>

\_\_\_\_\_. 2012a. 'Good Practices in Resilient Internet Interconnections.' June 2012. As of 17 July 2017: <https://www.enisa.europa.eu/publications/enisa-report-on-resilient-internet-interconnections>

\_\_\_\_\_. 2012b. 'National Cyber Security Strategies: An Implementation Guide.' As of 17 July 2017: <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>

\_\_\_\_\_. 2013. 'Recommended cryptographic measures.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securig-personal-data>

\_\_\_\_\_. 2014a. 'Algorithms, key size and parameters report 2014.' 21 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

- \_\_\_\_\_. 2014b. 'Methodologies for the identification of Critical Information Infrastructure assets and services.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis>
- \_\_\_\_\_. 2014c. 'National/governmental CERTs: ENISA's recommendations on baseline capabilities.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities>
- \_\_\_\_\_. 2014d. 'Study on cryptographic protocols.' 21 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols>
- \_\_\_\_\_. 2016a. 'Definition of Cybersecurity - Gaps and overlaps in standardisation.' As of 17 July 2017: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>
- \_\_\_\_\_. 2016b. 'New good practice guide by ENISA on disclosing vulnerabilities.' 18 January. As of 10 November 2017: <https://www.enisa.europa.eu/news/enisa-news/new-good-practice-guide-by-enisa-on-disclosing-vulnerabilities>
- EPIC (Electronic Privacy Information Center). 2017. 'Vulnerabilities Equities Process.' As of 10 November 2017: <https://epic.org/privacy/cybersecurity/vep/>
- ETSI (European Telecommunications Standards Institute). 2017. 'Search and Browse Standards.' As of 1 November 2017: <http://www.etsi.org/standards-search>
- EU Council. 2008. 'On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.' 23 December. As of 17 July 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>
- EU Data Protection Regulation. 2015. 'Data Protection by Design and by Default.' As of 17 July 2017: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>
- Farivar, Cyrus. 2016. 'FBI paid at least \$1.3M for zero-day to get into San Bernardino iPhone.' 21 April. As of 17 July 2017: <https://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/>
- Financial Industry Regulatory Authority. 2015. 'Report on Cybersecurity Practices.' As of 17 July 2017: <https://www.finra.org/file/report-cybersecurity-practices>
- Fowler, Martin, & Jim Highsmith. 2001. 'The agile manifesto.' *Software Development* 9(8): 28-35.
- Friedman, Sam, & Adam Thomas. 2017. 'Demystifying cyber insurance coverage.' *Deloitte Insights*, 23 February. As of 31 October 2017: <https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html>
- Government of Japan. 2015. *The Basic Policy of Critical Information Infrastructure Protection*. Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)

- Hackmageddon. 2017. '2016 Cyber Attacks Statistics.' 19 January. As of 17 July 2017: <http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/>
- Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis & Panagiotis Trimintzios. 2013. *Resilience of the internet interconnection ecosystem*. In *Economics of Information Security and Privacy III*. Springer.
- IANA (Internet Assigned Numbers Authority). N.d. 'About Us.' As of 31 October 2017: <https://www.iana.org/about>
- ICANN (International Corporation for Assigned Names and Numbers). 2017. 'Get Started.' As of 31 October 2017: <https://www.icann.org/get-started>
- IEC (International Electrotechnical Commission). 2017. 'Feeds/Alerts.' As of 13 November 2017: <http://www.iec.ch/subscribe/?ref=toplinks>
- IEEE Standards Association. 2016. 'Working Group Areas.' As of 10 November 2017: <http://grouper.ieee.org/groups/>
- . 2017. 'About Us.' As of 31 October 2017: <http://standards.ieee.org/about/ieeesa.html>
- IEEE Xplore. 2017. 'IEEE GET Program.' As of 13 November 2017: <http://ieeexplore.ieee.org/browse/standards/get-program/page/?reload=true>
- IETF (Internet Engineering Task Force). 2017. 'Transport Layer Security (tls).' As of 17 July 2017: <https://datatracker.ietf.org/wg/tls/charter/>
- . N.d.-a. 'About the IETF.' As of 31 October 2017: <https://www.ietf.org/about/>
- . N.d.-b. 'Email Lists.' As of 13 November 2017: <https://www.ietf.org/list/>
- . N.d.-c. 'The IESG.' As of 31 October 2017: <https://www.ietf.org/iesg/>
- . N.d.-d. 'OpenPGP Message Format.' As of 10 November 2017: <https://tools.ietf.org/html/rfc4880>
- ISA (International Society of Automation). N.d. 'Home page.' As of 1 November 2017: <http://isa99.isa.org/>
- ISF (Information Security Forum). 2017. 'The ISF Standard of Good Practice for Information Security.' As of 1 November 2017: <https://www.securityforum.org/research/thestandardofgoodpractice2016/>
- ISO (International Organization for Standardization). 2009. 'ISO/IEC 15408-1:2009.' As of 31 October 2017: <https://www.iso.org/standard/50341.html>
- . 2011a. 'ISO/IEC 25010:2011.' As of 10 November 2017: <https://www.iso.org/standard/35733.html>
- . 2011b. 'ISO/IEC 27005:2011.' As of 31 October 2017: <https://www.iso.org/standard/56742.html>

- \_\_\_\_\_. 2012. 'ISO/IEC 27032:2012.' As of 31 October 2017:  
<https://www.iso.org/standard/44375.html>
- \_\_\_\_\_. 2013a. 'ISO/IEC 27001:2013.' As of 31 October 2017:  
<https://www.iso.org/standard/54534.html>
- \_\_\_\_\_. 2013b. 'ISO/IEC 30111:2013.' As of 10 November 2017:  
<https://www.iso.org/standard/53231.html>
- \_\_\_\_\_. 2014. 'ISO/IEC 29147:2014.' As of 10 November 2017:  
<https://www.iso.org/standard/45170.html>
- \_\_\_\_\_. 2015. 'ISO/IEC 27010:2015.' As of 10 November 2017:  
<https://www.iso.org/standard/68427.html>
- \_\_\_\_\_. 2017a. 'ISO 20400:2017.' As of 10 November 2017:  
<https://www.iso.org/obp/ui/#iso:std:iso:20400:ed-1:v1:en>
- \_\_\_\_\_. 2017b. 'ISO 20400: Sustainable Procurement — Guidance.' As of 31 October 2017:  
<https://www.iso.org/obp/ui/#iso:std:iso:20400:ed-1:v1:en>
- \_\_\_\_\_. N.d.-a. 'Freely Available Standards.' As of 10 November 2017:  
<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
- \_\_\_\_\_. N.d.-b. 'Technical Committees.' As of 10 November 2017:  
<https://www.iso.org/technical-committees.html>
- ISO/IEC. 2013. *Information technology -- Security techniques -- Information security management systems -- Requirements.* 27001:2013 ed.
- \_\_\_\_\_. 2014. *Software engineering -- Guidelines for the application of ISO 9001:2008 to computer software.* 90003:2014 ed.
- ITU (International Telecommunications Union). 2008. 'Overview of Cybersecurity.' As of 10 November 2017: <http://www.itu.int/rec/T-REC-X.1205-200804-I>
- \_\_\_\_\_. 2009. 'Guidelines for Policy Makers on Child Online Protection.' As of 17 July 2017:  
<http://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf>
- \_\_\_\_\_. 2010a. 'Approved ICT Security Standards.' As of 10 November 2017:  
[http://www.itu.int/itu-t/security/task\\_details.aspx?isn=3092&isnView=1&from=b1\\_2!b2\\_-1!b3\\_-1!t1\\_-1!k\\_security%20compendium](http://www.itu.int/itu-t/security/task_details.aspx?isn=3092&isnView=1&from=b1_2!b2_-1!b3_-1!t1_-1!k_security%20compendium)
- \_\_\_\_\_. 2010b. 'Security Roadmap Search.' As of 10 November 2017:  
[https://www.itu.int/ITU-T/security/main\\_table.aspx](https://www.itu.int/ITU-T/security/main_table.aspx)
- \_\_\_\_\_. 2015. 'National Spectrum Management.' As of 10 November 2017:  
<http://handle.itu.int/11.1002/pub/80c5a2ed-en>
- \_\_\_\_\_. 2017a. 'About International Telecommunication Union (ITU).' As of 31 October 2017:  
<http://www.itu.int/en/about/Pages/default.aspx>

- \_\_\_\_\_. 2017b. 'BRIDGING THE DIGITAL INNOVATION DIVIDE: A toolkit for strengthening ICT centric ecosystems.' As of 10 November 2017: [http://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Policy\\_Toolkit-Innovation\\_D012A0000D13301PDFE.pdf](http://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Policy_Toolkit-Innovation_D012A0000D13301PDFE.pdf)
- \_\_\_\_\_. 2017c. 'ITU-T Membership and Services.' As of 10 November 2017: <http://www.itu.int/en/ITU-T/membership/Pages/default.aspx>
- \_\_\_\_\_. 2017d. 'ITU-T Recommendations.' As of 31 October 2017: <http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx>
- \_\_\_\_\_. 2017e. 'Regional Cybersecurity Centres.' As of 10 November 2017: [http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Regional\\_Cybersecurity\\_Centre.aspx](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Regional_Cybersecurity_Centre.aspx)
- Kick, Jason. 2014. 'Cyber Exercise Playbook.' November. As of 17 July 2017: [http://www.mitre.org/sites/default/files/publications/pr\\_14-3929-cyber-exercise-playbook.pdf](http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)
- Klimberg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication. As of 17 July 2017: <https://ccdcoc.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>
- KPMG. 2016. *Cyber Insurance: Are insurers finding growth or looking for trouble?* As of 31 October 2017: <https://assets.kpmg.com/content/dam/kpmg/us/pdf/cyber-insurance-whitepaper.pdf>
- Kravets, David. 2016a. 'Apple defends crypto fight against government during launch event.' 21 March. As of 17 July 2017: <https://arstechnica.com/tech-policy/2016/03/apple-defends-crypto-fight-against-government-during-launch-event/>
- \_\_\_\_\_. 2016b. 'FBI v. Apple is a security and privacy issue. What about civil rights?', 15 March. As of 17 July 2017: <https://arstechnica.com/tech-policy/2016/03/fbi-v-apple-is-a-security-and-privacy-issue-what-about-civil-rights/>
- Landau, Susan. 2013. 'Making sense from Snowden: What's significant in the NSA surveillance revelations.' *IEEE Security & Privacy* 11(4): 54-63. As of 1 November 2017: [http://www.cs.siu.edu/~wwhite/IS376/ReadingAssignments/0930\\_MakingSenseFromSnowden.pdf](http://www.cs.siu.edu/~wwhite/IS376/ReadingAssignments/0930_MakingSenseFromSnowden.pdf)
- Layton, Peter. 2012. 'The Idea of Grand Strategy.' *The RUSI Journal* 157(4): 56-61. doi:10.1080/03071847.2012.714193 As of 31 October 2017:
- Let's Encrypt. N.d. 'About Let's Encrypt.' As of 13 November 2017: <https://letsencrypt.org/about/>
- Lyon, David. 2014. 'Surveillance, Snowden, and big data: Capacities, consequences, critique.' *Big Data & Society* 1(2).
- MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies & James Ball. 2013. 'GCHQ taps fibre-optic cables for secret access to world's communications.' 21 June. As of 7 July 2017: <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

- Merry, Paul, Matthew Smith, Matthew Martindale & Arturs Kokins. 2017. *Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age*. KPMG. As of 13 November 2017: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf>
- Microsoft. 2012. 'Security Development Lifecycle for Agile Development.' As of 17 July 2017: <https://msdn.microsoft.com/en-us/library/ee790621.aspx>
- \_\_\_\_\_. 2017. 'Microsoft Security Updates.' As of 10 November 2017: <https://technet.microsoft.com/en-us/security/bulletins.aspx>
- Nakashima, Ellen, & Jack Gillum. 2017. 'U.S. moves to ban Kaspersky software in federal agencies amid concerns of Russian espionage.' *The Washington Post*, 3 September. As of 10 November 2017: [https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152\\_story.html?utm\\_term=.eb819077f852](https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.eb819077f852)
- Natural Resource Governance Institute. 2015. 'Legal Framework: Navigating the Web of Laws and Contracts Governing Extractive Industries.' March. As of 17 July 2017: [https://resourcegovernance.org/sites/default/files/nrgi\\_Legal-Framework.pdf](https://resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf)
- NCCoE (National Cybersecurity Center of Excellence). 2017. 'About the Center.' As of 10 November 2017: <https://nccoe.nist.gov/about-the-center>
- NERC (North American Electric Reliability Corporation). 2016a. 'Home page.' As of 1 November 2017: [www.nerc.com](http://www.nerc.com)
- \_\_\_\_\_. 2016b. 'Reliability Standards.' As of 1 November 2017: [www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx](http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx)
- Newman, Lily Hay. 2016. 'What we know about Friday's massive east coast internet outage.' 21 October. As of 17 July 2017: <https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/>
- NISCC (National Infrastructure Security Co-ordination Centre). 2006. *Good Practice Guide to Telecommunications Resilience*. As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/85910/flu\\_niscc.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85910/flu_niscc.pdf)
- NIST (National Institute of Standards Technology). 2008. 'BitLocker Drive Encryption Security Policy: For FIPS 140-2 Validation.' As of 10 November 2017: <https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp947.pdf>
- \_\_\_\_\_. 2011. 'Managing Information Security Risk: Organization, Mission, and Information System View.' As of 10 November 2017: <https://csrc.nist.gov/publications/detail/sp/800-39/final>
- \_\_\_\_\_. 2016. 'National Standards Bodies.' 25 August. As of 31 October 2017: <https://www.nist.gov/iaao/national-standards-bodies>
- \_\_\_\_\_. N.d.-a. 'Computer Security Resource Center.' As of 13 November 2017: <https://csrc.nist.gov/>

- \_\_\_\_\_. N.d.-b. 'Computer Security Special Publications.' As of 1 November 2017: <http://csrc.nist.gov/publications/PubsSPs.html>
- \_\_\_\_\_. N.d.-c. 'Cybersecurity Framework.' As of 10 November 2017: <https://www.nist.gov/cyberframework>
- Northcutt, Stephen. 2009. 'Security Controls.' *SANS Technology Institute*. As of 10 November 2017: <https://www.sans.edu/cyber-research/security-laboratory/article/security-controls>
- NSA. 2016. 'Centers of Academic Excellence in Cybersecurity.' As of 10 November 2017: <https://www.nsa.gov/resources/educators/centers-academic-excellence/>
- Nye, Joseph S. 2014. 'The regime complex for managing global cyber activities.'
- NZ, Coding. 2017. 'Home page.' As of 10 November 2017: <http://codingnz.com/>
- Pressman, Roger. 2009. *Agile Development*. As of 10 November 2017: <http://nlp.chonbuk.ac.kr/SE/ch05.pdf>
- Regenscheid, Andrew R. 2016. *NIST Cryptographic Standards and Guidelines Development Process*. NIST. NISTIR-7977. As of 10 November 2017: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf>
- Robles, Rosslin John, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park & J Lee. 2008. 'Common threats and vulnerabilities of critical infrastructures.' *International journal of control and automation* 1(1): 17-22.
- Ross, Ronald. 2012. *Guide for Conducting Risk Assessments*. NIST. As of 10 November 2017: <https://www.nist.gov/publications/guide-conducting-risk-assessments>
- Rothwell, Richard. 2008. 'Creating wealth with free software.' *Free Software Magazine*, 5 August. As of 31 October 2017: [http://freesoftwaremagazine.com/articles/creating\\_wealth\\_free\\_software/](http://freesoftwaremagazine.com/articles/creating_wealth_free_software/)
- Sedgewick, Adam, Murugiah Souppaya & Karen Scarfone. 2017. *Guide to Application Whitelisting*. NIST. 800-167. As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>
- Souppaya, Murugiah, & Karen Scarfone. 2013. *Guidelines for managing the security of mobile devices in the enterprise*. NIST. 800-124. As of 10 November 2017: [https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise?pub\\_id=913427](https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise?pub_id=913427)
- Spamhaus. 2017. 'The 10 Worst Spammers.' 17 July 2017. As of 17 July 2017: <https://www.spamhaus.org/statistics/spammers/>
- Specialty, Allianz Global Corporate &. 2016. *A Guide to Cyber Risk*. Allianz. As of 31 October 2017: <http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf>
- Stoneburner, Gary. 2001. *Underlying technical models for information technology security*. NIST. 800-33. As of 13 November 2017: <https://csrc.nist.gov/publications/detail/sp/800-33/final>

- Symantec. 2010. 'Patch Management Best Practices.' As of 10 November 2017: [https://support.symantec.com/en\\_US/article.HOWTO3124.html](https://support.symantec.com/en_US/article.HOWTO3124.html)
- \_\_\_\_\_. 2017. 'Encryption, powered by PGP.' As of 10 November 2017: <https://www.pgp.com/>
- UK Government. 2015. 'Cyber security insurance: new steps to make UK world centre.' 23 March. As of 17 July 2017: <https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre>
- \_\_\_\_\_. 2016a. 'Agile delivery.' As of 17 July 2017: <https://www.gov.uk/service-manual/agile-delivery>
- \_\_\_\_\_. 2016b. 'Protect your business against cyber threats.' As of 1 November 2017: [www.cyberstreetwise.com/cyberessentials/](http://www.cyberstreetwise.com/cyberessentials/)
- \_\_\_\_\_. 2017. 'Students urged to apply for pioneering Cyber Schools Programme.' As of 31 October 2017: <https://www.gov.uk/government/news/students-urged-to-apply-for-pioneering-cyber-schools-programme>
- UN Development Programme. N.d. 'Sustainable Development Goals.' As of 10 November 2017: <http://www.undp.org/content/undp/en/home/sustainable-development-goals.html>
- United Nations General Assembly. 2011. *Resolution 33/2011. Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children.* 2011/33. As of 1 November 2017: <http://www.un.org/en/ecosoc/docs/2011/res%202011.33.pdf>
- UNODA (United Nations Office for Disarmament Affairs). 2017. 'Developments in the field of information and telecommunications in the context of international security.' As of 31 October 2017: <https://www.un.org/disarmament/topics/informationsecurity/>
- US Department of Homeland Security. 2008. 'Recommended Practice for Patch Management of Control Systems.' As of 10 November 2017: [https://ics-cert.us-cert.gov/sites/default/files/recommended\\_practices/RP\\_Patch\\_Management\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf)
- \_\_\_\_\_. 2013. 'Information Technology Sector-Specific Plan: An Annex to the NIPP 2013 '. As of 17 July 2017: <https://www.dhs.gov/publication/nipp-ssp-information-technology-2016>
- \_\_\_\_\_. 2016. 'Strategic Principles for securing the Internet of Things (IoT).' 15 November. As of 17 July 2017: [https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Interne\\_t\\_of\\_Things-2016-1115-FINAL....pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Interne_t_of_Things-2016-1115-FINAL....pdf)
- \_\_\_\_\_. 2017a. 'Cybersecurity Insurance.' As of 17 July 2017: <https://www.dhs.gov/cybersecurity-insurance>
- \_\_\_\_\_. 2017b. 'Cybersecurity Workforce Development Resources.' 17 October. As of 31 October 2017: <https://www.dhs.gov/cybersecurity-workforce-development-resources>

- \_\_\_\_\_. 2017c. 'National Cyber Security Awareness Month.' As of 17 July 2017: <https://www.dhs.gov/national-cyber-security-awareness-month>
- \_\_\_\_\_. N.d. 'Communications Sector.' As of 10 November 2017: <https://www.dhs.gov/communications-sector>
- US Department of Justice. 2017. 'Justice Department Announces Actions to Dismantle Kelihos Botnet.' 10 April. As of 17 July 2017: <https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0>
- Van Eeten, Michel, Johannes M Bauer, Hadi Asghari, Shirin Tabatabaie & David Rand. 2010. 'The role of internet service providers in botnet mitigation an empirical analysis based on spam data.' *TPRC 2010*. As of 31 October 2017: <https://ssrn.com/abstract=1989198>
- Voldal, Daniel. 2003. *A Practical Methodology for Implementing a Patch management Process*. InfoSec Reading Room: SANS Institute. As of 10 November 2017: <https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206>
- W3C. 2017. 'About W3C.' As of 31 October 2017: <https://www.w3.org/Consortium/>
- Ward, Dan, & Robert Morgus. 2016. *Professor Cy Burr's Graphic Guide to: International Cyber Norms*. New America. As of 1 November 2017: <https://na-production.s3.amazonaws.com/documents/CyberNorms11.14.pdf>
- Wayra. N.d. 'GCHQ Cyber Accelerator.' As of 10 November 2017: <https://wayra.co.uk/gchq/>
- Weingart, Steve H. 2000. 'Physical security devices for computer subsystems: A survey of attacks and defenses.' *International Workshop on Cryptographic Hardware and Embedded Systems*: 302-17. As of 31 October 2017: [https://link.springer.com/content/pdf/10.1007/3-540-44499-8\\_24.pdf](https://link.springer.com/content/pdf/10.1007/3-540-44499-8_24.pdf)
- West-Brown, Molra J, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece & Robin Ruefle. 2003. 'Handbook for computer security incident response teams (csirts).' As of 17 July 2017: [http://resources.sei.cmu.edu/asset\\_files/Handbook/2003\\_002\\_001\\_14102.pdf](http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf)
- Whitney, Lance. 2011. 'Microsoft Patch Tuesday to target Windows, IE.' *Cnet*, 10 October. As of 31 October 2017: <https://www.cnet.com/news/microsoft-patch-tuesday-to-target-windows-ie/>
- World Bank. 2014. 'The Korean Trust Fund on ICT4D.' 18 June. As of 10 November 2017: <http://www.worldbank.org/en/topic/ict/brief/the-korean-trust-fund-on-ict4d>
- \_\_\_\_\_. 2017. 'Information & Communication Technologies.' As of 10 November 2017: <http://www.worldbank.org/en/topic/ict/overview>
- Yale Information Technology Services. 2017. 'Physical security for desktop computers.' As of 31 October 2017: <https://its.yale.edu/secure-computing/security-standards-and-guidance/device-security/physical-security-devices/physical-security-desktop-computers>

## Full reference list

---

- (ISC)<sup>2</sup> (International Information System Security Certification Consortium). 2017. 'Certified Cyber Forensics Professional.' As of 13 November 2017: <https://www.isc2.org/Certifications/CCFP>
- Acar, Yasemin, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek & Christian Stransky. 2017. 'How Internet Resources Might Be Helping You Develop Faster but Less Securely.' *IEEE Security & Privacy* 15(2): 50-60.
- ACORN (Australian Cybercrime Online Reporting Network). N.d. 'Home page.' As of 10 November 2017: <https://www.acorn.gov.au/>
- Action Fraud. N.d. 'About Us.' As of 9 November 2017: <https://www.actionfraud.police.uk/about-us/who-we-are>
- AfricaCERT. N.d. 'About Us.' As of 9 November 2017: <https://www.africacert.org/home/about-us/>
- APCERT. 2017. 'Mission Statement.' As of 9 November 2017: <https://www.apcert.org/about/mission/index.html>
- APMG International. 2017. 'Accreditation.' As of 31 October 2017: <https://apmg-international.com/our-services/accreditation>
- APWG (Anti-Phishing Working Group). 2017. 'About APWG.' As of 9 November 2017: <https://www.antiphishing.org/about-APWG/>
- ARIN (American Registry for Internet Numbers). 2017. 'Regional Internet Registries.' As of 31 October 2017: <https://www.arin.net/knowledge/rirs.html>
- Australian Department of Defence. 2013. 'Top 4 strategies to mitigate targeted cyber intrusions: Mandatory requirements explained.' 2017. As of 17 July 2017: <https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>
- AXELOS. N.d. 'Global Best Practice Solutions.' As of 31 October 2017: <https://www.axelos.com/>
- Bada, Maria, Angela Sasse & Jason Nurse. 2014. 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?' *Global Cyber Security Capacity Centre*. As of 31 October 2017: <http://discovery.ucl.ac.uk/1468954/>
- Bandos, Tim. 2017. 'The Five Steps of Incident Response.' *DigitalGuardian*, 27 July. As of 13 November 2017: <https://digitalguardian.com/blog/five-steps-incident-response>

Bayuk, Jennifer L, Jason Healey, Paul Rohmeyer, Marcus H Sachs, Jeffrey Schmidt & Joseph Weiss. 2012. *Cyber security policy guidebook*. John Wiley & Sons.

BBC. 2014. 'GCHQ accredits UK master's degrees for 'cyber spies'.' *BBC*, 2 August. As of 10 November 2017: <http://www.bbc.com/news/uk-28623365>

Bennett, Alex. 2017. 'Cybersecurity in 2025: the skills we'll need to tackle threats of the future.' *Wired*, 4 April. As of 31 October 2017: <http://www.wired.co.uk/article/cybersecurity-2025-skills-risks>

Berejka, Marc, & Ari M Schwartz. 2011. 'Cybersecurity, Innovation and the Internet Economy.' As of 17 July 2017: [http://www.nisc.go.jp/eng/pdf/actionplan\\_ci\\_eng\\_v3.pdf](http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf)

Bertot, John Carlo, Paul T Jaeger & Derek Hansen. 2012. 'The impact of polices on government social media usage: Issues, challenges, and recommendations.' *Government information quarterly* 29(1): 30-40.

Black, Paul E, Lee Badger, Barbara Guttman & Elizabeth Fong. 2016. *Dramatically Reducing Software Vulnerabilities*. NIST. NISTIR 8151. As of 10 November 2017: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf>

BLS (United States Bureau of Labor Statistics). 2015. 'Labor force characteristics by race and ethnicity, 2014.' *US Bureau of Labor Statistics* November(Report 1057). As of 31 October 2017: <https://www.bls.gov/opub/reports/race-and-ethnicity/archive/labor-force-characteristics-by-race-and-ethnicity-2014.pdf>

BSA. 2015. *Asia-Pacific Cybersecurity Dashboard. A Path to a Secure Global Cyberspace*. Washington, DC: BSA Worldwide. As of 31 October 2017: [http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study\\_apac\\_cybersecurity\\_en.pdf](http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf)

Carr, Madeline. 2016. 'Public-private partnerships in national cyber-security strategies.' *International Affairs* 92(1): 43-62. As of 31 October 2017: [https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92\\_1\\_03\\_Carr.pdf](https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf)

Cătălui, Daria. 2014. *Public Private Partnerships in Network and Information Security Education*. ENISA. As of 31 October 2017: <https://www.enisa.europa.eu/publications/public-private-partnerships-in-network-and-information-security-education>

CBPRs (Cross Border Privacy Rules System). N.d. 'Home page.' As of 9 November 2017: <http://www.cbprs.org/>

Central District of California United States Attorney's Office. 2017. 'The Cybersecurity Program.' 18 October. As of 31 October 2017: <https://www.justice.gov/usao-cdca/cybersecurity-program>

Centres of Academic Excellence in Cybersecurity Community. 2017. 'Home page.' As of 31 October 2017: <https://www.caecommunity.org/>

CERT. 2017. 'SEI CERT Coding Standards.' As of 10 November 2017: <https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards>

- Cichonski, Paul, Tom Millar, Tim Grance & Karen Scarfone. 2012. *Computer security incident handling guide*. NIST. 800-61. As of 13 November 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- Cole, Jennifer, & Edward Hawker. 2014. 'Emergency Services Communications: Resilience for the Twenty-First Century.' As of 17 July 2017: [https://rusi.org/sites/default/files/201405\\_op\\_emergency\\_services\\_communications.pdf](https://rusi.org/sites/default/files/201405_op_emergency_services_communications.pdf)
- College of Policing. N.d. 'Digital and cyber crime.' As of 10 November 2017: [http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-cri-me/Pages/Digital-and-cyber\\_crime.aspx](http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-cri-me/Pages/Digital-and-cyber_crime.aspx)
- Constantin, Lucian. 2014. '5 things you need to know about cybersecurity insurance.' 25 April. <http://www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html>
- Correia, John, & Deborah Compeau. 2017. 'Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA.' *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Council of Europe. 2008. 'Convention on Cybercrime.' *European Treaty Series* 185. As of 10 November 2017: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_17\\_c\\_onv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_17_c_onv_budapest_en.pdf)
- \_\_\_\_\_. 2017a. 'International Cooperation against Cybercrime.' As of 17 July 2017: <https://www.coe.int/en/web/cybercrime/international-cooperation>
- \_\_\_\_\_. 2017b. 'Law enforcement - Internet service provider Cooperation.' As of 17 July 2017: <https://www.coe.int/en/web/cybercrime/lea/-isp-cooperation>
- CPNI (Centre for the Protection of National Infrastructure). 2017. 'Supply Chain.' As of 31 October 2017: <https://www.cpni.gov.uk/supply-chain>
- CPS (The Crown Prosecution Service). N.d. 'Cybercrime - Legal Guidance.' As of 10 November 2017: [http://www.cps.gov.uk/legal/a\\_to\\_c/cybercrime/](http://www.cps.gov.uk/legal/a_to_c/cybercrime/)
- Craiger, J Philip. 2005. 'Computer forensics procedures and methods.' In *Handbook of Information Security*, Edited by H. Bigdoli. New York: John Wiley & Sons. As of 10 November 2017: <http://www.cyberace.org/Publications/craiger.forensics.methods.procedures.DRAFT.pdf>
- Creasey, Jason. 2013. *Cyber Security Incident Response Guide*. CREST. As of 13 November 2017: <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>
- Cyber Security Challenge UK. 2017. 'Novice Toolkit.' As of 31 October 2017: <https://cybersecuritychallenge.org.uk/novice-toolkit>
- CyberSecurity Malaysia. 2017. 'CyberSAFE.' As of 31 October 2017: <http://www.cybersafe.my/en/>
- CyberSeek. N.d. 'Hack the Gap: Close the cybersecurity talent gap with interactive tools and data.' As of 31 October 2017: <http://cyberseek.org/index.html>

- Daly, Kathleen, & Rick Sarre. 2017. 'Criminal justice system: Aims and processes.' In *Crime and Justice: A Guide to Criminology*, Edited by Darren Palmer, Williem de Lint & Derek Dalton. Sydney: Lawbook Co. As of 10 November 2017: [https://www.griffith.edu.au/\\_data/assets/pdf\\_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf](https://www.griffith.edu.au/_data/assets/pdf_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf)
- Defence Academy of the United Kingdom. 2017. 'Defence Cyber School.' As of 9 November 2017: <https://www.da.mod.uk/colleges-schools/technology-school/defence-cyber-school>
- Deloitte. 2015. *The Deloitte Consumer Review: Consumer data under attack: The growing threat of cyber crime.* As of 10 November 2017: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf>
- Dutch Ministry of Defence. 2012. 'The Defence Cyber Strategy.' As of 10 November 2017: [https://ccdcoe.org/strategies/Defence\\_Cyber\\_Strategy\\_NDL.pdf](https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf)
- e-Estonia. 2017. 'Estonia to open the world's first data embassy in Luxembourg.' *e-estonia*, June. As of 10 November 2017: <https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/>
- EC-Council. 2017a. 'About Us.' As of 13 November 2017: <https://www.eccouncil.org/about/>
- \_\_\_\_\_. 2017b. 'Accreditations.' As of 31 October 2017: <https://www.eccouncil.org/accreditations/>
- \_\_\_\_\_. 2017c. 'Handle Security Incidents: Become an ECIH.' As of 13 November 2017: <https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/>
- EFF. N.d.-a. 'How to Deploy HTTPS Correctly.' As of 10 November 2017: <https://www.eff.org/https-everywhere/deploying-https>
- \_\_\_\_\_. N.d.-b. 'HTTPS Everywhere.' As of 10 November 2017: <https://www.eff.org/https-everywhere/>
- \_\_\_\_\_. N.d.-c. 'HTTPS Everywhere FAQ.' As of 10 November 2017: <https://www.eff.org/https-everywhere/faq>
- Ehuan, Art, & Alvarez & Marshall. 2016. *Managing the effectiveness of a cyber security program through a nist cyber security framework evaluation*. OAS: Global Cyber Risk Services LLC. As of 10 November 2017: <https://www.sites.oas.org/cyber/Documents/2016%20-%20Gestionando%20la%20efectividad%20de%20un%20Programa%20de%20Ciberseguridad%20utilizando%20las%20normas%20NIST-Art%20Ehuan.pdf>
- Emergency Communications Preparedness Centre. 2016. 'Federal Financial Assistance Reference Guide.' As of 17 July 2017: [https://www.911.gov/pdf/2016\\_ECPC\\_Reference\\_Guide.pdf](https://www.911.gov/pdf/2016_ECPC_Reference_Guide.pdf)
- ENISA (European Union Agency for Network and Information Security). 2006a. 'A step-by-step approach on how to set up a CSIRT.' As of 17 June 2017: [https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at\\_download/fullReport](https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport)

- \_\_\_\_\_. 2006b. 'A step-by-step approach on how to set up a CSIRT.' [https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at\\_download/fullReport](https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport)
- \_\_\_\_\_. 2007. *Information security awareness initiatives: Current proactive and the measurement tools.*
- \_\_\_\_\_. 2009. 'National Exercise - Good Practice Guide.' December. As of 17 June 2017: <https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide>
- \_\_\_\_\_. 2013a. 'National-level Risk Assessments: An Analysis Report.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/nlra-analysis-report>
- \_\_\_\_\_. 2013b. 'Recommended cryptographic measures.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securin-perso-nal-data>
- \_\_\_\_\_. 2014a. 'Algorithms, key size and parameters report 2014.' 21 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>
- \_\_\_\_\_. 2014b. 'Methodologies for the identification of Critical Information Infrastructure assets and services.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis>
- \_\_\_\_\_. 2014c. 'Report on Cyber Crisis Cooperation and Management.' 6 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/ccc-study>
- \_\_\_\_\_. 2014d. *Roadmap for NHS education programmes in Europe.* As of 31 October 2017: [https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe/at\\_download/fullReport](https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe/at_download/fullReport)
- \_\_\_\_\_. 2014e. 'Study on cryptographic protocols.' 21 November. As of 17 June 2017: <https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols>
- \_\_\_\_\_. 2015a. 'Critical Information Infrastructures Protection approaches in EU.' July. As of 17 June 2017: <https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf>
- \_\_\_\_\_. 2015b. *Status of privacy and NIS course curricula in EU Member States.* As of 31 October 2017: <https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-memb-er-states>
- \_\_\_\_\_. 2016a. 'Definition of Cybersecurity - Gaps and overlaps in standardisation.' As of 17 July 2017: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>
- \_\_\_\_\_. 2016b. 'Good Practice Guide on National Cyber Security Strategies.' As of 17 June 2017: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/good-practice-gui-de-on-national-cyber-security-strategies>
- \_\_\_\_\_. 2016c. 'New good practice guide by ENISA on disclosing vulnerabilities.' 18 January. As of 10 November 2017: <https://www.enisa.europa.eu/news/enisa-news/new-good-practice-guide-by-enisa-on-disclosing-vulnerabilities>

- \_\_\_\_\_. 2016d. 'Strategies for incident response and cyber crisis cooperation.' As of 17 June 2017: <https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation>
- \_\_\_\_\_. 2017. 'ENISA Threat Landscape Report 2016.' 8 February. As of 17 June 2017: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>
- EPIC (Electronic Privacy Information Center). 2017. 'Vulnerabilities Equities Process.' As of 10 November 2017: <https://epic.org/privacy/cybersecurity/vep/>
- EPSRC (Engineering and Physical Sciences Research Council). 2017. 'Academic Centres of Excellence in Cyber Security Research.' As of 31 October 2017: <https://www.epsrc.ac.uk/research/centres/acecybersecurity/>
- EU Council. 2008. 'On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.' 23 December. As of 17 July 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>
- EU Data Protection Regulation. 2015. 'Data Protection by Design and by Default.' As of 17 July 2017: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>
- European Commission. 2014. 'Working Document on surveillance of electronic communications for intelligence and national security purposes.' As of 17 July 2017: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf)
- \_\_\_\_\_. 2015. 'Risk Management Capability Assessment Guidelines.' As of 17 July 2017: [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)&from=EN)
- \_\_\_\_\_. N.d. 'Overview on Binding Corporate rules.' As of 9 November 2017: [http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm)
- European Cyber Security Month. N.d. 'Home page.' As of 9 November 2017: <https://cybersecuritymonth.eu/>
- European Parliament. 2016a. 'General Data Protection Regulation.' As of 17 July 2017: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en>
- \_\_\_\_\_. 2016b. 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46.' *Official Journal of the European Union (OJ)* 59: 1-88. As of 9 November 2017: [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)
- European Union, & Council of Europe. 2011. *Specialised cybercrime units: Good practice study*. Strasbourg, France: Directorate General of Human Rights and Rule of Law. As of 10 November 2017: <https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33>

- Europol. 2016. 'The relentless growth of cybercrime.' As of 17 July 2017: <https://www.europol.europa.eu/newsroom/news/reckless-growth-of-cybercrime>
- \_\_\_\_\_. 2017. 'European cybercrime centre - EC3.' As of 10 November 2017: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
- \_\_\_\_\_. N.d. 'Training and Capacity Building.' As of 10 November 2017: <https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building>
- FBI IC3 (Federal Bureau of Investigation Internet Crime Complaint Center). N.d. 'Home page.' As of 9 November 2017: <https://www.ic3.gov/about/default.aspx>
- Federal Emergency Management Agency. 2015. 'Fact sheet: Disaster emergency communications.' As of 17 July 2017: [https://www.fema.gov/media-library-data/1440617086804-f6489d2de59dddeba8bebc9b4d419009/DEC\\_June\\_2015.pdf](https://www.fema.gov/media-library-data/1440617086804-f6489d2de59dddeba8bebc9b4d419009/DEC_June_2015.pdf)
- Financial Industry Regulatory Authority. 2015. 'Report on Cybersecurity Practices.' As of 17 July 2017: <https://www.finra.org/file/report-cybersecurity-practices>
- FIRST. 2017. 'Mission Statement.' As of 9 November 2017: <https://www.first.org/about/mission>
- Fischer, Eric A. 2014. 'Cybersecurity Issues and challenges: in brief.' 12 August. As of 17 July 2017: <https://fas.org/sgp/crs/misc/R43831.pdf>
- Forensic Science Regulator. 2015. 'Newsletter.' October(26). As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/470526/FSR\\_Newsletter\\_26\\_October\\_2015.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470526/FSR_Newsletter_26_October_2015.pdf)
- Forensic Science Simplified. N.d. *A Simplified Guide To Digital Evidence*. NFSTC. As of 10 November 2017: <http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf>
- Fraunhofer Academy. 2017. 'Structure and Organization of Fraunhofer-Gesellschaft.' As of 31 October 2017: <https://www.fraunhofer.de/en/about-fraunhofer/profile-structure/structure-organization.html>
- \_\_\_\_\_. N.d. *Cybersecurity Training Lab.* As of 31 October 2017: [https://www.academy.fraunhofer.de/content/dam/academy/en/documents/Information%20und%20Kommunikation\\_en/Cybersecurity\\_Info\\_Brochure\\_2017\\_web.pdf](https://www.academy.fraunhofer.de/content/dam/academy/en/documents/Information%20und%20Kommunikation_en/Cybersecurity_Info_Brochure_2017_web.pdf)
- Friedland, Carsten, & Monika Muylkens, eds. 2009. *ITU e-Government Implementation Toolkit*. Geneva: ITU. As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/app/e-gov.html>
- Friedman, Sam, & Adam Thomas. 2017. 'Demystifying cyber insurance coverage.' *Deloitte Insights*, 23 February. As of 31 October 2017: <https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html>
- G7 Cyber Expert Group. 2016. 'G7 fundamental elements for cyber security.' As of 1 July 2017: <https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security>

- Gant, Jon P., ed. 2008. *Electronic government for developing countries*. Geneva: ITU. As of 17 July 2017: [http://www.itu.int/ITU-D/cyb/app/docs/e-gov\\_for\\_dev\\_countries-report.pdf](http://www.itu.int/ITU-D/cyb/app/docs/e-gov_for_dev_countries-report.pdf)
- Gasser, Urs, Nancy Gertner, Jack L Goldsmith, Susan Landau, Joseph S Nye, David O'Brien, Matthew G Olsen, Daphna Renan, Julian Sanchez & Bruce Schneider. 2016. *Don't Panic: Making Progress on the "Going Dark" Debate*. Harvard University: The Berkman Center for Internet & Society. As of 9 November 2017: [https://cyber.harvard.edu/pubrelease/dont-panic/Dont\\_Panic\\_Making\\_Progress\\_on\\_Going\\_Dark\\_Debate.pdf](https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)
- GCHQ. 2016. *GCHQ Certification of Cyber Security Training Courses*. NCSC. As of 10 November 2017: [https://www.ncsc.gov.uk/content/files/protected\\_files/document\\_files/GCT%20scheme%20-%20Course%20Content%20Criteria%20v2%200.pdf](https://www.ncsc.gov.uk/content/files/protected_files/document_files/GCT%20scheme%20-%20Course%20Content%20Criteria%20v2%200.pdf)
- \_\_\_\_\_. N.d. 'CyberFirst.' As of 31 October 2017: <https://www.gchq-careers.co.uk/early-careers/cyberfirst.html>
- GCSCC (Global Cyber Security Capacity Centre). 2014. 'Cyber security capability maturity model (CMM) - V1.2.' Oxford, 15 December. As of 17 July 2017: [https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201\\_2\\_0.pdf](https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf)
- \_\_\_\_\_. (Global Cyber Security Capacity Centre). 2017. *Cyber security capability maturity model for Nations (CMM): Revised Edition*. Oxford: University of Oxford. As of 13 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition\\_0902\\_2017\\_1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_0902_2017_1.pdf)
- GenCyber. N.d.-a. 'GenCyber: Girls in CybHER Security.' As of 31 October 2017: <http://www.gencybergirls.camp/about-us.html>
- \_\_\_\_\_. N.d.-b. 'Inspiring the Next Generation of Cyber Stars.' As of 31 October 2017: <https://www.gen-cyber.com/about/>
- GIAC Certifications (Global Information Assurance Certification). 2017a. 'GIAC Certified Handler (GCIH).' As of 13 November 2017: <https://www.giac.org/certification/certified-incident-handler-gcih>
- \_\_\_\_\_. 2017b. 'GIAC Information Security Certification - Program Overview.' As of 13 November 2017: <https://www.giac.org/about/program-overview>
- \_\_\_\_\_. 2017c. 'GIAC Response and Industrial Defense (GRID).' As of 13 November 2017: <https://www.giac.org/certification/response-industrial-defense-grid>
- GLACY (Global Action on Cybercrime). 2014. 'Good practice study: Cybercrime reporting mechanisms.' September. As of 17 July 2017: <https://rm.coe.int/168030287c>
- Goolsby, Rebecca. 2013. 'On Cybersecurity, Crowdsourcing, and Social Cyber-Attack.' 4 March. As of 17 July 2017: <https://www.wilsoncenter.org/publication/cybersecurity-crowdsourcing-and-social-cyber-attack>
- Gordon, Sarah, & Richard Ford. 2006. 'On the definition and classification of cybercrime.' *Journal in Computer Virology* 2(1): 13-20. As of 10 November 2017:

[https://www.griffith.edu.au/\\_data/assets/pdf\\_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf](https://www.griffith.edu.au/_data/assets/pdf_file/0011/924878/2017-Daly-and-Sarre-Criminal-Justice-System-FINAL-23-Oct-2016.pdf)

Government of Japan. 2015. *The Basic Policy of Critical Information Infrastructure Protection.* Cybersecurity Strategic Headquarters: Information Security Policy Council. As of 17 November 2017: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan\\_ci\\_eng\\_v3\\_r1.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_eng_v3_r1.pdf)

Government of the Netherlands. 2013a. *International Security Strategy.* As of 9 November 2017: <https://www.government.nl/documents/policy-notes/2013/06/21/international-security-strategy>

———. 2013b. *The Netherlands' Defence Industry Strategy.* As of 9 November 2017: <https://www.government.nl/topics/commissariat-for-military-production/documents/publications/2014/10/22/the-netherlands-defence-industry-strategy>

Hackmageddon. 2017. '2016 Cyber Attacks Statistics.' 19 January. As of 17 July 2017: <http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/>

Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis & Panagiotis Trimintzios. 2013. *Resilience of the internet interconnection ecosystem.* In *Economics of Information Security and Privacy III.* Springer.

Hall, Suzanne, Sloane Menkes & Emily Stapf. 2017. 'Women in Cybersecurity: Underrepresented, untapped potential.' PwC, 31 October, 07:14 EDT. As of 31 October 2017: <https://www.pwc.com/us/en/cybersecurity/women-in-cybersecurity.html>

Hodge, Neil. 2012. 'The EU: Privacy by Default.' *In-House Persp.* 8: 19. As of 17 July 2017: <https://www.ibanet.org/Document/Default.aspx?DocumentUid=83F52EA7-E19A-4E4B-A2E5-A77EDC535F6B>

Home Office. 2010. *Cyber Crime Strategy.* London:: UK Parliament. Cm 7842. As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228826/7842.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf)

IANA (Internet Assigned Numbers Authority). N.d. 'About Us.' As of 31 October 2017: <https://www.iana.org/about>

IAPP (International Association of Privacy Professionals). 2017. 'About the IAPP.' As of 31 October 2017: <https://iapp.org/about/>

ICANN (International Corporation for Assigned Names and Numbers). 2017. 'Get Started.' As of 31 October 2017: <https://www.icann.org/get-started>

ICC (International Chamber of Commerce). 2015. 'ICC Cyber Security Guide for Business.' As of 17 July 2017: <https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/>

ICMCP (International Consortium of Minority Cybersecurity Professionals). 2017. 'Home page.' As of 31 October 2017: <https://icmcp.org/>

IEC (International Electrotechnical Commission). 2017. 'Feeds/Alerts.' As of 13 November 2017: <http://www.iec.ch/subscribe/?ref=toplinks>

- IEEE Standards Association. 2016. 'Working Group Areas.' As of 10 November 2017: <http://grouper.ieee.org/groups/>
- . 2017. 'About Us.' As of 31 October 2017: <http://standards.ieee.org/about/ieesa.html>
- IEEE Xplore. 2017. 'IEEE GET Program.' As of 13 November 2017: <http://ieeexplore.ieee.org/browse/standards/get-program/page/?reload=true>
- IETF (Internet Engineering Task Force). 2017. 'Transport Layer Security (tls).' As of 17 July 2017: <https://datatracker.ietf.org/wg/tls/charter/>
- . N.d.-a. 'About the IETF.' As of 31 October 2017: <https://www.ietf.org/about/>
- . N.d.-b. 'Email Lists.' As of 13 November 2017: <https://www.ietf.org/list/>
- . N.d.-c. 'The IESG.' As of 31 October 2017: <https://www.ietf.org/iesg/>
- . N.d.-d. 'OpenPGP Message Format.' As of 10 November 2017: <https://tools.ietf.org/html/rfc4880>
- IISP. 2010. 'Information Security Skills Framework.' As of 10 November 2017: <https://www.iisp.org/imis15/CMDDownload.aspx?ContentKey=1c057e3e-05f0-4e65-9274-48722282033b&ContentItemKey=4952be86-df54-47f4-ada6-b89c3b81da41>
- Insafe. N.d. 'About Safer Internet Day.' As of 31 October 2017: <https://www.saferinternetday.org/web/sid/about>
- Intel. 2015. 'Understanding cyberthreat motivations to improve defences.' As of 17 July 2017: <https://www.mcafee.com/us/resources/deflect-targeted-attacks/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf>
- Interpol. 2017a. 'Activities.' As of 10 November 2017: <https://www.interpol.int/Crime-areas/Cybercrime/Activities/Digital-forensics>
- . 2017b. 'ASEAN Cyber Forensic Investigation Capability Project – first training course.' As of 10 November 2017: <https://www.interpol.int/News-and-media/Events/2015/ASEAN-Cyber-Forensic-Investigation-Capability-Project/ASEAN-Cyber-Forensic-Investigation-Capability-Project-%E2%80%93-first-training-course>
- . 2017c. 'The INTERPOL Global Complex for Innovation.' As of 10 November 2017: <https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI>
- ISO. 2011a. 'ISO/IEC 25010:2011.' As of 10 November 2017: <https://www.iso.org/standard/35733.html>
- . 2011b. 'ISO/IEC 27005:2011.' As of 31 October 2017: <https://www.iso.org/standard/56742.html>
- . 2012. 'ISO/IEC 27032:2012.' As of 31 October 2017: <https://www.iso.org/standard/44375.html>

- \_\_\_\_\_. 2013a. 'ISO/IEC 27001:2013.' As of 31 October 2017: <https://www.iso.org/standard/54534.html>
- \_\_\_\_\_. 2013b. 'ISO/IEC 30111:2013.' As of 10 November 2017: <https://www.iso.org/standard/53231.html>
- \_\_\_\_\_. 2014. 'ISO/IEC 29147:2014.' As of 10 November 2017: <https://www.iso.org/standard/45170.html>
- \_\_\_\_\_. 2015. 'ISO/IEC 27010:2015.' As of 10 November 2017: <https://www.iso.org/standard/68427.html>
- \_\_\_\_\_. 2017. 'ISO 20400:2017.' As of 10 November 2017: <https://www.iso.org/obp/ui/#iso:std:iso:20400:ed-1:v1:en>
- \_\_\_\_\_. N.d.-a. 'Freely Available Standards.' As of 10 November 2017: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
- \_\_\_\_\_. N.d.-b. 'Technical Committees.' As of 10 November 2017: <https://www.iso.org/technical-committees.html>
- ITU (International Telecommunications Union). 2008. 'Overview of Cybersecurity.' As of 10 November 2017: <http://www.itu.int/rec/T-REC-X.1205-200804-I>
- \_\_\_\_\_. 2010a. 'Approved ICT Security Standards.' As of 10 November 2017: [http://www.itu.int/itu-t/security/task\\_details.aspx?isn=3092&isnView=1&from=b1\\_2!b2\\_-1!b3\\_-1!t1\\_-1!k\\_security%20compendium](http://www.itu.int/itu-t/security/task_details.aspx?isn=3092&isnView=1&from=b1_2!b2_-1!b3_-1!t1_-1!k_security%20compendium)
- \_\_\_\_\_. 2010b. 'ITU Toolkit for Cybercrime Legislation.' As of 17 July 2017: <http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf>
- \_\_\_\_\_. 2010c. 'Security Roadmap Search.' As of 10 November 2017: [https://www.itu.int/ITU-T/security/main\\_table.aspx](https://www.itu.int/ITU-T/security/main_table.aspx)
- \_\_\_\_\_. 2011a. *ITU National Cybersecurity Strategy Guide*. Geneva, Switzerland: ITU. As of 1 November 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>
- \_\_\_\_\_. 2011b. *Understanding Cybercrime: A Guide For Developing Countries*. Geneva, Switzerland. As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html>
- \_\_\_\_\_. 2012. *Understanding cybercrime: Phenomena, challenges and legal response*. As of 17 July 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html>
- \_\_\_\_\_. 2014. 'The quest for cyber confidence.' As of 17 July 2017: <http://handle.itu.int/11.1002/pub/80b7079c-en>
- \_\_\_\_\_. 2015. 'National Spectrum Management.' As of 10 November 2017: <http://handle.itu.int/11.1002/pub/80c5a2ed-en>

- \_\_\_\_\_. 2017a. 'BRIDGING THE DIGITAL INNOVATION DIVIDE: A toolkit for strengthening ICT centric ecosystems.' As of 10 November 2017: [http://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Policy\\_Toolkit-Innovation\\_D012A0000D13301PDFE.pdf](http://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Policy_Toolkit-Innovation_D012A0000D13301PDFE.pdf)
- \_\_\_\_\_. 2017b. 'ITU-T Membership and Services.' As of 10 November 2017: <http://www.itu.int/en/ITU-T/membership/Pages/default.aspx>
- \_\_\_\_\_. 2017c. 'ITU-T Recommendations.' As of 31 October 2017: <http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx>
- \_\_\_\_\_. 2017d. 'Regional Cybersecurity Centres.' As of 10 November 2017: [http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Regional\\_Cybersecurity\\_Centre.aspx](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Regional_Cybersecurity_Centre.aspx)
- Jagasia, Arnav. 2017. 'A look into public private partnerships for cybersecurity.' *Public Policy Initiative*, Penn Wharton University of Pennsylvania, 18 April. As of 31 October 2017: <https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for>
- Johnson, Craig L. 2008. 'A framework for pricing government e-services.' *Electronic Commerce Research and Applications* 6(4): 484-9.
- Joint Forces Command. N.d. 'About Us.' UK Government. As of 9 November 2017: <https://www.gov.uk/government/organisations/joint-forces-command/about>
- Kick, Jason. 2014. 'Cyber Exercise Playbook.' November. As of 17 July 2017: [http://www.mitre.org/sites/default/files/publications/pr\\_14-3929-cyber-exercise-playbook.pdf](http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)
- Klimberg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication. As of 17 July 2017: <https://ccdcoc.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>
- Kornblum, Jesse. 2002. *Preservation of Fragile Digital Evidence by First Responders*. As of 10 November 2017: [http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/Jesse\\_Kornblum.pdf](http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/Jesse_Kornblum.pdf)
- KPMG. 2016. *Cyber Insurance: Are insurers finding growth or looking for trouble?* As of 31 October 2017: <https://assets.kpmg.com/content/dam/kpmg/us/pdf/cyber-insurance-whitepaper.pdf>
- Let's Encrypt. N.d. 'About Let's Encrypt.' As of 13 November 2017: <https://letsencrypt.org/about/>
- Libicki, Martin C, David Senty & Julia Pollak. 2014. *Hackers Wanted: an examination of the cybersecurity labor market*. Santa Monica, Calif.: Rand Corporation. RR-430. As of 31 October 2017: [https://www.rand.org/pubs/research\\_reports/RR430.html](https://www.rand.org/pubs/research_reports/RR430.html)
- Lord, Nate. 2017. 'Cybersecurity higher education: The top cybersecurity colleges and degrees.' *Digital Guardian*, 18 August. As of 31 October 2017: <https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees>

- Luijif, Eric, Tom van Schie, Theo van Ruijven & Auke Huistra. 2016a. 'The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.' As of 17 July 2017: <https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf>
- \_\_\_\_\_. 2016b. 'The GFCE-Meridian Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.' <https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf>
- Lyon, David. 2014. 'Surveillance, Snowden, and big data: Capacities, consequences, critique.' *Big Data & Society* 1(2).
- Malmedal, Bjarte, & Hanne Eggen Røislien. 2016. *The Norwegian Cyber Security Culture*. NorSIS. As of 10 November 2017: <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>
- Merry, Paul, Matthew Smith, Matthew Martindale & Arturs Kokins. 2017. *Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age*. KPMG. As of 13 November 2017: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf>
- Microsoft. 2013. 'Privacy by Default.' As of 17 July 2017: [http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy\\_by\\_default.pdf](http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy_by_default.pdf)
- \_\_\_\_\_. 2017. 'Microsoft Security Updates.' As of 10 November 2017: <https://technet.microsoft.com/en-us/security/bulletins.aspx>
- Microsoft Digital Crimes Unit. 2015. *Digital Crimes Unit Fact Sheet*. As of 10 November 2017: [https://news.microsoft.com/download/presskits/DCU/docs/dcufs\\_160115.pdf](https://news.microsoft.com/download/presskits/DCU/docs/dcufs_160115.pdf)
- Minárik, Tomáš. 2016. *National cyber security organisation: Czech Republic*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdoe.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_CZE\\_032016.pdf](https://ccdoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf)
- Ministère de l'Intérieur. N.d. 'Portail officiel de signalement des contenus illicites de l'Internet.' As of 9 November 2017: <https://www.internet-signalement.gouv.fr/PortalWeb/planets/Accueil!input.action>
- Nakashima, Ellen, & Jack Gillum. 2017. 'U.S. moves to ban Kaspersky software in federal agencies amid concerns of Russian espionage.' *The Washington Post*, 3 September. As of 10 November 2017: [https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152\\_story.html?utm\\_term=.eb819077f852](https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.eb819077f852)
- National Crime Agency. N.d. 'National Cyber Crime Unit.' As of 10 November 2017: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>
- NATO (North Atlantic Treaty Organization). 2017. 'NATO Cyber Defence Fact Sheet.' As of 9 November 2017:

[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2017\\_05/20170515\\_1705-factsheet-cyber-defence-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/20170515_1705-factsheet-cyber-defence-en.pdf)

NATO Cooperative Cyber Defence Centre of Excellence. N.d. 'Cyber Defence Training.' As of 31 October 2017: <https://ccdcoc.org/training.html>

NATO Industry Cyber Partnership. 2016. 'Objectives and Principles.' As of 9 November 2017: <http://www.nicp.nato.int/objectives-and-principles/index.html>

Natural Resource Governance Institute. 2015. 'Legal Framework: Navigating the Web of Laws and Contracts Governing Extractive Industries.' March. As of 17 July 2017: [https://resourcegovernance.org/sites/default/files/nrgi\\_Legal-Framework.pdf](https://resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf)

NCSC. 2015. 'GCHQ Certified Training.' 1 August 2016. As of 31 October 2017: <https://www.ncsc.gov.uk/scheme/gchq-certified-training>

\_\_\_\_\_. 2016. *Common cyber attacks: reducing the impact.* As of 13 November 2017: [https://www.ncsc.gov.uk/content/files/protected\\_files/guidance\\_files/common\\_cyber\\_attacks\\_ncsc.pdf](https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf)

\_\_\_\_\_. 2017a. 'About the NCSC.' 9 June. As of 31 October 2017: <https://www.ncsc.gov.uk/information/about-ncsc>

\_\_\_\_\_. 2017b. 'Cyber Security Information Sharing Partnership (CiSP).' 27 September 2016. As of 10 November 2017: <https://www.ncsc.gov.uk/cisp>

\_\_\_\_\_. 2017c. 'NCSC-certified degrees.' 12 August. As of 31 October 2017: <https://www.ncsc.gov.uk/information/ncsc-certified-degrees>

\_\_\_\_\_. 2017d. 'Public Private Partnerships.' 9 June 2017. As of 9 November 2017: <https://www.ncsc.nl/english/Cooperation/public-private-partnership.html>

Newman, Lily Hay. 2016. 'What we know about Friday's massive east coast internet outage.' 21 October. As of 17 July 2017: <https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/>

NICCS (National Initiative for Cybersecurity Careers and Studies). 2017. 'Cybersecurity.' 8 September 2017. As of 31 October 2017: <https://niccs.us-cert.gov/cybersecurity>

NICE (National Initiative for Cybersecurity Education). 2013. *2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report.* US Department of Homeland Security. As of 31 October 2017: <https://www.dhs.gov/cybersecurity-workforce-development-resources>

\_\_\_\_\_. 2017. *Cyber Ranges.* National Institute of Standards Technology. As of 31 October 2017: [https://www.nist.gov/sites/default/files/documents/2017/05/23/cyber\\_ranges\\_2017.pdf](https://www.nist.gov/sites/default/files/documents/2017/05/23/cyber_ranges_2017.pdf)

NISC (National Center of Incident Readiness and Strategy for Cybersecurity). 2014. 'The Basic Policy of Critical Information Infrastructure Protection.' 19 May. As of 17 July 2017: [http://www.nisc.go.jp/eng/pdf/actionplan\\_ci\\_eng\\_v3.pdf](http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf)

NISCC (National Infrastructure Security Co-ordination Centre). 2006. *Good Practice Guide to Telecommunications Resilience.* As of 10 November 2017:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/85910/flu\\_niscc.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85910/flu_niscc.pdf)

- NIST (National Institute of Standards Technology). 2008. 'BitLocker Drive Encryption Security Policy: For FIPS 140-2 Validation.' As of 10 November 2017: <https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp947.pdf>
- \_\_\_\_\_. 2011a. *Information Security*. NIST Special Publication 800-39. As of 17 July 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- \_\_\_\_\_. 2011b. 'Managing Information Security Risk: Organization, Mission, and Information System View.' As of 10 November 2017: <https://csrc.nist.gov/publications/detail/sp/800-39/final>
- \_\_\_\_\_. 2014. 'Framework for Improving Critical Infrastructure Cybersecurity.' 12 February. As of 17 July 2017: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- \_\_\_\_\_. 2016. 'National Standards Bodies.' 25 August. As of 31 October 2017: <https://www.nist.gov/iaao/national-standards-bodies>
- \_\_\_\_\_. 2017. 'NICE Cybersecurity Workforce Framework.' 19 October. As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>
- \_\_\_\_\_. N.d.-a. 'Computer Security Resource Center.' As of 13 November 2017: <https://csrc.nist.gov/>
- \_\_\_\_\_. N.d.-b. 'Cybersecurity Framework.' As of 10 November 2017: <https://www.nist.gov/cyberframework>
- \_\_\_\_\_. N.d.-c. 'Home page.' As of 31 October 2017: <https://www.nist.gov/>
- \_\_\_\_\_. N.d.-d. 'Information Technology Laboratory: Applied Cybersecurity Division.' As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity>
- Northcutt, Stephen. 2009. 'Security Controls.' *SANS Technology Institute*. As of 10 November 2017: <https://www.sans.edu/cyber-research/security-laboratory/article/security-controls>
- Norwegian Ministries. 2012. *Cyber Security Strategy for Norway*. As of 31 October 2017: [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway\\_Cyber\\_Security\\_StrategyNO.pdf](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway_Cyber_Security_StrategyNO.pdf)
- Nye, Joseph S. 2014. 'The regime complex for managing global cyber activities.'
- OAS (Organization of American States). 2015a. 'Best Practices for Establishing a National CSIRT.' April. As of 17 July 2017: <https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>

- \_\_\_\_\_. 2015b. *Cybersecurity awareness campaign toolkit*. As of 31 October 2017: [https://www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20\(English\).pdf](https://www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20(English).pdf)
- \_\_\_\_\_. 2016. *Best Practices for Establishing a National CSIRT*. As of 10 November 2017: <https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>
- Odinot, G, MA Verhoeven, RLD Pool & CJ de Poot. 2017. 'Organised Cybercrime in the Netherlands.' As of 17 July 2017: [https://www.wodc.nl/binaries/Cahier%202017-1\\_Full%20text\\_tcm28-244615.pdf](https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf)
- OECD (Organisation for Economic Co-operation and Development). 2007. 'OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.' As of 9 November 2017: <http://www.oecd.org/internet/ieconomy/38770483.pdf>
- \_\_\_\_\_. 2008. 'OECD Recommendations on the Protection of Critical Information Infrastructures.' As of 17 July 2017: <http://www.oecd.org/sti/ieconomy/ciip.htm>
- \_\_\_\_\_. 2012. 'High Level Risk Forum: Strategic Crisis Management.' 13-14 December. As of 17 July 2017: [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/HLRF\(2012\)3&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/HLRF(2012)3&docLanguage=En)
- \_\_\_\_\_. 2013. 'The OECD Privacy Framework.' As of 17 July 2017: [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
- \_\_\_\_\_. 2017. 'Key issues for digital transformation in the G20.' 12 January. As of 17 July 2017: <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>
- Oliker, Olga, Lynn E Davis, Keith Crane, Andrew Radin, Celeste Ward Gventer, Susanne Sondergaard, James T Quinlivan, Stephan B Seabrook, Jacopo Bellasio & Bryan Frederick. 2016. *Security Sector Reform in Ukraine*. Rand Corporation.
- Osula, Anna-Maria. 2015. *National cyber security organisation: United Kingdom*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdcoc.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_UK\\_032015\\_0.pdf](https://ccdcoc.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf)
- Oxley, Alan. 2011. 'A best practices guide for mitigating risk in the use of social media.' As of 17 July 2017: [https://ofti.org/wp-content/uploads/2012/07/71490\\_riskuseofsocialmedia.pdf](https://ofti.org/wp-content/uploads/2012/07/71490_riskuseofsocialmedia.pdf)
- Pârvu, Daniela, & Cristina Voicu-Olteanu. 2009. 'Advantages and limitations of the public private partnerships and the possibility of using them in Romania.' *Transylvanian Review of Administrative Sciences* 5(27): 189-98. As of 31 October 2017: [http://www.ucv.ro/pdf/invatamant/educatie/scoala\\_doctorala/pirvu\\_daniela/portofoliu/2.pdf](http://www.ucv.ro/pdf/invatamant/educatie/scoala_doctorala/pirvu_daniela/portofoliu/2.pdf)
- Pernik, Piret, Jesse Wojtkowiak & Alexander Verschoor-Kirss. 2016. *National cyber security organisation: United States*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. As of 9 November 2017: [https://ccdcoc.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_USA\\_122015.pdf](https://ccdcoc.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf)

Ponemon Institute. 2014. *2014 Best Schools for Cybersecurity*. Sponsored by HP Enterprise Security. As of 31 October 2017: [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_2014\\_Best\\_Schools\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf)

Prasanthi, Lakshmi, & Tata A S K Ishwarya. 2015. 'Cyber Crime: Prevention & Detection.' *International Journal of Advanced Research in Computer and Communication Engineering* 4(3). As of 10 November 2017: <https://www.ijarcce.com/upload/2015/march-15/IJARCCE%2011.pdf>

Prayudi, Yudi, Ahmad Ashari & Tri K Priyambodo. 2014. 'Digital evidence cabinets: A proposed framework for handling digital chain of custody.' *International Journal of Computer Applications* 107(9). As of 10 November 2017: [https://www.researchgate.net/profile/Yudi\\_Prayudi/publication/273131361\\_Digital\\_Evidence\\_Cabinets\\_A\\_Proposed\\_Framework\\_for\\_Handling\\_Digital\\_Chain\\_of\\_Custody/links/54f880130cf210398e96b370/Digital-Evidence-Cabinets-A-Proposed-Framework-for-Handling-Digital-Chain-of-Custody.pdf](https://www.researchgate.net/profile/Yudi_Prayudi/publication/273131361_Digital_Evidence_Cabinets_A_Proposed_Framework_for_Handling_Digital_Chain_of_Custody/links/54f880130cf210398e96b370/Digital-Evidence-Cabinets-A-Proposed-Framework-for-Handling-Digital-Chain-of-Custody.pdf)

Prayudi, Yudi, & Azhari Sn. 2015. 'Digital chain of custody: State of the art.' *International Journal of Computer Applications* 114(5). As of 10 November 2017: [https://www.researchgate.net/profile/Yudi\\_Prayudi/publication/273694917\\_Digital\\_Chain\\_of\\_Custody\\_State\\_of\\_The\\_Art/links/5508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf](https://www.researchgate.net/profile/Yudi_Prayudi/publication/273694917_Digital_Chain_of_Custody_State_of_The_Art/links/5508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf)

Pressman, Roger. 2009. *Agile Development*. As of 10 November 2017: <http://nlp.chonbuk.ac.kr/SE/ch05.pdf>

Purser, Steve. 2014. *Standards for Cyber Security*. IOS Press: ENISA. As of 31 October 2017: <https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security>

Queensland Government. 2016. 'Criminal Justice Framework: Guidelines for evaluating criminal justice initiatives.' As of 10 November 2017: <https://www.premiers.qld.gov.au/publications/categories/guides/assets/criminal-justice-evaluation-framework.pdf>

Raguseo, Domenico. 2017. 'The Future of Cybersecurity.' *SecurityIntelligence*, 10 February. As of 31 October 2017: <https://securityintelligence.com/the-future-of-cybersecurity/>

RAND Corporation. 2017. 'Military Doctrine.' As of 9 November 2017: <https://www.rand.org/topics/military-doctrine.html>

Regenscheid, Andrew R. 2016. *NIST Cryptographic Standards and Guidelines Development Process*. NIST. NISTIR-7977. As of 10 November 2017: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf>

Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle & Pablo Rodriguez. 2013. *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) : unclassified summary*. Santa Monica, Calif.: RAND Corporation. RR-286. [http://www.rand.org/pubs/research\\_reports/RR286.html](http://www.rand.org/pubs/research_reports/RR286.html)

- Robles, Rosslin John, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park & J Lee. 2008. 'Common threats and vulnerabilities of critical infrastructures.' *International journal of control and automation* 1(1): 17-22.
- Ross, Ronald. 2012. *Guide for Conducting Risk Assessments*. NIST. As of 10 November 2017: <https://www.nist.gov/publications/guide-conducting-risk-assessments>
- Sales, Nathan Alexander. 2012. 'Regulating cyber-security.' As of 1 November 2017: <http://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1/>
- SANS. 2017. 'World Leading Cyber Security Training.' As of 31 October 2017: <https://uk.sans.org/>
- SANS Digital Forensics and Incident Response. 2017. 'GIAC Computer Forensics Certifications.' As of 13 November 2017: <https://digital-forensics.sans.org/certification>
- Sedgewick, Adam, Murugiah Souppaya & Karen Scarfone. 2017. *Guide to Application Whitelisting*. NIST. 800-167. As of 31 October 2017: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>
- Simon, Tobby. 2017. 'Critical Infrastructure and the Internet of Things.' January. As of 17 July 2017: [https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46\\_0.pdf](https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf)
- Singapore Institute of Technology. 2017. 'Information and Communications Technology (Information Security), BEng (Hons).' As of 31 October 2017: <https://www.singaporetech.edu.sg/undergraduate-programmes/ict-information-security>
- Souppaya, Murugiah, & Karen Scarfone. 2013. *Guidelines for managing the security of mobile devices in the enterprise*. NIST. 800-124. As of 10 November 2017: [https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise?pub\\_id=913427](https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise?pub_id=913427)
- Staro, Sergio. 2010. *The G8 24/7 Network*. Italian delegation at the G8 Rome/Lyon Group (Subgroup on High Tech Crime). As of 10 November 2017: <https://rm.coe.int/16802fa06e>
- Stay Safe Online. 2017. 'Home page.' As of 17 July 2017: <https://staysafeonline.org>
- Stoneburner, Gary. 2001. *Underlying technical models for information technology security*. NIST. 800-33. As of 13 November 2017: <https://csrc.nist.gov/publications/detail/sp/800-33/final>
- Stop Think Connect. 2017. 'Home Page.' As of 17 July 2017: <https://www.stophinkconnect.org/>
- Suter, Manuel. 2007. 'A Generic National Framework For Critical Information Infrastructure Protection (CIIP).' August. As of 27 July 2017: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>
- Symantec. 2010. 'Patch Management Best Practices.' As of 10 November 2017: [https://support.symantec.com/en\\_US/article.HOWTO3124.html](https://support.symantec.com/en_US/article.HOWTO3124.html)
- . 2017. 'Encryption, powered by PGP.' As of 10 November 2017: <https://www.pgp.com/>

The Guardian. 2012. 'IT Governance Ltd.' *The Guardian*, 21 February. As of 31 October 2017: <https://www.theguardian.com/guardian-professional/2012/feb/21/it-governance-ltd>

The White House. 2016. 'FACT SHEET: Cybersecurity National Action Plan.' 9 February. As of 17 July 2017: <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

Tikk-Ringas, Eneken. 2015. *Legal Framework of Cyber Security*. In *Cyber Security: Analytics, Technology and Automation*. Springer. As of 1 November 2017: [https://link.springer.com/chapter/10.1007/978-3-319-18302-2\\_8](https://link.springer.com/chapter/10.1007/978-3-319-18302-2_8)

Tirrell, William K. 2012. *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?* : Army Command And General Staff Coll Fort Leavenworth Ks. As of 31 October 2017: <https://www.hsdl.org/?view&did=729810>

Trend Micro, & Organization of American States. 2015. *Cyber Security and Critical Infrastructure in the Americas*. Trend Micro Publication. As of 17 July 2017: [https://www.sites.oas.org/cyber/Certs\\_Web/OAS-Trend%20Micro%20Report%20on%20Cyber\\_security%20and%20CIP%20in%20the%20Americas.pdf](https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cyber_security%20and%20CIP%20in%20the%20Americas.pdf)

UK Cabinet Office. 2010. 'Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.' March. As of 17 July 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/62504/strategic-framework.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf)

\_\_\_\_\_. N.d. 'About Us.' As of 31 October 2017: <https://www.gov.uk/government/organisations/cabinet-office/about>

UK Centre for the Protection on National Infrastructure. 2017. 'Critical National Infrastructure.' As of 17 July 2017: <https://www.cpni.gov.uk/critical-national-infrastructure-0>

UK Government. 2010. *Cyber Crime Strategy*. Cm 7842. As of 10 November 2017: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228826/7842.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf)

\_\_\_\_\_. 2014a. 'Accreditation and conformity assessment: guidance for business and government departments.' As of 31 October 2017: <https://www.gov.uk/government/publications/accreditation-and-conformity-assessment-guidance-for-business-and-government-departments/>

\_\_\_\_\_. 2014b. *Serious and organised crime strategy*. As of 10 November 2017: <https://www.gov.uk/government/publications/serious-organised-crime-strategy>

\_\_\_\_\_. 2015a. 'Cyber security insurance: new steps to make UK world centre.' 23 March. <https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre>

\_\_\_\_\_. 2015b. *National Security Strategy and Strategic Defence and Security Review 2015*. Cm 9161. As of 1 November 2017: <https://www.eda.europa.eu/docs/default-source/procurement/uk-national-security-strategy-and-strategic-defence-security-review-2015.pdf>

- \_\_\_\_\_. 2016a. 'Agile delivery.' As of 17 July 2017: <https://www.gov.uk/service-manual/agile-delivery>
- \_\_\_\_\_. 2016b. 'Cyber Essentials.' As of 9 November 2017: <https://www.cyberaware.gov.uk/cyberessentials/faq.html>
- \_\_\_\_\_. 2016c. 'Cyber security training for business.' As of 31 October 2017: <https://www.gov.uk/government/collections/cyber-security-training-for-business>
- \_\_\_\_\_. 2016d. 'Millions invested in degree apprenticeships.' As of 31 October 2017: <https://www.gov.uk/government/news/millions-invested-in-degree-apprenticeships>
- \_\_\_\_\_. 2016e. 'National Cyber Security Strategy 2016 to 2021.' 11 September 2017. As of 10 November 2017: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>
- \_\_\_\_\_. 2017a. 'Extracurricular cyber clubs to inspire and identify tomorrow's cyber security professionals.' As of 31 October 2017: <https://www.gov.uk/government/news/extracurricular-cyber-clubs-to-inspire-and-identify-tomorrows-cyber-security-professionals>
- \_\_\_\_\_. 2017b. 'Students urged to apply for pioneering Cyber Schools Programme.' As of 31 October 2017: <https://www.gov.uk/government/news/students-urged-to-apply-for-pioneering-cyber-schools-programme>
- \_\_\_\_\_. N.d.-a. 'The Defence Science and Technology Laboratory (Dstl).' As of 9 November 2017: <https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory>
- \_\_\_\_\_. N.d.-b. 'Home Office: About Us.' As of 10 November 2017: <https://www.gov.uk/government/organisations/home-office/about>
- \_\_\_\_\_. N.d.-c. 'More about R-Cloud.' As of 9 November 2017: <https://rcloud.dstl.gov.uk/about>
- \_\_\_\_\_. N.d.-d. 'Office of Cyber Security and Information Assurance.' As of 31 October 2017: <https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance>
- \_\_\_\_\_. N.d.-e. 'View capability areas for research.' As of 9 November 2017: <https://rcloud.dstl.gov.uk/application/start>
- UK Government House of Commons Defence Committee. 2012. 'Defence and Cyber-Security: Sixth Report of Session 2012-13.' As of 10 November 2017: <https://publications.parliament.uk/pa/cm201213/cmselect/cmdefence/106/106.pdf>
- UK Ministry of Defence. 2017a. 'Defence Cyber Protection Partnership.' 26 October. As of 9 November 2017: <https://www.gov.uk/government/collections/defence-cyber-protection-partnership>
- \_\_\_\_\_. 2017b. 'Single departmental plan: 2015 to 2020.' As of 9 November 2017: <https://www.gov.uk/government/publications/mod-single-departmental-plan-2015-to-2020/single-departmental-plan-2015-to-2020>
- UK Ministry of Justice. 2014. *Transforming the Criminal Justice System Strategy and Action Plan – Implementation Update.* As of 10 November 2017:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/330690/cjs-strategy-action-plan.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330690/cjs-strategy-action-plan.pdf)

UK National Cyber Security Centre. 2016. 'We work for government and the Critical National Infrastructure.' 2 October. As of 17 July 2017: <https://www.ncsc.gov.uk/information/we-work-government-and-critical-national-infrastructure>

UK Parliament. 2014a. 'Chapter 2: Social media and the law.' As of 17 July 2017: <https://publications.parliament.uk/pa/l201415/lselect/lcomuni/37/3704.htm#note2>

\_\_\_\_\_. 2014b. 'How laws are made.' As of 10 November 2017: <http://www.parliament.uk/education/about-your-parliament/how-laws-are-made/>

\_\_\_\_\_. 2016. 'Digital Forensics and Crime.' As of 10 November 2017: <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0520>

UN Development Programme. N.d. 'Sustainable Development Goals.' As of 10 November 2017: <http://www.undp.org/content/undp/en/home/sustainable-development-goals.html>

UNCTAD. 2015. 'Information Economy Report.' As of 17 July 2017: [http://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf)

\_\_\_\_\_. 2016. 'Data protection regulations and international data flows: Implications for trade and development.' As of 17 July 2017: [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)

United States Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense. As of 31 October 2017: [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

UNODA (United Nations Office for Disarmament Affairs). 2017. 'Developments in the field of information and telecommunications in the context of international security.' As of 31 October 2017: <https://www.un.org/disarmament/topics/informationsecurity/>

UNODC. 2013. 'Comprehensive Study on Cybercrime.' February. [https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf)

US Department of Defence. 2015. 'The DOD Cyber Strategy.' As of 10 November 2017: [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

US Department of Homeland Security. 2013. 'Information Technology Sector-Specific Plan: An Annex to the NIPP 2013'. As of 17 July 2017: <https://www.dhs.gov/publication/nipp-ssp-information-technology-2016>

\_\_\_\_\_. 2014a. 'National Emergency Communications Plan.' As of 17 July 2017: [https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan\\_October%202014.pdf](https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%202014.pdf)

- \_\_\_\_\_. 2014b. *National Emergency Communications Plan*. As of 13 November 2017: [https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan\\_October%2029%202014.pdf](https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf)
- \_\_\_\_\_. 2016. 'Strategic Principles for securing the Internet of Things (IoT).' 15 November. As of 17 July 2017: [https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL....pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf)
- \_\_\_\_\_. 2017a. 'Cyber Storm: Securing Cyber Space.' 21 July. As of 9 November 2017: <https://www.dhs.gov/cyber-storm>
- \_\_\_\_\_. 2017b. 'Cybersecurity Insurance.' <https://www.dhs.gov/cybersecurity-insurance>
- \_\_\_\_\_. 2017c. 'Cybersecurity Workforce Development Resources.' 17 October. As of 31 October 2017: <https://www.dhs.gov/cybersecurity-workforce-development-resources>
- \_\_\_\_\_. 2017d. 'National Cyber Security Awareness Month.' As of 17 July 2017: <https://www.dhs.gov/national-cyber-security-awareness-month>
- \_\_\_\_\_. N.d. 'Communications Sector.' As of 10 November 2017: <https://www.dhs.gov/communications-sector>
- Van Eeten, Michel, Johannes M Bauer, Hadi Asghari, Shirin Tabatabaie & David Rand. 2010. 'The role of internet service providers in botnet mitigation an empirical analysis based on spam data.' *TPRC 2010*. As of 31 October 2017: <https://ssrn.com/abstract=1989198>
- Vandeven, Sally. 2014. *Forensic Images: For Your Viewing Pleasure*. InfoSec Reading Room: SANS Institute. As of 10 November 2017: <https://uk.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447>
- Voldal, Daniel. 2003. *A Practical Methodology for Implementing a Patch management Process*. InfoSec Reading Room: SANS Institute. As of 10 November 2017: <https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206>
- W3C. 2017. 'About W3C.' As of 31 October 2017: <https://www.w3.org/Consortium/>
- WEF (World Economic Forum). 2017. *Guidance on Public-Private Information Sharing against Cybercrime*. As of 10 November 2017: [http://www3.weforum.org/docs/WEF\\_Guidance\\_Cybercrime\\_report\\_2017.pdf](http://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf)
- West-Brown, Molra J, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece & Robin Ruefle. 2003. 'Handbook for computer security incident response teams (csirts).' [http://resources.sei.cmu.edu/asset\\_files/Handbook/2003\\_002\\_001\\_14102.pdf](http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf)
- Whitney, Lance. 2011. 'Microsoft Patch Tuesday to target Windows, IE.' *Cnet*, 10 October. As of 31 October 2017: <https://www.cnet.com/news/microsoft-patch-tuesday-to-target-windows-ie/>
- Wilson, Mark, & Joan Hash. 2003. 'Building an information technology security awareness and training program.' *NIST Special publication 800(50)*: 1-39.

- World Bank. 2014. 'The Korean Trust Fund on ICT4D.' 18 June. As of 10 November 2017: <http://www.worldbank.org/en/topic/ict/brief/the-korean-trust-fund-on-ict4d>
- \_\_\_\_\_. 2016. *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*. Washington, DC: The World Bank. As of 10 November 2017: <http://www.combattingcybercrime.org/>
- \_\_\_\_\_. 2017. 'Information & Communication Technologies.' As of 10 November 2017: <http://www.worldbank.org/en/topic/ict/overview>
- Yampolskiy, Roman. 2017. 'Ai is the future of cybersecurity, for better and for worse.' *Harvard Business Review*, 8 March. As of 31 October 2017: <https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse>



## Document endnotes

---

<sup>1</sup> Hathway & Spidalieri (2015).

<sup>2</sup> Klimberg (2012).

<sup>3</sup> Examples of frameworks include the following: US Department of Energy – Cybersecurity Capability Maturity Model (C2M2); Potomac Institute for Policy Studies – Cyber Readiness Index; ITU – ITU National Cybersecurity/Critical Information Infrastructure Protection Self-Assessment Tool; GCSCC – National Cybersecurity Capacity Maturity Model.

<sup>4</sup> The project team recognises that different types of stakeholders exist who would benefit from a toolbox such as this. However, for the purpose of this project, the research team focuses on the national cyber lead as a single stakeholder group or organisation type, in the development of the proof of concept of the method.

<sup>5</sup> GCSCC (2014).

<sup>6</sup> GCSCC (2014); GCSCC (2017).

<sup>7</sup> Oliker, Davis et al. (2016).

<sup>8</sup> ENISA (2016b, 4).

<sup>9</sup> ENISA (2017, 73). There are a wide range of motivations that drive these attacks, including personal financial gain, organisational gain, ideology, disgruntlement, coercion, notoriety, dominance, and personal satisfaction. See Intel (2015).

<sup>10</sup> For example, malware, ransomware, botnets, phishing, spam, identity theft, cyber espionage, insiders, exploit kit, and physical damage or theft. See ENISA (2017, 76).

<sup>11</sup> Hackmageddon (2017).

<sup>12</sup> ENISA (2016b).

<sup>13</sup> West-Brown et al. (2003, 10-1).

<sup>14</sup> West-Brown, Stikvoort et al. (2003, 10-1).

<sup>15</sup> West-Brown, Stikvoort et al. (2003, 10).

<sup>16</sup> Ehuan & Alvarez & Marshall (2016).

<sup>17</sup> Trend Micro & Organization of American States (2015, 34).

<sup>18</sup> West-Brown, Stikvoort et al. (2003, 17).

<sup>19</sup> Trend Micro & Organization of American States (2015, 35).

<sup>20</sup> Trend Micro & Organization of American States (2015, 36).

<sup>21</sup> West-Brown, Stikvoort et al. (2003, 17).

<sup>22</sup> Trend Micro & Organization of American States (2015, 39).

<sup>23</sup> Trend Micro & Organization of American States (2015, 40).

<sup>24</sup> ENISA (2016b, 2–12).

<sup>25</sup> “Internal organisations” are only relevant when the CSIRT is part of a larger host organisation.

<sup>26</sup> West-Brown, Stikvoort et al. (2003, 34-5).

<sup>27</sup> Ehuan & Alvarez & Marshall (2016).

<sup>28</sup> OAS (2016).

<sup>29</sup> OAS (2016).

<sup>30</sup> NIST (2017).

<sup>31</sup> OAS (2016).

<sup>32</sup> EC-Council (2017c).

<sup>33</sup> EC-Council (2017a).

<sup>34</sup> GIAC Certifications (2017a).

<sup>35</sup> GIAC Certifications (2017a).

<sup>36</sup> GIAC Certifications (2017b).

<sup>37</sup> GIAC Certifications (2017c).

<sup>38</sup> GIAC Certifications (2017c).

<sup>39</sup> (ISC)<sup>2</sup> (2017).

<sup>40</sup> (ISC)<sup>2</sup> (2017).

<sup>41</sup> SANS Digital Forensics and Incident Response (2017).

<sup>42</sup> OAS (2016).

<sup>43</sup> OAS (2016).

<sup>44</sup> ENISA (2016b, 26).

<sup>45</sup> See, for example: Cichonski et al. (2012, 21); Creasey (2013, 20); ENISA (2016d, 15); Bandos (2017).

<sup>46</sup> Cichonski, Millar et al. (2012, 21).

<sup>47</sup> Cichonski, Millar et al. (2012, 21).

<sup>48</sup> Bandos (2017).

<sup>49</sup> Creasey (2013, 38).

<sup>50</sup> Creasey (2013, 39).

<sup>51</sup> Creasey (2013, 40).

<sup>52</sup> Creasey (2013).

<sup>53</sup> Cichonski, Millar et al. (2012, 38–41).

<sup>54</sup> Cichonski, Millar et al. (2012, 41).

<sup>55</sup> Cichonski, Millar et al. (2012, 4).

<sup>56</sup> NCSC (2016, 7–11).

<sup>57</sup> Creasey (2013, 4).

<sup>58</sup> ENISA (2006b, 47-50).

<sup>59</sup> OAS (2016).

<sup>60</sup> ENISA (2006a, 56–60).

<sup>61</sup> ENISA (2006a, 34–45).

<sup>62</sup> ENISA (2016d, 29–30).

<sup>63</sup> FIRST (2017).

<sup>64</sup> ENISA (2016d, 29–30).

<sup>65</sup> APCERT (2017).

<sup>66</sup> AfricaCERT (N.d.).

<sup>67</sup> EU Council (2008).

<sup>68</sup> EU Council (2008).

<sup>69</sup> Luijif et al. (2016a, 10); ENISA (2014b, 22-4).

<sup>70</sup> Luijif, van Schie et al. (2016a, 30-2).

<sup>71</sup> Luijif, van Schie et al. (2016a, 1).

<sup>72</sup> Luijif, van Schie et al. (2016a, 31-2).

<sup>73</sup> Luijif, van Schie et al. (2016a, 30-1).

<sup>74</sup> US Department of Homeland Security (2016).

<sup>75</sup> Luijif, van Schie et al. (2016a, 21-7).

<sup>76</sup> Luijif, van Schie et al. (2016a, 31).

<sup>77</sup> Luijif, van Schie et al. (2016a, 1,5).

<sup>78</sup> Robles et al. (2008).

<sup>79</sup> Simon (2017, 2).

<sup>80</sup> Non-state actors include, for example, terrorist groups and transnational criminal organisations. The distinction between cyberwarfare, hacktivism and cybercrime is blurred. Source: Simon (2017, 4).

<sup>81</sup> Simon (2017, 2-4).

<sup>82</sup> Luijif, van Schie et al. (2016a, 17).

<sup>83</sup> Luijif, van Schie et al. (2016a, 14).

<sup>84</sup> Luijif, van Schie et al. (2016a, 39).

<sup>85</sup> ENISA (2015a).

<sup>86</sup> UK National Cyber Security Centre (2016); UK Centre for the Protection on National Infrastructure (2017).

<sup>87</sup> Based on structure in Luijif, van Schie et al. (2016a).

<sup>88</sup> Luijif, van Schie et al. (2016a, 39).

<sup>89</sup> Suter (2007, 11).

<sup>90</sup> Suter (2007, 11).

<sup>91</sup> Luijif, van Schie et al. (2016a, 15-8).

<sup>92</sup> Luijif, van Schie et al. (2016a, 14-8).

<sup>93</sup> Luijif, van Schie et al. (2016a, 17-8,49-57).

<sup>94</sup> Luijif, van Schie et al. (2016a, 13,21,9).

<sup>95</sup> Luijif, van Schie et al. (2016a, 21,9).

<sup>96</sup> Based on points discussed in Luijif et al. (2016b, 21).

<sup>97</sup> NIST (2011a).

<sup>98</sup> Luijif, van Schie et al. (2016a, 23).

<sup>99</sup> Luijif, van Schie et al. (2016b, 23-4).

<sup>100</sup> Luijif, van Schie et al. (2016b, 23-7).

<sup>101</sup> UK Cabinet Office (2010, 25–6).

<sup>102</sup> Luijif, van Schie et al. (2016a, 29).

<sup>103</sup> Luijif, van Schie et al. (2016a, 30-4).

<sup>104</sup> Luijif, van Schie et al. (2016a, 13-8); ENISA (2013a, 2).

<sup>105</sup> European Commission (2015).

<sup>106</sup> ENISA (2013a, 14).

<sup>107</sup> Luijif, van Schie et al. (2016a, 38).

<sup>108</sup> ENISA (2013a, 15); Luijif, van Schie et al. (2016a, 7,44).

<sup>109</sup> UK Cabinet Office (2010, 25–6).

<sup>110</sup> ENISA (2013a, iii).

<sup>111</sup> Luijif, van Schie et al. (2016a, 37,43).

<sup>112</sup> ENISA (2015a).

<sup>113</sup> OECD (2008, 8).

<sup>114</sup> OECD (2008, 14).

<sup>115</sup> Suter (2007).

<sup>116</sup> Luijif, van Schie et al. (2016a, 43).

<sup>117</sup> European Commission (2015).

<sup>118</sup> NIST (2014).

<sup>119</sup> European Commission (2015).

<sup>120</sup> Luijif, van Schie et al. (2016a, 43).

<sup>121</sup> Luijif, van Schie et al. (2016a, 37).

<sup>122</sup> NISC (2014).

<sup>123</sup> Luijif, van Schie et al. (2016a, 43).

<sup>124</sup> Luijif, van Schie et al. (2016a, 45).

<sup>125</sup> Luijif, van Schie et al. (2016a, 49).

<sup>126</sup> Luijif, van Schie et al. (2016a, 49).

<sup>127</sup> Luijif, van Schie et al. (2016a, 49).

<sup>128</sup> ENISA (2016d).

<sup>129</sup> Kick (2014).

<sup>130</sup> Kick (2014); BBK (2011)

<sup>131</sup> BBK (2011); Kick (2014)

<sup>132</sup> ENISA (2009)

<sup>133</sup> ENISA (2009, 36).

<sup>134</sup> ENISA (2009, 36).

<sup>135</sup> ENISA (2009, 38-9).

<sup>136</sup> ENISA (2009, 45).

<sup>137</sup> US Department of Homeland Security (2017a).

<sup>138</sup> ENISA (2009, 53).

<sup>139</sup> ENISA (2009, 55).

<sup>140</sup> ENISA (2009, 54).

<sup>141</sup> ENISA (2009, 54).

<sup>142</sup> ENISA (2009, 54).

<sup>143</sup> Dutch MOD (2012, 4).

<sup>144</sup> See for example the recognition of cyberspace as the fifth operational domain enshrined in the North Atlantic Treaty Organisation's (NATO) *Warsaw Summit Communiqué* (2016).

<sup>145</sup> Osula (2015).

<sup>146</sup> Joint Forces Command (N.d.).

<sup>147</sup> Minárik (2016, 11).

<sup>148</sup> Pernik et al. (2016, 19).

<sup>149</sup> UK Government House of Commons Defence Committee (2012, 11-2).

<sup>150</sup> UK Government House of Commons Defence Committee (2012, 11-2).

<sup>151</sup> UK Government (2016e, 38); US Department of Defence (2015, 3-4).

<sup>152</sup> UK Government House of Commons Defence Committee (2012, 11-2).

<sup>153</sup> Dutch Ministry of Defence (2012, 8).

<sup>154</sup> Dutch Ministry of Defence (2012, 14).

<sup>155</sup> Government of the Netherlands (2013a).

<sup>156</sup> Government of the Netherlands (2013b).

<sup>157</sup> UK Government (2015b).

<sup>158</sup> UK Ministry of Defence (2017b).

<sup>159</sup> This is based on both the Oxford Cybersecurity Maturity Model, Dutch and US cyber defence strategies. Sources: Dutch Ministry of Defence (2012); GCSOC (2014); US Department of Defence (2015).

<sup>160</sup> Dutch Ministry of Defence (2012, 10).

<sup>161</sup> US Department of Defence (2015, 23).

<sup>162</sup> UK Ministry of Defence (2017a).

<sup>163</sup> Dutch Ministry of Defence (2012, 11).

<sup>164</sup> Dutch Ministry of Defence (2012, 11).

<sup>165</sup> US Department of Defence (2015, 24).

<sup>166</sup> US Department of Defence (2015, 10).

<sup>167</sup> Dutch Ministry of Defence (2012, 15).

<sup>168</sup> Dutch Ministry of Defence (2012, 9).

<sup>169</sup> US Department of Defence (2015, 12).

<sup>170</sup> Dutch Ministry of Defence (2012).

<sup>171</sup> US Department of Defence (2015, 17-8).

<sup>172</sup> Defence Academy of the United Kingdom (2017).

<sup>173</sup> Robinson et al. (2013, 8).

<sup>174</sup> US Department of Defence (2015, 18).

<sup>175</sup> Dutch Ministry of Defence (2012, 15).

<sup>176</sup> NCSC (2017d).

<sup>177</sup> Dutch Ministry of Defence (2012).

<sup>178</sup> US Department of Defence (2015, 25).

<sup>179</sup> Dutch Ministry of Defence (2012, 15).

<sup>180</sup> GCSCC (2014, 23).

<sup>181</sup> US Department of Defence (2015, 25).

<sup>182</sup> NATO Industry Cyber Partnership (2016).

<sup>183</sup> Dutch Ministry of Security and Justice (2013).

<sup>184</sup> US Department of Defence (2015, 33).

<sup>185</sup> US Department of Defence (2015, 25).

<sup>186</sup> UK Government (N.d.-c).

<sup>187</sup> UK Government (N.d.-e).

<sup>188</sup> UK Government (N.d.-a).

<sup>189</sup> US Department of Defence (2015, 25).

<sup>190</sup> US Department of Defence (2015, 25).

<sup>191</sup> Kaska (2015).

<sup>192</sup> NATO (2017).

<sup>193</sup> RAND Corporation (2017).

<sup>194</sup> Robinson et al (2014, 7)

<sup>195</sup> Ormrod & Turnbull (2016)

<sup>196</sup> Ormrod & Turnbull (2016)

<sup>197</sup> Ling & van Dijk (2009)

<sup>198</sup> US DOD (2015, 19).

<sup>199</sup> Robinson et al. (2013).

<sup>200</sup> GCSCC (2014, 5).

<sup>201</sup> Cole & Hawker (2014, 39).

<sup>202</sup> OECD (2012, 6).

<sup>203</sup> OECD (2012, 11).

<sup>204</sup> OECD (2012, 4).

<sup>205</sup> OECD (2012, 6).

<sup>206</sup> ENISA (2014c, 20).

<sup>207</sup> Cole & Hawker (2014, 41); ENISA (2014c, 20).

<sup>208</sup> GCSCC (2014, 15).

<sup>209</sup> Cole & Hawker (2014, 41–2); ENISA (2014c, 47).

<sup>210</sup> Cole & Hawker (2014, 41).

<sup>211</sup> Cole & Hawker (2014, 39).

<sup>212</sup> Cole & Hawker (2014, 39–41).

<sup>213</sup> US Department of Homeland Security (2014b, 14,40–1).

<sup>214</sup> Cole & Hawker (2014, 16–21).

<sup>215</sup> US Department of Homeland Security (2014a, 20).

<sup>216</sup> Emergency Communications Preparedness Centre (2016, 9).

<sup>217</sup> Emergency Communications Preparedness Centre (2016, 12).

<sup>218</sup> US Department of Homeland Security (2014b, 38).

<sup>219</sup> OECD (2012, 6).

<sup>220</sup> GCSCC (2014, 15).

<sup>221</sup> Federal Emergency Management Agency (2015, 1).

<sup>222</sup> US Department of Homeland Security (2014b, iii).

<sup>223</sup> US Department of Homeland Security (2014b, 42).

<sup>224</sup> US Department of Homeland Security (2014b, ii).

<sup>225</sup> ENISA (2014c, 46).

<sup>226</sup> ENISA (2014c, 46).

<sup>227</sup> ENISA (2014c, 46).

<sup>228</sup> US Department of Homeland Security (2014b, iii).

<sup>229</sup> US Department of Homeland Security (2014b, iii).

<sup>230</sup> US Department of Homeland Security (2014b, iii).

<sup>231</sup> US Department of Homeland Security (2014b, 36).

<sup>232</sup> US Department of Homeland Security (2014b, 39).

<sup>233</sup> US Department of Homeland Security (2014b, 45).

<sup>234</sup> US Department of Homeland Security (2014b, 40).

<sup>235</sup> Gant (2008, 56).

<sup>236</sup> Gant (2008, 56).

<sup>237</sup> Gant (2008, 56).

<sup>238</sup> Gant (2008, 56).

<sup>239</sup> ICC (2015, 12).

<sup>240</sup> Financial Industry Regulatory Authority (2015, 31).

<sup>241</sup> ICC (2015).

<sup>242</sup> ICC (2015, 10).

<sup>243</sup> Financial Industry Regulatory Authority (2015, 7).

<sup>244</sup> G7 Cyber Expert Group (2016).

<sup>245</sup> ICC (2015, 19).

<sup>246</sup> ICC (2015, 10).

<sup>247</sup> ICC (2015, 10).

<sup>248</sup> ICC (2015, 10).

<sup>249</sup> Financial Industry Regulatory Authority (2015, 32).

<sup>250</sup> Financial Industry Regulatory Authority (2015, 31).

<sup>251</sup> ICC (2015, 16).

<sup>252</sup> UNCTAD (2015).

<sup>253</sup> Gant (2008, 15).

<sup>254</sup> Gant (2008, 15).

<sup>255</sup> This is sometimes presented as four sub-categories, whereby government-to-employee (G2E) is also included. However, both these refer to internal government processes, and so it can be grouped collectively under G2G. Source: Gant (2008, 15-8).

<sup>256</sup> Johnson (2008).

<sup>257</sup> Gant (2008, 15).

<sup>258</sup> UNCTAD (2015, 2-7).

<sup>259</sup> ITU (2014, 4).

<sup>260</sup> Berejka & Schwartz (2011).

<sup>261</sup> In this instance, authentic refers to services that are provided by government or recognised public or private organisations, as opposed to fake or malicious platforms.

<sup>262</sup> “Unfairly exploited” is a subjective term that refers to the manner in which internet users disclose personal or sensitive information, and the ways in which this information is then used by private or public sector actors. It is a complex discussion within the broader topic of *Internet Governance* that will not be presented here

<sup>263</sup> ITU (2014, 4).

<sup>264</sup> Gant (2008, 54).

<sup>265</sup> Gant (2008, 54-5).

<sup>266</sup> Gant (2008, 54-5).

<sup>267</sup> Gant (2008, 54).

<sup>268</sup> ITU (2014, 4-9).

<sup>269</sup> Gant (2008, 52).

<sup>270</sup> Gant (2008, 52).

<sup>271</sup> Gant (2008, 53).

<sup>272</sup> Gant (2008, 53).

<sup>273</sup> ITU (2014, 15).

<sup>274</sup> ITU (2014, 17).

<sup>275</sup> ITU (2014, 17).

<sup>276</sup> ITU (2014, 10).

<sup>277</sup> Gant (2008, 53-4).

<sup>278</sup> Gant (2008, 55).

<sup>279</sup> Gant (2008, 55).

<sup>280</sup> Gant (2008, 55).

<sup>281</sup> Gant (2008, 54).

<sup>282</sup> Gant (2008, 55).

<sup>283</sup> Gant (2008, 15).

<sup>284</sup> Friedland & Muylkens (2009, 6).

<sup>285</sup> Gant (2008, 56).

<sup>286</sup> World Bank (2016, 28).

<sup>287</sup> World Bank (2016, 194-7).

<sup>288</sup> Friedland & Muylkens (2009, 9).

<sup>289</sup> OECD (2017, 101-2).

<sup>290</sup> OECD (2017, 101-2).

<sup>291</sup> OECD (2017, 101-2).

<sup>292</sup> OECD (2017, 100-1).

<sup>293</sup> Friedland & Muylkens (2009, 53).

<sup>294</sup> Gant (2008, 53).

<sup>295</sup> UNCTAD (2015, 31-4).

<sup>296</sup> UNCTAD (2015, 34-9).

<sup>297</sup> UNCTAD (2015, 64).

<sup>298</sup> UNCTAD (2016, 6).

<sup>299</sup> UNCTAD (2016, 6).

<sup>300</sup> UNCTAD (2016, 6).

<sup>301</sup> UNCTAD (2015, 64).

<sup>302</sup> UNCTAD (2015, 64).

<sup>303</sup> UNCTAD (2015, 66-8).

<sup>304</sup> UNCTAD (2015, 68-9).

<sup>305</sup> UNCTAD (2015, 71).

<sup>306</sup> UNCTAD (2015, 72-3).

<sup>307</sup> UNCTAD (2015, 64).

<sup>308</sup> Berejka & Schwartz (2011, iv).

<sup>309</sup> OAS (2015b).

<sup>310</sup> Berejka & Schwartz (2011, 37).

<sup>311</sup> Berejka & Schwartz (2011, 37).

<sup>312</sup> Berejka & Schwartz (2011, 4).

<sup>313</sup> UK Government (2016b).

<sup>314</sup> Berejka & Schwartz (2011, 4).

<sup>315</sup> Berejka & Schwartz (2011, 67).

<sup>316</sup> OECD (2013, 4).

<sup>317</sup> OECD (2013).

<sup>318</sup> OECD (2013, 20).

<sup>319</sup> OECD (2013, 15).

<sup>320</sup> OECD (2013).

<sup>321</sup> OECD (2013).

<sup>322</sup> European Commission (N.d.).

<sup>323</sup> CBPRs (N.d.).

<sup>324</sup> OECD (2007); OECD (2013).

<sup>325</sup> OECD (2013).

<sup>326</sup> OECD (2013, 67).

<sup>327</sup> Correia & Compeau (2017).

<sup>328</sup> OECD (2013).

<sup>329</sup> OECD (2013).

<sup>330</sup> Stay Safe Online (2017). Stop Think Connect (2017).

<sup>331</sup> OECD (2013).

<sup>332</sup> US Department of Homeland Security (2017d).

<sup>333</sup> European Cyber Security Month (N.d.).

<sup>334</sup> Lyon (2014). UNCTAD (2016, 15)

<sup>335</sup> Fischer (2014, 1-2). Gasser et al. (2016).

<sup>336</sup> European Commission (2014, 50 ).

<sup>337</sup> EU Data Protection Regulation (2015).

<sup>338</sup> Microsoft (2013).

<sup>339</sup> Hodge (2012). European Parliament (2016b).

<sup>340</sup> European Parliament (2016a).

<sup>341</sup> Microsoft (2013).

<sup>342</sup> OECD (2013, 103).

<sup>343</sup> OECD (2013, 104).

<sup>344</sup> European Parliament (2016b).

<sup>345</sup> GLACY (2014).

<sup>346</sup> GLACY (2014, 9).

<sup>347</sup> GLACY (2014, 13).

<sup>348</sup> GLACY (2014, 13).

<sup>349</sup> GLACY (2014, 30).

<sup>350</sup> GLACY (2014, 6).

<sup>351</sup> GLACY (2014, 7-8).

<sup>352</sup> Europol (2016).

<sup>353</sup> ITU (2012, 82).

<sup>354</sup> ITU (2012, 82).

<sup>355</sup> ITU (2012, 82).

<sup>356</sup> GLACY (2014).

<sup>357</sup> GLACY (2014, 8-9).

<sup>358</sup> Ministère de l'Intérieur (N.d.).

<sup>359</sup> GLACY (2014, 9).

<sup>360</sup> Action Fraud (N.d.).

<sup>361</sup> FBI IC3 (N.d.).

<sup>362</sup> GLACY (2014, 12).

<sup>363</sup> APWG (2017).

<sup>364</sup> GLACY (2014, 30-1).

<sup>365</sup> GLACY (2014, 17).

<sup>366</sup> GLACY (2014, 14-5).

<sup>367</sup> GLACY (2014).

<sup>368</sup> GLACY (2014, 12,5,23).

<sup>369</sup> GLACY (2014, 17).

<sup>370</sup> Goolsby (2013).

<sup>371</sup> ITU (2014).

<sup>372</sup> Bertot et al (2012)

<sup>373</sup> Bertot et al (2012)

<sup>374</sup> UK Parliament (2014a).

<sup>375</sup> Bertot et al. (2012).

<sup>376</sup> Oxley (2011).

<sup>377</sup> Bertot, Jaeger et al. (2012).

<sup>378</sup> For more information, see: <https://twitter.com/cyber>

<sup>379</sup> NCSC (2017a).

<sup>380</sup> Norwegian Ministries (2012).

<sup>381</sup> BSA (2015); CyberSecurity Malaysia (2017).

<sup>382</sup> Stay Safe Online (2017); Stop Think Connect (2017).

<sup>383</sup> ENISA (2007).

<sup>384</sup> Bada et al. (2014).

<sup>385</sup> OAS (2015b, 19).

<sup>386</sup> OAS (2015b, 20).

<sup>387</sup> OAS (2015b, 22–6).

<sup>388</sup> OAS (2015b, 28,30).

<sup>389</sup> OAS (2015b, 12–5).

<sup>390</sup> OAS (2015a, 40–9).

<sup>391</sup> Insafe (N.d.).

<sup>392</sup> For more information, see: Cyber Security Challenge UK (2017).

<sup>393</sup> Bada, Sasse et al. (2014).

<sup>394</sup> AXELOS (N.d.); OAS (2015b, 45).

<sup>395</sup> OAS (2015b, 45,54).

<sup>396</sup> Wilson & Hash (2003, 38).

<sup>397</sup> ENISA (2007, 14).

<sup>398</sup> Bada, Sasse et al. (2014, 125).

<sup>399</sup> OAS (2015a).

<sup>400</sup> Malmedal & Røislien (2016).

<sup>401</sup> GCHQ (2016).

<sup>402</sup> IISP (2010).

<sup>403</sup> UK Cabinet Office (N.d.).

<sup>404</sup> UK Government (2017a).

<sup>405</sup> UK Government (2017b).

<sup>406</sup> GCHQ (N.d.).

<sup>407</sup> UK Government (2016d).

<sup>408</sup> UK Government (N.d.-d).

<sup>409</sup> IAPP (2017).

<sup>410</sup> The Guardian (2012).

<sup>411</sup> Lord (2017).

<sup>412</sup> Singapore Institute of Technology (2017).

<sup>413</sup> NCSC (2017a).

<sup>414</sup> Yampolskiy (2017).

<sup>415</sup> Raguseo (2017).

<sup>416</sup> Bennett (2017).

<sup>417</sup> Hall et al. (2017).

<sup>418</sup> Hall, Menkes et al. (2017).

<sup>419</sup> BLS (2015).

<sup>420</sup> GenCyber (N.d.-b).

<sup>421</sup> GenCyber (N.d.-a).

<sup>422</sup> ICMCP (2017).

<sup>423</sup> Pârvu & Voicu-Olteanu (2009, 90).

<sup>424</sup> Pârvu & Voicu-Olteanu (2009).

<sup>425</sup> Jagasia (2017).

<sup>426</sup> Carr (2016).

<sup>427</sup> Cătălui (2014).

<sup>428</sup> UK Government (2017b).

<sup>429</sup> ENISA (2014d, 22).

<sup>430</sup> ENISA (2014d, 10).

<sup>431</sup> ENISA (2014d, 15-20).

<sup>432</sup> ENISA (2014d, 11).

<sup>433</sup> GCSCC (2014).

<sup>434</sup> ENISA (2015b).

<sup>435</sup> See, for example, Lord (2017). and Ponemon Institute (2014).

<sup>436</sup> EPSRC (2017).

<sup>437</sup> GCHQ (N.d.).

<sup>438</sup> ENISA (2014d).

<sup>439</sup> ENISA (2014a).

<sup>440</sup> US Department of Homeland Security (2017c); Tirrell (2012).

<sup>441</sup> NIST (N.d.-d).

<sup>442</sup> NIST (N.d.-c).

<sup>443</sup> United States Department of Defense (2015, 18).

<sup>444</sup> Central District of California United States Attorney's Office (2017).

<sup>445</sup> Libicki et al. (2014).

<sup>446</sup> NIST (2017).

<sup>447</sup> NICE (2013).

<sup>448</sup> CyberSeek (N.d.).

<sup>449</sup> CyberSeek (N.d.).

<sup>450</sup> SANS (2017).

<sup>451</sup> EC-Council (2017b).

<sup>452</sup> NATO Cooperative Cyber Defence Centre of Excellence (N.d.).

<sup>453</sup> Fraunhofer Academy (N.d.).

<sup>454</sup> Fraunhofer Academy (2017).

<sup>455</sup> Fraunhofer Academy (2017).

<sup>456</sup> Bayuk et al. (2012, 174).

<sup>457</sup> UK Government (2014a).

<sup>458</sup> UK Government (2014a).

<sup>459</sup> Purser (2014).

<sup>460</sup> NCSC (2015).

<sup>461</sup> APMG International (2017).

<sup>462</sup> See, for example, NIST (2017).

<sup>463</sup> NICE (2017).

<sup>464</sup> See, for example, UK Government (2016c).

<sup>465</sup> NICCS (2017).

<sup>466</sup> NICCS (2017).

<sup>467</sup> ENISA (2014d, 12).

<sup>468</sup> ENISA (2014d, 12).

<sup>469</sup> ENISA (2015b, 21).

<sup>470</sup> ENISA (2014a).

<sup>471</sup> Bayuk, Healey et al. (2012, 174).

<sup>472</sup> Centres of Academic Excellence in Cybersecurity Community (2017).

<sup>473</sup> The White House (2016).

<sup>474</sup> Natural Resource Governance Institute (2015).

<sup>475</sup> Tikk-Ringas (2015).

<sup>476</sup> Tikk-Ringas (2015, 109-10).

<sup>477</sup> Tikk-Ringas (2015, 109-10).

<sup>478</sup> These are the conventional approaches, but other approaches have been proposed, as in Sales (2012).

<sup>479</sup> World Bank (2016, 132-40).

<sup>480</sup> ITU (2012).

<sup>481</sup> ITU (2012).

<sup>482</sup> Some sources differentiate between procedural law and legal responses to digital evidence, such as ITU (2011a), whereas other sources, such as ITU (2010b), do not take this approach.

<sup>483</sup> ITU (2011a).

<sup>484</sup> ITU (2010b, 104).

<sup>485</sup> World Bank (2016, 41).

<sup>486</sup> World Bank (2016).

<sup>487</sup> ITU (2010b, 22).

<sup>488</sup> World Bank (2016, 103).

<sup>489</sup> ITU (2011a, 151-2).

<sup>490</sup> ITU (2011a, 151).

<sup>491</sup> ITU (2011a, 151).

<sup>492</sup> World Bank (2016, 62).

<sup>493</sup> World Bank (2016, 141).

<sup>494</sup> ITU (2011a, 152).

<sup>495</sup> ITU (2011a, 181).

<sup>496</sup> World Bank (2016).

<sup>497</sup> ITU (2010b).

<sup>498</sup> World Bank (2016, 79).

<sup>499</sup> World Bank (2016, 87-8).

<sup>500</sup> World Bank (2016, 85-6).

<sup>501</sup> World Bank (2016, 102).

<sup>502</sup> World Bank (2016, 103).

<sup>503</sup> World Bank (2016, 106-7).

<sup>504</sup> World Bank (2016, 153-4,64).

<sup>505</sup> Klimberg (2012, 150).

<sup>506</sup> Klimberg (2012, 150-1).

<sup>507</sup> World Bank (2016, 155).

<sup>508</sup> Klimberg (2012, 151-5); ITU (2010b).

<sup>509</sup> ITU (2012, 82-3).

<sup>510</sup> World Bank (2016, 141).

<sup>511</sup> Klimberg (2012, 150).;

<sup>512</sup> World Bank (2016, 62).

<sup>513</sup> GCSCC (2014, 41-4).

<sup>514</sup> CPS (N.d.).

<sup>515</sup> UK Parliament (2014b).

<sup>516</sup> GCSCC (2014).

<sup>517</sup> Daly & Sarre (2017, 3).

<sup>518</sup> See Gordon & Ford (2006); ITU (2011b); World Bank (2016).

<sup>519</sup> World Bank (2016, 56).

<sup>520</sup> Gordon & Ford (2006, 2).

<sup>521</sup> ITU (2011a, 7).

<sup>522</sup> ITU (2011a, 31).

<sup>523</sup> World Bank (2016, 24,37).

<sup>524</sup> Deloitte (2015).

<sup>525</sup> ITU (2011a, 123-54).

<sup>526</sup> World Bank (2016, 38-9).

<sup>527</sup> UK Government (2010).

<sup>528</sup> UK Government (N.d.-b).

<sup>529</sup> UK Government (2016e).

<sup>530</sup> National Crime Agency (N.d.).

<sup>531</sup> CPS (N.d.); UK Ministry of Justice (2014).

<sup>532</sup> Home Office (2010).

<sup>533</sup> UK Government (2014b).

<sup>534</sup> UK Government (2016e).

<sup>535</sup> UK Ministry of Justice (2014).

<sup>536</sup> World Bank (2016, 190).

<sup>537</sup> UK Government (2016e, 48).

<sup>538</sup> World Bank (2016, 222-5).

<sup>539</sup> World Bank (2016, 78-100).

<sup>540</sup> UNODC (2013, 119).

<sup>541</sup> Prasanthi & Ishwarya (2015, 2).

<sup>542</sup> World Bank (2016, 145).

<sup>543</sup> World Bank (2016, 90).

<sup>544</sup> Forensic Science Simplified (N.d.).

<sup>545</sup> UK Parliament (2016).

<sup>546</sup> Kornblum (2002).

<sup>547</sup> Forensic Science Regulator (2015, 3).

<sup>548</sup> UK Parliament (2016, 2).

<sup>549</sup> Vandeven (2014).

<sup>550</sup> Craiger (2005).

<sup>551</sup> Prayudi & Sn (2015).

<sup>552</sup> World Bank (2016, 80).

<sup>553</sup> World Bank (2016, 79-80).

<sup>554</sup> World Bank (2016, 82).

<sup>555</sup> World Bank (2016, 85).

<sup>556</sup> UK Parliament (2016, 1).

<sup>557</sup> Vandeven (2014, 7).

<sup>558</sup> Prayudi et al. (2014, 31).

<sup>559</sup> Prayudi & Sn (2015).

<sup>560</sup> World Bank (2016, 94-5).

<sup>561</sup> World Bank (2016, 196).

<sup>562</sup> College of Policing (N.d.).

<sup>563</sup> NCSC (2017c).

<sup>564</sup> Europol (N.d.).

<sup>565</sup> Interpol (2017a).

<sup>566</sup> Interpol (2017b).

<sup>567</sup> World Bank (2016, 186).

<sup>568</sup> GCSCC (2014, 45-6).

<sup>569</sup> CPS (N.d.).

<sup>570</sup> GCSCC (2014, 45-6); World Bank (2016, 170).

<sup>571</sup> World Bank (2016, 42).

<sup>572</sup> World Bank (2016, 186).

<sup>573</sup> ITU (2011b, 38).

<sup>574</sup> ITU (2011b, 36-8).

<sup>575</sup> GCSCC (2014, 45).

<sup>576</sup> European Union & Council of Europe (2011, 5).

<sup>577</sup> World Bank (2016, 42).

<sup>578</sup> World Bank (2016, 42).

<sup>579</sup> Odinot et al. (2017, 18).

<sup>580</sup> See, for example, Queensland Government (2016).

<sup>581</sup> UK Parliament (2016, 49).

<sup>582</sup> Council of Europe (2017a).

<sup>583</sup> World Bank (2016).

<sup>584</sup> World Bank (2016).

<sup>585</sup> Council of Europe (2008).

<sup>586</sup> World Bank (2016).

<sup>587</sup> World Bank (2016).

<sup>588</sup> For more information, see: Europol (2017).

<sup>589</sup> For more information, see: Europol (2017). and Interpol (2017c).

<sup>590</sup> World Bank (2016).

<sup>591</sup> Staro (2010).

<sup>592</sup> Council of Europe (2017b); WEF (2017).

<sup>593</sup> NCSC (2017b).

<sup>594</sup> Microsoft Digital Crimes Unit (2015).

<sup>595</sup> ENISA (2016a).

<sup>596</sup> For more information, see: NIST (2016).

<sup>597</sup> ISO (2013a).

<sup>598</sup> ITU (2010a).

<sup>599</sup> ITU (2010c).

<sup>600</sup> ISO (2012).

<sup>601</sup> NIST (N.d.-b).

<sup>602</sup> ITU (2008).

<sup>603</sup> ISO (2011b).

<sup>604</sup> ISO (2011b).

<sup>605</sup> Ross (2012).

<sup>606</sup> NIST (2011b).

<sup>607</sup> See: ISO (N.d.-a).

<sup>608</sup> ISO (2017).

<sup>609</sup> ISO (2011a).

<sup>610</sup> Black et al. (2016).

<sup>611</sup> CERT (2017).

<sup>612</sup> CPNI (2017).

<sup>613</sup> For more information, see: ITU (2017c).

<sup>614</sup> For more information, see: IEEE Standards Association (2017).

<sup>615</sup> For more information, see: IETF (N.d.-a).

<sup>616</sup> For more information, see: IETF (N.d.-c).

<sup>617</sup> For more information, see: W3C (2017).

<sup>618</sup> For more information, see: IANA (N.d.).

<sup>619</sup> For more information, see: ICANN (2017).

<sup>620</sup> Nye (2014).

<sup>621</sup> For more information, see: ARIN (2017).

<sup>622</sup> For more information, see: UNODA (2017).

<sup>623</sup> US Department of Homeland Security (2013).

<sup>624</sup> US Department of Homeland Security (2013).

<sup>625</sup> ITU (2017a).

<sup>626</sup> UN Development Programme (N.d.).

<sup>627</sup> UN Development Programme (N.d.); World Bank (2017).

<sup>628</sup> World Bank (2014).

<sup>629</sup> Hall et al. (2013).

<sup>630</sup> Newman (2016).

<sup>631</sup> US Department of Homeland Security (N.d.).

<sup>632</sup> US Department of Homeland Security (2013).

<sup>633</sup> ITU (2015).

<sup>634</sup> NISCC (2006).

<sup>635</sup> e-Estonia (2017).

<sup>636</sup> ISO (2015).

<sup>637</sup> BBC (2014).

<sup>638</sup> DevOps is a clipped compound of "software DEVelopment" and "information technology OPerationS".

<sup>639</sup> ISO (2011a).

<sup>640</sup> Black, Badger et al. (2016).

<sup>641</sup> UK Government (2016a).

<sup>642</sup> UK Government (2016a).

<sup>643</sup> Pressman (2009).

<sup>644</sup> Voldal (2003).

<sup>645</sup> Microsoft (2017).

<sup>646</sup> Voldal (2003).

<sup>647</sup> Symantec (2010).

<sup>648</sup> CERT (2017).

<sup>649</sup> Whitney (2011).

<sup>650</sup> Acar et al. (2017).

<sup>651</sup> Northcutt (2009).

<sup>652</sup> Sedgewick et al. (2017).

<sup>653</sup> Australian Department of Defence (2013).

<sup>654</sup> Van Eeten et al. (2010).

<sup>655</sup> ISO (N.d.-b).

<sup>656</sup> ITU (2017b).

<sup>657</sup> IEEE Standards Association (2016).

<sup>658</sup> Stoneburner (2001).

<sup>659</sup> ENISA (2014e).

<sup>660</sup> NIST (2008).

<sup>661</sup> Symantec (2017).

<sup>662</sup> IETF (N.d.-d).

<sup>663</sup> Souppaya & Scarfone (2013).

<sup>664</sup> ENISA (2013b).

<sup>665</sup> ENISA (2014e).

<sup>666</sup> WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy) are used for authentication of network devices and the protocol was developed by the Wi-Fi Alliance to secure wireless computer networks

<sup>667</sup> EMV is a technical standard for ‘chip and pin’ cards used at payment terminals and automated teller machines.

<sup>668</sup> ENISA (2014a).

<sup>669</sup> Regenscheid (2016).

<sup>670</sup> Hypertext Transfer Protocol (HTTP) is the commonly used protocol to transport webpages from servers to clients.

<sup>671</sup> EFF (N.d.-c).

<sup>672</sup> EFF (N.d.-b).

<sup>673</sup> EFF (N.d.-a).

<sup>674</sup> Let's Encrypt (N.d.).

<sup>675</sup> IEC (2017).

<sup>676</sup> IEEE Xplore (2017).

<sup>677</sup> IETF (N.d.-b).

<sup>678</sup> NIST (N.d.-a).

<sup>679</sup> IETF (2017).

<sup>680</sup> ENISA (2014e, iv).

<sup>681</sup> ENISA (2014e).

<sup>682</sup> US Department of Homeland Security (2017b).

<sup>683</sup> KPMG (2016).

<sup>684</sup> Friedman & Thomas (2017).

<sup>685</sup> Merry et al. (2017).

<sup>686</sup> Friedman & Thomas (2017).

<sup>687</sup> ACORN (N.d.).

<sup>688</sup> Friedman & Thomas (2017).

<sup>689</sup> Constantin (2014).

<sup>690</sup> KPMG (2016).

<sup>691</sup> Merry, Smith et al. (2017).

<sup>692</sup> US Department of Homeland Security (2017b).

<sup>693</sup> UK Government (2015a).

<sup>694</sup> Friedman & Thomas (2017).

<sup>695</sup> Nakashima & Gillum (2017).

<sup>696</sup> ITU (2017d).

<sup>697</sup> ENISA (2016c).

<sup>698</sup> ISO (2014).

<sup>699</sup> ISO (2013b).

<sup>700</sup> ENISA (2016c).

<sup>701</sup> ISO (N.d.-a).

<sup>702</sup> ENISA (2016c).

<sup>703</sup> EPIC (2017).

<sup>704</sup> ENISA (2016c).