

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

International Security Management Knowledge Alliance (ISM-KA)

Addressing Security Challenges in an Interconnected World



Work Package 2

Developing Guidelines for Education in International Security Management

Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	Guidelines for Education in International Security Management
Relevant Work package:	WP 2 Developing Guidelines for Education in International Security Management
Dissemination Level:	PU
Document version:	V1.0 V2.0 V3.0
Date:	30 September 2017 25 January 2018 1 November 2018
Authors:	Alison Lyle
Document description:	Describes process developed and applied to initial work, provides rationale for this and gives indication of first outputs, as well as relationship with other work packages. With annexes containing the work completed by 1 November 2018

Document Updates			
Date	Version	Sections amended / updated	Name / Organisation
30.09.2017	V1.0	Whole document first draft	Alison Lyle (CENTRIC)
25.01.2018	V2.0	Addition of work completed on modules by 15 January 2018.	Alison Lyle (CENTRIC)
01.11.2018	V3.0	Small final edits	Alison Lyle (CENTRIC)

Table of Contents

1. INTRODUCTION	11
2. PURPOSE AND SCOPE.....	11
3. STRUCTURE AND CONTENT	12
4. OVERVIEW OF WORK PACKAGE 2.....	12
5. IDENTIFICATION OF MODULE TOPICS.....	14
6. ALLOCATION OF TOPICS TO PARTNERS	15
7. METHODOLOGY	16
8. HORIZON SCANNING.....	17
9. DESK BASED RESEARCH.....	20
10. IDENTIFICATION OF THEMES AND ISSUES.....	21
11. LEARNING OUTCOMES AND INDICATIVE CONTENT	22
12. EXPERT VALIDATION.....	23
13. CONCLUSION	25
CHANGE MANAGEMENT	26
1 MODULE DESCRIPTOR.....	28
2 DESK BASED RESEARCH COMPONENT	29
3 MASTER PROGRAMMES	30
3.1 Current courses Change management	30
3.2 Professional courses (as current courses).....	30
3.3 Main topics outlined (Master programmes and Professional courses):	30
3.4 SUMMARY – Current courses	31
4 STAKEHOLDERS PERSPECTIVE	32
4.1 Enhancing awareness on Change management.....	33
4.2 How to lead successful change.....	33
4.3 Understanding the context of change	33
4.4 Applying new knowledge to organisational change	34
4.5 SUMMARY - Stakeholders’ perspective.....	34
5 BACKGROUND.....	34
5.1 Current research	34
5.2 Statistics	35
5.3 Reports	35
5.4 SUMMARY - Background	36
6 CURRENT POLICIES	37

6.1	Current policies	37
6.2	SUMMARY – Current policies.....	38
7	CURRENT PRACTICE.....	38
7.1	Current practices	38
7.2	SUMMARY – Current practice	39
8	‘THOR’ SUMMARY	40
	CO-CREATION & CROWDSOURCING.....	41
1.	MODULE DESCRIPTOR.....	43
2.	DESK BASED RESEARCH COMPONENT	43
3.	MASTER PROGRAMMES	44
3.1.	Specific courses (as current courses)	44
3.2.	Main topics outlined (Master programmes and Professional courses):	44
3.3.	SUMMARY – Current courses	45
4.	STAKEHOLDERS PERSPECTIVE	46
4.1.	Enhancing awareness on Co-Creation and Crowdsourcing	47
4.2.	Context of Co-Creation and the Changing Role of Leadership for Security Professionals	47
4.3.	Applying new knowledge to Co-Creation and Crowdsourcing	47
4.4.	SUMMARY - Stakeholders’ perspective.....	48
5.	BACKGROUND.....	48
5.1.	Current research	48
5.2.	Reports	48
5.3.	SUMMARY - Background	49
6.	‘THOR’ SUMMARY	49
	INTERNATIONAL SECURITY COOPERATION	50
1.	MODULE DESCRIPTOR.....	51
2.	CURRENT COURSES.....	52
2.1.	Masters Courses	52
2.2.	Professional courses (as current courses).....	52
2.3.	Main topics outlined (Master programmes and Professional courses):	52
2.4.	SUMMARY – Current courses	53
3.	STAKEHOLDERS PERSPECTIVE	54
3.1.	Enhancing awareness on Security policies.....	54
3.2.	Cooperation and information exchange	54
3.3.	International legislative system	55
3.4.	Awareness, education and training.....	55
3.5.	Technological evolution.....	56
3.6.	SUMMARY - Stakeholders’ perspective.....	56
4.	BACKGROUND.....	57
4.1.	Current Research	57
4.2.	Reports	57

4.3. SUMMARY - Background	58
5. CURRENT POLICIES	59
5.1. Government & Institutions	59
5.2. Industry	59
5.3. Law Enforcement	60
5.4. SUMMARY – Current policies	60
6. CURRENT PRACTICE.....	62
6.1. Europe	62
6.2. International	62
6.3. National	62
6.4. SUMMARY – Current practice	63
7. ‘THOR’ SUMMARY	64
PUBLIC SAFETY	67
1. MODULE DESCRIPTOR.....	69
2. MASTER PROGRAMMES	70
2.1. Current courses.....	70
2.2. Main topics outlined (Master programmes and Professional courses):	72
2.3. SUMMARY – Current courses	72
3. STAKEHOLDERS PERSPECTIVE	73
3.1. Stakeholder perspective general	73
3.2. Public safety and the field of security	74
3.3. Antisocial behaviour	75
3.4. Violence	75
3.5. Property crime	75
3.6. Trafficking.....	76
3.7. Large scale public events	78
3.8. Natural and technological hazard	78
3.9. Traffic and road security	78
4. STAKEHOLDERS PERSPECTIVE	78
4.1. SUMMARY - Stakeholders’ perspective.....	81
5. BACKGROUND.....	82
5.1. History	82
5.2. Policing models	83
5.3. Organizational models.....	83
6. BACKGROUND.....	84
6.1. Current research	84
6.2. Statistics	84
6.3. Reports	85
6.4. SUMMARY - Background	86
7. CURRENT POLICIES	87
7.1. Security sector	87
7.2. National policies.....	87

7.3.	International policies	88
7.4.	Public safety policies.....	89
7.5.	International policies	90
7.6.	Private security	90
7.7.	SUMMARY - Policies	91
8.	CURRENT PRACTICE.....	91
8.1.	Prevention and response to call	91
8.2.	Police services	92
8.3.	Neighbourhood, local communities, citizen commitment	92
8.4.	Private security	93
8.5.	Public private partnerships	93
8.6.	Surveillance and predictive policing	93
9.	CURRENT PRACTICES	93
9.1.	SUMMARY – Current practice	97
10.	LEGAL FACTORS	98
10.1.	Human rights and privacy	98
10.2.	Commercial and penal fraud	98
10.3.	Criminalisation, prosecution and trial	98
10.4.	SUMMARY - Legal factors	99
11.	‘THOR’ SUMMARY	100
	REFERENCE LIST	102
	ORGANISED CRIME.....	103
1.	MODULE DESCRIPTOR.....	105
2.	MASTER PROGRAMMES	106
2.1.	Current courses.....	106
2.2.	SUMMARY – Current courses	108
3.	STAKEHOLDERS PERSPECTIVES.....	108
3.1.	Stakeholder perspective general	108
3.2.	Corruption and hostile take over	109
3.3.	Trafficking illicit goods and services	109
3.4.	Illicit trade of licit goods/illicit trade.....	110
3.5.	Frauds and money laundering	111
3.6.	Embedded and concealed operations	112
3.7.	Business responsibility, due diligences and compliance.....	112
3.8.	Violence and Racketeering.....	113
3.9.	Desk based research stakeholders perspective	113
3.10.	SUMMARY - Stakeholders’ perspective.....	114
4.	BACKGROUND.....	115
4.1.	Traditional mafias	115
4.2.	Drugs and major trafficking	116
4.3.	International organised crime.....	116
5.	BACKGROUND.....	117

5.1.	Current research	117
5.2.	Statistics general view	117
5.3.	Statistics sources	118
5.4.	SUMMARY - Background	118
6.	CURRENT POLICIES AND LEGAL FACTORS.....	119
6.1.	Organised crime	119
6.2.	Drugs, Human trafficking, Money Laundering.....	119
6.3.	Illicit trade	120
6.4.	International police and judiciary cooperation.....	120
6.5.	Criminal asset seizure.....	121
6.6.	Sources	121
6.7.	SUMMARY - Policies and regulation	122
7.	CURRENT PRACTICES	122
7.1.	Undercover operations and controlled deliveries.....	122
7.2.	Surveillance and tracking	123
7.3.	Private public cooperation.....	123
7.4.	Criminal analysis.....	123
7.5.	Plea bargaining and cooperative witnesses	124
7.6.	Sources	124
7.7.	SUMMARY – Current practice	125
8.	THOR’ SUMMARY	125
	REFERENCE LIST	127
	CYBERCRIME.....	128
1.	MODULE DESCRIPTOR.....	130
2.	CURRENT COURSES.....	131
2.1.	Masters Courses	131
2.2.	Professional Training	133
2.3.	CPD Courses	134
3.	STAKEHOLDER PERSPECTIVES	134
3.1.	Institutional Bodies	134
3.2.	Law Enforcement	135
3.3.	Businesses And NGOs	136
4.	BACKGROUND.....	136
4.1.	Current Research	136
4.2.	Statistics	137
4.3.	Reports	138
5.	CURRENT POLICIES	139
5.1.	Governments & Institutions	139
5.2.	Industry.....	140
5.3.	Law Enforcement	140
6.	CURRENT PRACTICE.....	141
6.1.	EU.....	141

6.2.	International	141
6.3.	National	142
7.	LEGAL FACTORS	142
7.1.	National	142
7.2.	European.....	142
7.3.	International	144
8.	CURRENT COURSES.....	144
8.1.	Master Programmes.....	144
8.2.	Professional Development Courses.....	145
8.3.	Continuing Professional Development Courses.....	148
8.4.	Summary - Current Courses	149
9.	STAKEHOLDER PERSPECTIVES	150
9.1.	Enhancing capability of investigators	150
9.2.	Erasmus+ Advisory Board	153
9.3.	Summary – Stakeholder Perspectives	155
10.	BACKGROUND.....	157
10.1.	Current Research	157
10.2.	Statistics	158
10.3.	Reports	159
10.4.	Key legislation on cyber security and data flows in 2016:	161
10.5.	Summary – Background.....	162
11.	CURRENT POLICIES	164
11.1.	European Institutions.....	164
11.2.	Industry.....	167
11.3.	Law Enforcement	168
11.4.	Summary – Current Policies	169
12.	CURRENT PRACTICE.....	171
12.1.	Europe	171
12.2.	International	172
12.3.	National	177
12.4.	Summary – Current Practice	184
13.	LEGAL FACTORS	186
13.1.	European.....	186
13.2.	International	188
14.	OVERALL SUMMARY	189
14.1.	‘THOR’ Summary.....	189
COUNTER TERRORISM		191
1. MODULE DESCRIPTOR.....		193
HORIZON SCANNING		194
2. CURRENT COURSES		194
2.2	Current Courses.....	194

2.2	CPD Courses	194
3.	STAKEHOLDER PERSPECTIVES	195
3.1.	Institutional Bodies	195
3.2.	Law Enforcement	195
3.3.	Businesses and NGO's	195
4.	CURRENT RESEARCH	195
4.1.	Statistics	195
4.2.	Reports	196
5.	CURRENT POLICIES	196
5.1.	Government & Institutions	196
5.2.	Industry.....	196
5.3.	Law Enforcement	197
6.	CURRENT PRACTICE.....	197
6.1.	European.....	197
6.2.	International	197
6.3.	National	197
7.	LEGAL FACTORS	198
7.1.	National	198
7.2.	European.....	198
7.3.	International	198
8.	CURRENT COURSES.....	199
8.1.	Master Programmes.....	199
8.2.	Professional Development Courses.....	199
8.3.	THOR Summary - Current Courses	200
9.	STAKEHOLDER PERSPECTIVES	201
9.1.	Counter Terrorism Strategy.....	201
9.2.	Radicalisation	201
9.3.	Online Terrorist Propaganda	202
9.4.	Finance	202
9.5.	Terrorism is a key business risk	203
9.6.	Human Rights.....	203
9.7.	State terrorism	203
9.8.	THOR Summary - Stakeholder Perspectives	204
10.	BACKGROUND.....	205
10.1.	Current Research	205
10.2.	Reports	206
10.3.	THOR Summary - Background.....	208
11.	CURRENT POLICIES	210
11.1.	Government and Institutions	210
11.2.	Law Enforcement	212
11.3.	THOR Summary - Current Policies	213
12.	CURRENT PRACTICE.....	213

12.1. National	213
12.2. European Union.....	214
12.3. International	215
12.4. THOR Summary - Current Practice	215
13. LEGAL FACTORS	216
13.1. National	216
13.2. European.....	216
13.3. International	217
13.4. THOR Summary - Legal Factors	218
OVERALL SUMMARY	218
14. THOR - OVERALL SUMMARY	218

1. Introduction

Work Package 2 develops the guidelines for education in the field of international security management; this document is the report on the first educational guidelines produced. There are three specified outputs within the Work Package:

T2.1 – Defining education needs in international security management;

T2.2 – Developing educational guidelines based on current EU policies and the state of the art in related fields;

T2.3 – Examining international frameworks for extending the educational reach of the ISM-KA.

These focus points are represented in the activities carried out thus far and continuing contributions will extend these aims so they are realised as the work progresses.

Although the stages of work described here provide the main input to enable work package 3 to proceed, the activities will continue throughout the duration of the project representing the ongoing alignment with purposes, principles and high quality.

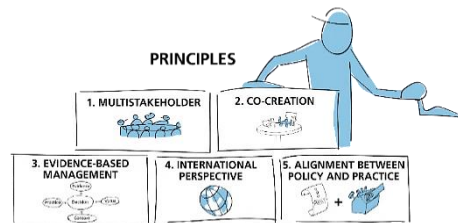


Figure 1: ISM-KA Project Principles

2. Purpose and scope

This document describes the process that has been established and followed in order to fulfil the initial obligations of Work Package 2. The ways in which this reflects the overall aims and objectives of the project is clarified, as well as the way that this work package continues at the core of ongoing development of the project outputs. The interaction between Work Package 2 and others that have a direct relationship with it is also explained, so that the context and impact of the work can be understood.

At the time of writing, Work Package 2 activities are ongoing, as they will throughout the project; these will be described at the appropriate intervals. As many of the outcomes as possible will be referred to. This document will be updated at each point (to be determined) that output is produced and fed into ongoing development work. The version control table at the front of the document will records all changes and additions.

3. Structure and content

The structure of this document reflects the stages of the process adopted. An overview of the Work Package, the aims, objectives and focus points are outlined. The relationship between the Work Packages is also provided to create context and facilitate understanding. The process that was developed and applied for the work is described and is followed by further explanation and examples for each of the stages.

Flow charts, diagrams and examples are used throughout the document to provide clarity and insight; this is aimed at creating context and understanding of the ways in which the work contributes to the overall project. The full results of the work are not presented, but excerpts are included as a representation. At the time of writing, the full methodology reports and some results are awaited; however, these will be included as an annex at a later date.

4. Overview of Work Package 2

In recognition of the fact that security challenges encompass the whole range of societal domains, Work Package 2 aims to capture information from a variety of sources, across all sectors, in order to account for as many perspectives as possible and assess and analyse these, in order to present the most pertinent issues that are most relevant for inclusion in the international security management learning modules.

The construction and method applied to Work Package 2 closely aligns with the principles that underpin the entire project as well as the 5 strategic requirements in respect of improvements in European safety and security management:

- 1) Increased multi-stakeholder collaboration
- 2) Increased co-creation
- 3) Shift to evidence based management
- 4) Better alignment between policy and practice
- 5) International perspective

Within the Work Package, distinct stages were identified; the whole process was a progressive one, which provided a logical working pattern and achieved transparency in methods and approach. This approach also facilitated a uniformed and manageable output from the various partners involved, otherwise this may have been challenging to achieve due to the volume of material, across such a range of topics. The overall process is described in Figure 2:

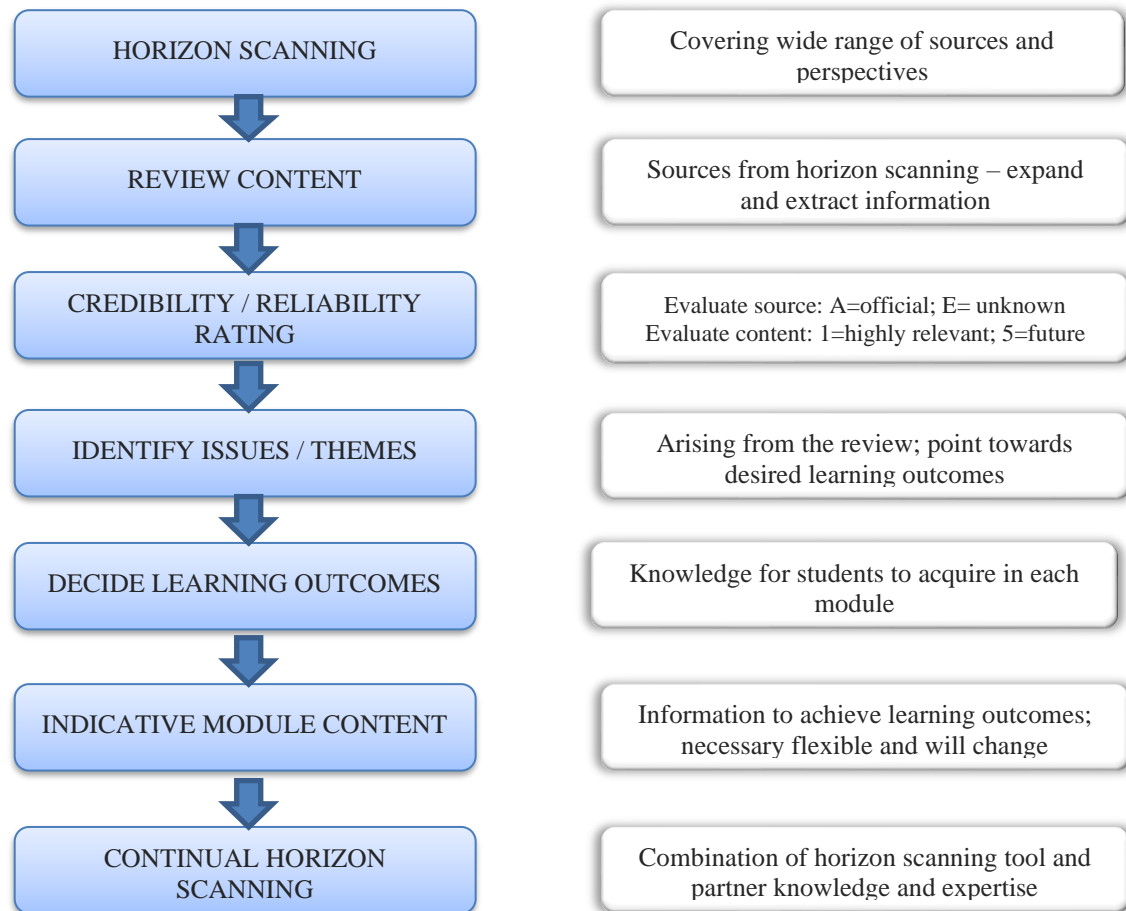


Figure 2: Stages of Work Package 2

The relationship and dependencies between the first three work packages are illustrated in Figure 3, below. The basic inputs are indicated, along with the flow. This shows the way in which both Work Package 1 and Work Package 2 will continue after initial delivery points; this is an essential feature of the organisation of the work to ensure that relevant, up to date and accurate information is continually fed into the development of the master's.

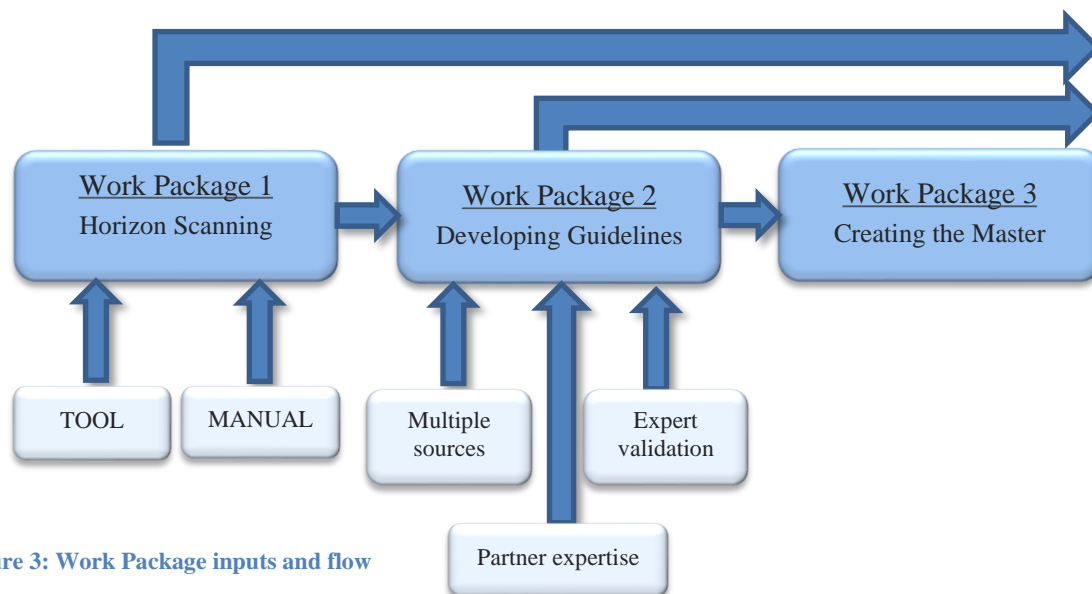


Figure 3: Work Package inputs and flow

It can be seen that the horizon scanning inputs for Work Package 1, which then provide Work Package 2 with information to review and analyse, consist of the horizon scanning tool as well as manual activities. Due to unforeseen circumstances within Work Package 1, the initial horizon scanning consisted solely of manual activity by the partners developing the guidelines and was thus incorporated into Work Package 2 activity to enable the development work to progress.

5. Identification of module topics

The number of modules reflects the usual requirements of master's courses; eight modules have been identified initially. These were decided upon early in the project, at an event where all of the partners were represented in a physical meeting. Extensive discussions took place and the topics were chosen as representing the key areas to be addressed in relation to international security management. The discussions incorporated the output of the first Advisory Board (AB) meeting that all had attended the previous day, thus incorporating both partner experience and AB input. It was also emphasised that additional topics could be developed at a later stage in order to offer students the opportunity to specialise in certain areas of relevant expertise. The modules are as follows:

- **Co-creative and crowdsourcing**
- **Counter terrorism**
- **Change management**
- **Cybercrime**
- **Serious and organised crime**
- **Public safety management**
- **International security collaboration**
- **EU policies, laws and regulations**

6. Allocation of topics to partners

CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), with its track record in developing innovative solutions for public safety and security and expertise in many aspects of the security domain, specifically cybercrime and terrorism studies, were ideally placed to develop the **Cybercrime** and **Counter Terrorism** learning guidelines. As one of the academic partners in the project, CENTRIC also lead Work Package 2.

RSM is a high-ranking business school, developing business leaders with international careers. With their innovative approach and extensive experience in developing and delivering leadership education, RSM have the necessary expertise to contribute to the development of the **Co-creative and crowdsourcing** and **Public Safety Management** modules and to fully develop the **Change Management** module.

As top-level experts in co-creation methodologies, primarily within the safety and security domains, Initiatives offered to contribute to the **Co-creation** module. Their experience in partnering thought leaders from across the world was valuable input for this work.

FORMIT took on the task of developing the **International Security Collaboration** module. They have decades of experience forging synergistic relationships with and between those producing research and those benefitting from it. As consultants with specific focus on security and technologies, their extensive international collaboration experience, as well as direct involvement with the University for International Studies in Rome, meant that FORMIT could ensure this module incorporated the most up to date and relevant information.

The educational guidelines for the **Serious and Organised Crime** module were developed by Lapprand Conseil International; a consultancy derived from extensive knowledge and experience in security and policing. Providing training, advice and solutions to an array of top-level, international organisations, LCI has the expertise and knowledge to develop this module and to contribute to the **Public Safety Management** module.

A decision was made to incorporate the **EU Policies, laws and regulations** development as part of the other modules, each one identifying the laws most relevant and pertinent within each field according to the knowledge of the relevant experts. A final overview will be provided by CENTRIC.

7. Methodology

In order to provide structure and uniformity to the initial phases of work within Work Package 2, a specific process was developed. This incorporated fundamental aims and objectives, not only of the Work Package, but of the project as a whole. The process also facilitated a methodical approach and provided a means of organising a large amount of information in a useful and meaningful way. Diagrams, explanations and examples were provided to those engaging in the activities so that understanding and consistency could be achieved.

In recognition of the fact that security challenges encompass the whole range of societal domains, Work Package 2 aimed to capture information from a variety of sources, across all sectors, in order to account for as many perspectives as possible and assess and analyse these in order to present the most pertinent issues that would influence the learning outcomes defined for each module.

The method used to discover, retrieve and review the material by partners developing the guidelines was established and applied in order to ensure credibility and integrity of the output. The emphasis could be said to be on three points:

- 1) Credibility and accuracy of the material collected and analysed.
- 2) Clear methodology to achieve consistency and to illustrate a rigorous process that reflects the aims, objectives and principles of the project as a whole.
- 3) Useful information, in an accessible and easily understandable format, to inject into Work Package 3.

The partners consulted a wide range of sources, predominantly material published on the internet and from open sources. The selection of sources within the process framework was subjective, based on individuals' knowledge of each topic area. This subjective assessment was also utilised when allocating weighting indicators to the sources and later to the information. As part of the initial analysis, both the source and the information was allocated an indication of credibility / validity and value. This was to allow the correct degree of reliance to be placed on the information in subsequent analyses and eventual use. The indicators below are derived from an established method used to assess police intelligence; it is simple to use and provides an immediate indication of the quality of both the source and the content. It was important that the experts made this subjective assessment, to ensure accuracy.

Source Evaluation

A	B	C	D	E
Primary / Official	Reliable secondary source	Expert but not peer-reviewed	Opinion	Not know / not measurable

Information Evaluation

1	2	3	4
Highly relevant; must be included	Very relevant	Of interest	Indication of future issues to be considered

A desk-based analysis of the sources from the first horizon scanning phase then took place. This involved the partners carrying out a detailed review of the material within the sources. While a specific method was not prescribed by the Work Package leads, it was emphasised that the resulting summaries, recommendations and guidelines should align with the overarching objectives of T2.1, T2.2 and T2.3, identifying common themes, issues and across existing approaches in order to inform the development of course content for the international security master's programme.

To provide structure and to assist with analysis, the process involved attributing the outcome of the analysis to specific headings. This was also a useful structure within which to present summaries of findings in the form of key issues and focal points. The structure was made up of four headings and are referred to as THOR summaries:

Technical – related to technology, technological approaches and solutions;

Human – human factors, behavioural and societal aspects;

Organisational – related to processes, procedures and policies within organisations, as well as cooperation (public-private / public-public) between organisations;

Regulatory – related to law, regulation, standardisation, accreditation.

These themes, issues and existing approaches were then interpreted by partners developing the various module guidelines and were used to influence and steer the last stage of the process, which was to identify learning outcomes for the modules and a description of the indicative content. In the name of consistency and ease of data management, partners were required to fill out a template table for this purpose.

Each of the stages of the methodology are described and illustrated below, using a selection of the outputs from partners.

8. Horizon scanning

As alluded to above, unforeseen circumstances within Work Package 1 resulted in manual horizon scanning activities being carried out in the first instance, within Work Package 2. Due to being carried out by the various consortium partners developing the guidelines, this horizon scanning was a manual, subjective search that was guided by the process followed by all. The process was developed to establish the required evidence base for each module and to establish a uniform and manageable approach. At the core of the horizon scanning task is the

identification of appropriate sources which will form the basis of the analysis defined within the Work Package 2 tasks.

The topics addressed by the modules represent the recognition that security management must address all sectors and domains and the horizon scanning was based on a typology that represented a wide range of sources and perspectives, in order to incorporate a holistic view of security issues. The areas and suggested content that were provided as a guide to those carrying out the horizon scanning are as follows:

- **Current Courses** - relevant subjects only
 - Including existing masters courses (content, structure, accreditation)
 - Practitioner CPD courses (requirements, standards and content)
 - Professional training (current practices and requirements)
- **Stakeholder perspectives**
 - Government / Institutional bodies (EU/UN)
 - Private industry
 - Law enforcement
- **Background**
 - Current research (concerns, issues, requirements, including reviews of academic literature)
 - Statistics (understand trends / growth areas)
 - Reports (e.g. Europol, Interpol etc. future / predictions)
- **Current policies**
 - Approaches, aims and priorities (UN, EU, national, international)
- **Current practices**
 - EU
 - National
 - Interpol, UN, international
- **Legal factors and implications**
 - EU
 - National
 - International

The aim was to gather as many relevant sources under each heading, and to add or omit headings, if this was appropriate, for particular module areas. At this stage, just the title or short description was recorded for each source, to serve as a list of references that would be reviewed and analysed during the following phase of desk-based research. This task was successfully carried out by partners; an excerpt of the cybercrime horizon scanning task is shown below. The bracketed references represent the weighting process that was applied at this stage.

The horizon scanning for each of the modules completed by January 2018 can be seen at Annex I.

Background

1.1.1 Current Research

- NATO Cooperative Cyber Defence Centre of Excellence - new study published April 2017 reveals vulnerabilities in the Most Widespread Network Security Solutions (A1)
<https://ccdcoe.org/new-study-reveals-vulnerabilities-most-widespread-network-security-solutions.html>
- CCDOE (2017) Hedgehog in the Fog: Creating and Detecting IPv6 Transition Mechanism-Based Information Exfiltration Covert Channels (A3)
<https://ccdcoe.org/multimedia/hedgehog-fog-creating-and-detecting-ipv6-transition-mechanism-based-information.html>
- Call for papers for 2017 International conference on cyber Conflict U.S. (CyCon U.S.) - deadline 10 July 2017. Conference on 7-8 November in Washington DC (B3)
<http://aci.cvent.com>
- 9th International CyCon (Tallinn 30 May - 2 June 2017) - international cooperation and conflict in cyberspace, technical challenges and requirements, legal frameworks, regulations and standards etc. General topic *Defending the Core* (B2)
www.cycon.org
- Cyber Power Conference 2016 materials, focusing on theme of *Cyber Power*, now available as part of IEEE publication (B2)
www.cycon.org
- Clark, R & Hakim, S. (eds) (2017) 'Cyber-Physical Security: protecting infrastructure at the State and local level' Switzerland: Springer International Publishing. (US perspective) (B2)
<http://www.fox.temple.edu/cms/wp-content/uploads/2016/08/Cyber-Physical-Security-PDF.pdf#page=197>
- RLD Pool & BHM Custers (2017) 'The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime' *European Journal of Crime, Criminal Law and Criminal Justice* Vol. 25, Issue 2, pp 123 - 144 (B2)
<http://booksandjournals.brillonline.com/content/journals/10.1163/15718174-25022109>
- Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D & Apostolopoulos, T. 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of the Tallinn Manual' *Computers & Security* 12 April 2017 (B2)
<http://www.sciencedirect.com/science/article/pii/S0167404817300822>

Figure 4: Excerpt from cybercrime horizon scanning exercise

9. Desk based research

During this stage of the process, the expertise, knowledge and experience of the partners was particularly depended upon. Although parameters had been set by the horizon scanning stage, there was nevertheless a vast amount of material and information to review and analyse. Main points, key issues and pertinent facts were extracted by the partners and emerging trends and themes were identified. Descriptions of the relevant information were recorded and presented, to reveal continuity and integrity. The below is an excerpt from the International Security Collaboration guideline development:

Law Enforcement

- Europol Strategy aim at reinforcing Europol as a trusted partner of law enforcement authorities, strengthening criminal information sharing and cooperation as the European criminal information hub and realising its role as a principal provider of operational support and expertise to Member States (MS) investigations. The new strategy laid EUROPOL to one based on full-scale delivery of operational service and impact, focusing its effort on consolidating all its capabilities and expertise to deliver the most effective support to MS investigations.
- The inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area represents a fundamental point to the EU Directorate General for Internal Policies. Complementarity, consistency and a good articulation between the different EU agencies and bodies (i.e. Europol, Eurojust, the European Judicial Network, the European Anti-Fraud Office and the future European Public Prosecutor's Office) are crucial to establish an area of Freedom, Security and Justice (AFSJ) that has a multidisciplinary approach to crime. Main recommendations include not only proposals to improve bilateral relations, but also proposals of a cross-cutting nature, addressing political and operational concerns.
- Transnational crime can only be countered by cross-border cooperation, with police, customs, border guards and other authorities working together. There has already been considerable progress in implementing training on cross-border matters in the EU. For instance, more than 300 exchange programmes between law enforcement officers across the EU were organized, while new learning methods, such as CEPOL's "webinars" were used by more than 3000 participants in 2012. Participation in EU training is growing, with more than 5000 enrolled at CEPOL and 3000 at Frontex last year. According to that, the European Commission' Communication proposes a European Law Enforcement Training Scheme to equip law enforcement officers with the knowledge and skills they need to prevent and combat cross-border crime effectively through efficient cooperation with their EU colleagues. (Communication from the Commission to the European Parliament, the

Figure 5: Excerpt from International Security Collaboration Guidelines

10. Identification of themes and issues

The use of THOR summaries within the Work Package 2 process provides a uniform presentation of main findings and contributes an additional method of categorisation that, it is anticipated, will be useful as Work Package 3 proceeds in constructing the master.

The headings used within the horizon scanning were continued throughout the process and partners created THOR summaries for each one. The below table is an excerpt from the cybercrime module development process document.

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<p>Implementation of tools to foster information sharing is considered relevant; Development of technological means to enhance communication between relevant actors/institutions involved to deal with the same issues.</p> <p>Technological evolution involves both risks and benefits; Security considerations on transmission of information are necessary.</p>
HUMAN	<p>Humans represent a key factor to enhance cooperation among agencies; Cooperation and information exchange requires trust to be established between institutions and people; The roles and responsibilities of individuals needs to be ascertained as well as improved governance of practices is required; both the nature and behaviour of delegates and responders must be accounted for.</p> <p>Awareness raising and education represents one of the most important pillar to support the process. All stakeholders should be aware of benefits from cooperation aiming at increasing resilience at all levels.</p>
ORGANISATIONAL	<p>Enhance communication procedures and information sharing through a more structured reporting mechanisms, including a clear and harmonised classification of concepts and assessment and evolution of policies.</p> <p>Avoid that cultures within organisations would form barriers to effective cooperation. Roles of main international actors need to be assessed to provide all the agencies with a clear framework. The organized cooperation between international institutions is a significant factor to be assessed. Organisations need to review their networks and data streams and develop strategies for their analysis and protection. Organisations bear a responsibility to train and raise awareness among employees and to set and maintain standards so that a culture of awareness can be established.</p>
REGULATORY	<p>The legal implications arising from cooperation and information exchange need to be considered; Differences in legislation and</p>

	<p>policy prevent effective cooperation. Data protection, classified information, and internal restrictions are the most relevant aspects. Policies for classifying documents also need to be reviewed to prevent delay or blocking access to information. Removal of jurisdictional barriers. Development and implementation of policies specifically related to cooperation and information sharing.</p>
--	--

Figure 6: THOR analysis - stakeholder issues

11. Learning outcomes and indicative content

Module descriptors, such as the counter terrorism one illustrated below, were produced for each of the modules. It is emphasised that at this initial stage, the content of the module descriptor may be indicative only, due to the rapidly changing nature of some of the topics being addressed. This is certainly true of counter terrorism and cybercrime. The partners maintain constant watch on developments in these areas and changes and updates will be made where necessary during the development phases. Changes may also occur as a result of ongoing stakeholder engagement and expert validation. Additionally, horizon scanning activity, which will be ongoing, by partners and the ISM-KA Horizon Scanning Tool may also have an impact on the content of the module descriptor. The process has been developed to account for and incorporate flexibility within a structured framework to accommodate these factors.

Module Name	Counter Terrorism
Module Aim	This module will provide insight into the fundamental issues in international terrorism, including Terrorist Modus Operandi, Terrorist Ideologies, Aims, Beliefs, Motivations, Counter Terrorism Strategy, Human Rights, Terrorist Financing, Border Security and Radicalisation.
Learning Outcomes	
LO1	Understand the role and impact of terrorism on the international community.
LO2	The threat to the international community and key features of an effective international response to terrorism.
LO3	Emerging trends in terrorism in the 21st century.
LO4	The background and characteristics of the international terrorist threat from terrorist organisations such as Al Qaeda, ISIS, Taliban, Boko Haram, Hamas and Hezbollah.
Indicative Content	<ul style="list-style-type: none"> Ideologies that motivate individuals and organisations to resort to terrorism. The use of various propaganda methods such as the

	<p>internet, by terrorist organisations and examining the global trends in terrorism.</p> <ul style="list-style-type: none"> • To provide students with an awareness of the functions that comprises of government and law enforcement responses, to international terrorism and considers the challenges to protect the international community from the threat of terrorism. • Students will consider and critically engage with and challenge common understandings of radicalisation and deradicalisation, in order to contribute to the improvement of the counter-radicalisation, deradicalisation and disengagement initiatives that play a crucial role in reducing the terrorist threat. • Participants will be introduced to the role that terrorist legislation and human rights standards, contributes in combating international terrorism, both in terms of the obligations, that they impose on governments and law enforcement, to protect citizens from harm and in terms of the constraints they place on the counter terrorism tactics that nations may adopt. • The question of how global information and intelligence sharing, supports numerous efforts to counter the international terrorist threat and the challenges of adapting to these challenges in today's world.
--	---

Figure 7: Counter terrorism module descriptor

12. Expert validation

In furtherance of the aim to create a shift in culture, Work Package 2 as a whole incorporates the spectrum of stakeholders, at every level and across a range of jurisdictions. The work is carried out by experienced, knowledgeable partners and will be validated by a range of stakeholders eminent in their respective fields. This is a key principle of the project and one that can be seen particularly within Work Package 2. The expert validation and input will be a continuous feature of ongoing progress. Initial plans and activities include:

- **Electronic questionnaire** – this will be the first direct contact with experts outside the consortium and AB. The format has been designed to be simple, clear and concise in recognition of the time constraints of participants and in order to maximise the number of responses, though individual experts have been / will be identified by partners in relation to each module area of expertise. This simple format will consist of the learning outcomes, that have been identified by those designing each learning module, being presented and the respondent being asked to rank its importance in this particular context. Space will be provided for suggestions and comments. This

activity is planned to take place immediately after the learning outcomes are received by partners.

- **Activity of choice** – although consistency is a key ingredient in order to organise and manage the information generated during the development of guidelines, it is also recognised that the module topic areas vary in their nature and characteristics. An additional consideration is the organisation and circumstances of different partners, therefore the activity following the questionnaire is not prescriptive but is open for partners to decide the most effective and efficient way of engaging with external experts in their respective fields. Examples developed at the time of writing include a physical workshop, telephone interviews, attendance at a European conference to obtain direct feedback captured in a short questionnaire and physical meetings with individuals. The output of these activities will be reported in the future.
- **Workshops** – in order to maximise the benefits accrued from the dissemination workshops planned for Work Package 4, it is anticipated that these can serve a dual purpose and provide a valuable opportunity to gain feedback and validation further on in the development of educational guidelines carried out in Work Package 2.

The ISM-KA AB membership is made up of experts and stakeholders from across the range of domains that are incorporated in the holistic approach to security adopted by the project. The particular value of this is that it facilitates an ongoing consultation and validation process rather than at predetermined intervals.

Prior to the first AB meeting, a questionnaire was circulated to all members, which asked their opinions on the most pertinent issues, challenges and suggested solutions in relation to the problem of tackling cybercrime. The response percentage was very high and the answers were detailed, revealing many different perspectives. These responses were analysed and the issues that arose from them were organised according to the THOR (Technical, Human, Organisational, Regulatory) model, as shown below.

ERASMUS ADVISORY BOARD PERSPECTIVES	
TECHNICAL	<i>Keeping up with technological developments was seen as a key factor for LEAs, this includes improving skills and recruiting specialists as well as creating and reconstructing more resilient software. On a wider scale, IT systems designed without inbuilt security measures were seen as a contributory problem.</i>
HUMAN	<i>LEAs need to be more skilled and competent in working with technology. Human factors relating to criminal activity involve the current low-risk / high reward equation that is a driving force for cybercrime; as this continues, the complexity of criminal networks and expertise of offenders increases. Varying perceptions of cybercrime in the global political arena presents significant challenges when trying</i>

	<p><i>to combat it.</i></p> <p><i>Awareness raising among all stakeholders is a key factor and includes recruiting key personnel in organisations as well as education of the public. Cybersecurity needs to be viewed as part of the general life rather than an isolated specialism. This shift in thinking extends to collaboration issues, which need to overcome traditional boundaries of all kinds, and stretches from authorities to individual citizens on a local and global scale. Another problem created by perception relates to victims; unwillingness to report for various reasons contributes to the scale of cybercrime.</i></p>
ORGANISATIONAL	<p><i>Organisational factors incorporate high level policy makers facilitating cooperation and collaboration and businesses and authorities effectively recruiting, training and embedding cultural change. In each stakeholder domain, a shift in approach is required so that security and awareness become inherent and collaboration is at the forefront of considerations.</i></p>
REGULATORY	<p><i>The international legal framework is important in achieving a balance between privacy and security and creating new collaborative norms. Effective and appropriate laws to secure convictions need to be put in place and sentences should reflect the impact of the wrongdoing, thereby serving as a deterrent. Cross-jurisdictional legal issues are a particular challenge when dealing with crime that recognises no boundaries. Rules relating to digital evidence and information gathering need to be understood.</i></p>

Figure 8: THOR summary of AB input for cybercrime module

In recognition of the sensitivity of some of the topics being addressed by the project, great care will be taken to ensure the protection of experts. This is particularly relevant to the counter terrorism and cybercrime modules. Only the individual having direct contact with the experts will have access to any information that enables them to be identified and any records will have strict access restrictions. This reduces not only risk to those involved but serves to reduce the burden on the project relating to its obligations in respect of information security and data protection. The use of pseudonyms will not negatively affect the quality or value of the information received.

13. Conclusion

The descriptions, illustrations and examples provide an insight to the initial stages of Work Package 2. The process developed achieved its aim of setting benchmarks and facilitating the production of a set of module descriptors that are the outcome of a methodical and thorough approach and will form the foundation for constructing the master, in Work Package 3.

Annex 1

CHANGE MANAGEMENT

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 Change Management Module

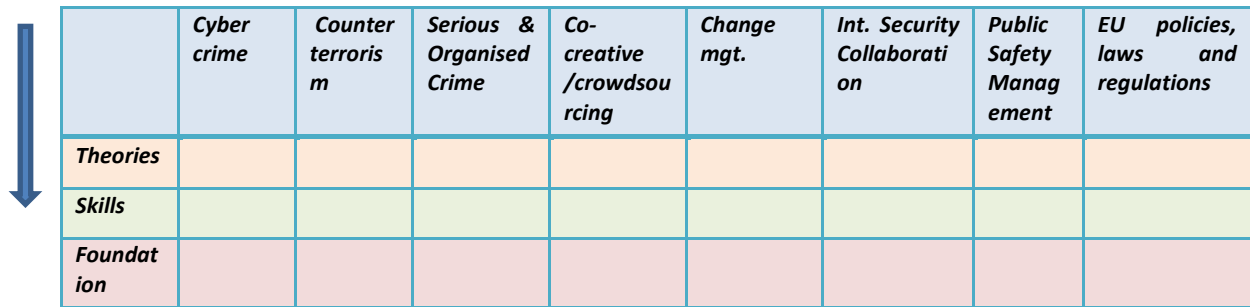
Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 Change Management Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V02
Date:	
Authors:	RSM
Document description:	Desk based analysis carried out by RSM

1 Module Descriptor

Module Name	Change Management
Module Aim	This module will provide insight in Change Management and offers hands-on knowledge about planning, implementing and evaluating complex change processes. It provides practical tools and theoretical foundations as well as a confidential and safe forum for participants to practice and exchange experiences.
Learning Outcomes	
LO1	Understand the role and impact of leadership in successful change
LO2	Understanding the context of change
LO3	Applying new knowledge to organisational change
Indicative Content	<ul style="list-style-type: none"> • Planning for complex change projects and determining the feasibility of change plans • Evaluating change success: defining adequate success criteria and analysing complex interdependencies • Change leadership • Planning and implementing change communication • Understanding and using change resistance • Engaging stakeholders • The role of technology, innovation and social media • The relevance of trust and legitimacy • Unintended side-effects of change: implications for employees and external stakeholders • The relevance of organisational identity for change success • Social costs of organisational change and downsizing • Communication skills for change management • Methodologies for co-creation • Exploring and applying group wisdom, in peer coaching sessions

The structure of the Change Management module: It will start in the first semester with foundation courses, which is a general introduction to security and management and change management. In the second semester we offer advanced courses with compulsory modules such as change management, cyber-security, counter terrorism and International Security Collaboration. In the thirds semester, students can choose a specialization into technical or governance track, depending on the background and interests of participants. A master thesis is planned for the 4th semester as empirical research project with direct practical relevance for work/organization of participation. A personal development track could run throughout programme. During the course we offer theories, knowledge and skills, which are reflected in depth in the different modules with themes/topics.

Methods / Themes and topics 



	<i>Cyber crime</i>	<i>Counter terrorism</i>	<i>Serious & Organised Crime</i>	<i>Co-creative /crowdsourcing</i>	<i>Change mgt.</i>	<i>Int. Security Collaboration</i>	<i>Public Safety Management</i>	<i>EU policies, laws and regulations</i>
<i>Theories</i>								
<i>Skills</i>								
<i>Foundation</i>								

2 Desk Based Research component

Horizon Scanning including 'THOR' Summary

In order to establish the required evidence base for this Change Management module and to establish a uniform and manageable approach, the following typology of content was considered as a baseline for this task. However, while these areas represent key considerations for this module it may be the case that additional or different topics will be pertinent to this module and we will continue to seek out relevant information, if this is the case. At the core of this Horizon Scanning task is the identification of appropriate sources which will form the basis of the analysis defined under the tasks defined under WP2. These sources include materials such as, but not excluded to:

- **Current Courses**
 - Including; existing masters courses (Inc. content, structure and accreditation)
 - Practitioner CPD courses (requirements, standards and content)
 - Professional training (current practices and requirements)
- **Stakeholder perspectives**
 - Government / institutional bodies (EU / UN)
 - Private industry
 - Law enforcement
- **Background**
 - Current research (concerns, issues, requirements, including reviews of academic literature)
 - Statistics (understand trends / growth areas)
 - Reports (e.g. Europol, Interop etc. future)
- **Current Policies**
 - Approaches, aims and priorities (UN, EU, National, international)
- **Current Practices**
 - EU
 - National
 - Interpol, UN, International
- **Legal Factors and Implications**
 - EU
 - National

- International

3 Master programmes

3.1 *Current courses Change management*

- Change Management
- Public services
- Security Management
- Entrepreneurship & Innovation
- Organisational Change
- Leadership in Professional Contexts
- Organizational Behavior
- Leadership and Management
- Leadership and Change Management
- Diversity and Change Management
- Change Management for Service Excellence
- Law and Politics of International Security
- Global Cooperation and Security
- International and European Security
- Security Management
- International Security and Global Governance
- Social change
- Change management
- Co-creation

3.2 *Professional courses (as current courses)*

- Change Management & Consulting
- Organizational Behavior Management

3.3 *Main topics outlined (Master programmes and Professional courses):*

- The role of technology, innovation, social media
- Engaging stakeholders
- Implementing change
- The relevance of trust and legitimacy
- Organisational identity for change success
- Improving quality decision making
- Change resistance
- group dynamics
- Social costs of organisational change
- Unintended side-effects of change
- Planning for complex change projects
- Collaboration and Competition
- Change leadership
- Communication.
- Communication skills for change management

- Human Resources Management
- Co –creation
- Risk management
- International relations
- International organizations
- International relations theory

3.4 SUMMARY – Current courses

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • Technology, innovation, social media
HUMAN	<ul style="list-style-type: none"> • Engaging stakeholders • Collaboration and Competition • Change leadership • Improving quality decision making
ORGANISATIONAL	<ul style="list-style-type: none"> • Engaging stakeholders • Implementing change • Risk management • The relevance of trust and legitimacy • Organisational identity for change success • Change resistance • Group dynamics • Social costs of organisational change • Unintended side-effects of change • Planning for complex change projects • Collaboration and Competition • Change leadership • Communication skills for change management • Human Resources Management • Co –creation • International relations • International organizations
REGULATORY	<ul style="list-style-type: none"> • Human Resources Management

PROFESSIONAL COURSES	
TECHNICAL	Technology for support in communication between stakeholders
HUMAN	Human aspects of organizational change and leadership mainly refer to trends and local procedures that would constitute the basis to build an effective leadership for change in and between organisations.
ORGANISATIONAL	Many of the modules are relate to organisational factors. In particular, train managers to lead change successfully by providing the theoretical background and the practical know-how to transparently plan, implement and evaluate complex change processes.
REGULATORY	Regulatory factors play a <i>subservient</i> role in change management at international level. Participant must gain understanding of laws pertaining to Human resources, international law and directives and cooperation protocols. Additionally, statutes, regulations and case law affecting the international collaboration are more widely are included.

4 Stakeholders perspective

- Change management--or change leadership?
<http://www.tandfonline.com/doi/abs/10.1080/714023845>
- How Does Authentic Leadership Influence Planned Organizational Change? The Role of Employees' Perceptions: Integration of Theory of Planned Behavior and Lewin's Three Step Model
<http://www.tandfonline.com/doi/abs/10.1080/14697017.2017.1299370>
- Influence of participation in strategic change: resistance, organizational commitment and change goal achievement
<http://www.tandfonline.com/doi/full/10.1080/1469701042000221696>
- Success and Failure In Organizational Change: An Exploration of the Role of Values
<http://www.tandfonline.com/doi/full/10.1080/14697017.2010.524655>
- The Hard Side of Change Management
<https://www.europeanleadershipplatform.com/assets/downloads/infoItems/167.pdf>
- The Impact of Leadership and Change Management Strategy on Organizational Culture and Individual Acceptance of Change during a Merger
<http://onlinelibrary.wiley.com/doi/10.1111/j.1467-8551.2006.00480.x/full>
- Internal communication during change management
<http://www.emeraldinsight.com/doi/full/10.1108/13563280210416035>
- Haunted by the Past: Effects of Poor Change Management History on Employee Attitudes and Turnover
<http://journals.sagepub.com/doi/abs/10.1177/1059601110392990>
- Transformational leadership in the context of organizational change
<http://www.emeraldinsight.com/doi/full/10.1108/09534819910263631>
- Influence of participation in strategic change: resistance, organizational commitment and change goal achievement
<http://www.tandfonline.com/doi/abs/10.1080/1469701042000221696>
- Want to, need to, ought to: employee commitment to organizational change
<http://www.emeraldinsight.com/doi/full/10.1108/09534810810847020>

A summary of all end-user engagement activities identified the following areas of priority or particular challenge:

4.1 Enhancing awareness on Change management

The quite unpredictable organizational environment of current volatility and uncertainty requires new forms of organizational adaptation. Practitioner observe since quite some time that greater uncertainty turns market forecasting and strategic planning in daunting tasks (Bennett & Lemoine, 2014¹; McKinsey 2010²). Persistent sources of disruptions emerged in the globalized world that cut down profits or seem to force organizations to miss market opportunities, just as new and unforeseen opportunities materialized (Doheny et al. 2012³). Complex organizational collaborations and the need to react to diverse stakeholder groups in interconnected markets are the ingredients for a nearly constant pressure on organizations to change.

It is very relevant in this volatile environment, to prepare organizations for the “unthinkable”. Change management gets in this context a different meaning, as organizations do not anymore face stable after changing times, but are in an environment of constant change. Also, does the interconnectivity of today's society imply, that crisis in all parts of the world can impact local players. The ability of people at the highest levels of corporate and public services leadership to be ready to spot and handle such crises while leveraging related opportunities, is of utmost importance. Executive leadership at the top levels of corporate, public service and political life faces new vulnerabilities. Change management provides a framework to help leaders, managers and organisations operate in a state of readiness to identify and manage crises by supporting risk management, improving quality decision making and implementing change through the business model.

4.2 How to lead successful change

While change must be well managed, it also requires effective leadership to be successfully introduced and sustained. An integrative model of leadership for change can be used, reflecting its cognitive, spiritual, emotional and behavioural dimensions and requirements. The model comprises vision, values, strategy, empowerment, and motivation and inspiration. The planning, implementing and evaluating complex change processes and determining the feasibility of change plans; Evaluating change success: defining adequate success criteria and analysing complex interdependencies; Change leadership; Planning and implementing change communication; Understanding and using change resistance. Practical tools and theoretical foundations for leading change successfully. A core ingredient of successful change is the ability to involve all relevant stakeholders. The complexity of most challenges requires knowledge on all levels of the organization.

4.3 Understanding the context of change

Engaging stakeholders; the role of technology, innovation and social media; the relevance of trust and legitimacy; Unintended side-effects of change: implications for employees and external stakeholders; The relevance of organisational identity for change success; Social costs of organisational change.

¹ Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons*, 57(3), 311-317.

² McKinsey (2010) Welcome to the volatile world. McKinsey Germany. Retrieved from www.mckinsey.com/.../mckinsey/.../welcome_to_the_volatile_world

³ Doheny, M., Nagali, V., and Weig, F. (2012) Agile operations for volatile times. McKinsey Quarterly. Retrieved from <http://www.mckinsey.com/business-functions/operations/our-insights/agile-operations-for-volatile-times>.

4.4 Applying new knowledge to organisational change

Communication skills for change management; Methodologies for co-creation; Exploring and applying group wisdom, in peer coaching sessions.

4.5 SUMMARY - Stakeholders' perspective

STAKEHOLDER PERSPECTIVES	
TECHNICAL	Technology refers to bridge a perceived gap between practitioner emphasis upon change management tools and techniques and academic emphasis upon change management theories, models and concepts. The classification of change management tools and techniques deepens understanding, enables more rigorous scrutiny of claims made for their efficacy, and forms the basis for change managers to make informed choices.
HUMAN	Strong leadership is central to successful major change, but some leaders shy away from engaging in it or declare victory too early. A good leader builds high levels of commitment and resolve. Ultimate success depends on discipline and the right implementation framework. The good leader is adaptable and can therefore navigate change successfully. Other key factors in change management are employee attitudes such as trust, job satisfaction, turnover intentions, change cynicism, and openness to change. A change vision, employee-manager relationship quality, job motivation, and role autonomy all influence commitment to change.
ORGANISATIONAL	The importance of leadership to the change management process is underscored by the fact that change, by definition, requires creating a new system and then institutionalizing the new approaches. Enhance internal communications procedure contribute to the "successful" implementation of change management programmes.
REGULATORY	The legal implications arising from successful change management need to be considered: differences in legislation and policy prevent effective change management and human resources. Development and implementation of labor and human resource policy are related to successfully implement change.

5 Background

5.1 Current research

- Belias D. Koustelios, A. (2014). The impact of leadership and change management strategy on organizational culture <file:///C:/Users/61456mfr/Downloads/2996-8812-1-PB.pdf>
In this paper, the authors present the impact of leadership and change management strategy on organizational culture. At first, they present the notion of culture. There are many attempts to describe "organizational culture", many of which are presented in this paper. After an assessment of organizational culture, the role of leader is pinpointed.
- Cummings, S. Bridgman, T. & Brown KG. (2016). Unfreezing change as three steps: Rethinking Kurt Lewin's legacy for change management.
<http://journals.sagepub.com/doi/abs/10.1177/0018726715577707>
Kurt Lewin's 'changing as three steps' (unfreezing → changing → refreezing) is regarded by many as the classic or fundamental approach to managing change. Lewin has been criticized by scholars for over-simplifying the change process and has been defended by others against such

charges. However, what has remained unquestioned is the model's foundational significance. It is sometimes traced to the first article ever published in Human Relations. Based on a comparison of what Lewin wrote about changing as three steps with how this is presented in later works, the authors argue that Lewin never developed such a model and it took form after his death. They investigate how and why 'changing as three steps' came to be understood as the foundation of the fledgling subfield of change management and to influence change theory and practice to this day, and how questioning this supposed foundation can encourage innovation

- Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., Kabst, R. (2016) How effective are behavior change interventions based on the theory of planned behavior?

<http://econtent.hogrefe.com/doi/abs/10.1027/2151-2604/a000255?journalCode=zfp>

The theory of planned behavior (TPB) is a prominent framework for predicting and explaining behavior in a variety of domains. The theory is also increasingly being used as a framework for conducting behavior change interventions. In this meta-analysis, the authors identified 82 papers reporting results of 123 interventions in a variety of disciplines. Their analysis confirmed the effectiveness of TPB-based interventions, with a mean effect size of .50 for changes in behavior and effect sizes ranging from .14 to .68 for changes in antecedent variables (behavioral, normative, and control beliefs, attitude, subjective norm, perceived behavioral control, and intention). Further analyses revealed that the interventions' effectiveness varied for the diverse behavior change methods. In addition, interventions conducted in public and with groups were more successful than interventions in private locations or focusing on individuals. Finally, the authors identified gender and education as well as behavioral domain as moderators of the interventions' effectiveness.

5.2 Statistics

- Harvard Business Review (2013) Change Management Needs to Change

<https://hbr.org/2013/04/change-management-needs-to-cha>

As a recognized discipline, change management has been in existence for over half a century. Yet despite the huge investment that companies have made in tools, training, and thousands of books (over 83,000 on Amazon), most studies still show a 60-70% failure rate for organizational change projects — a statistic that has stayed constant from the 1970's to the present. Given this evidence, is it possible that everything we know about change management is wrong and that we need to go back to the drawing board? Should we abandon Kotter's eight success factors, Blanchard's moving cheese, and everything else we know about engagement, communication, small wins, building the business case, and all of the other elements of the change management framework? While it might be plausible to conclude that we should rethink the basics, there could be an alternative explanation: The content of change management is reasonably correct, but the managerial capacity to implement it has been underdeveloped. In fact, instead of strengthening managers' ability to manage change, we've instead allowed managers to outsource change management to HR specialists and consultants instead of taking accountability themselves — an approach that often doesn't work.

5.3 Reports

- Deloitte. Demystifying change management.

<https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/public-sector/lu-demystifying-change-management.pdf>

The core leadership challenge is how to lead a company and government departments through the speed and nature of fundamental change that threatens the very conformity which has allowed the current leadership cohort to qualify for the top.

- Prosci. (2016) Best Practices in change Management. <http://www.assochange.it/wp-content/uploads/2016/07/Best-Practices-Executive-Summary.pdf>

This publishing of Prosci's benchmarking research in change management, the 2016 edition of Best Practices in Change Management compiles the experience and lessons learned from thousands of project and change leaders. Increase your effectiveness by leveraging these lessons learned, common success factors, and mistakes to avoid when implementing change management. Benchmark your organization's approach against best practices, add rigor to your practice and achieve more consistent outcomes. As the largest body of research in the field of change management, the Best Practices in Change Management – 2016 Edition report culminates two decades of research and insights from over 4,520 participants from 56 countries. With over 350 pages, and 275 tables and figures, this comprehensive report covers a broad range of change topics.

- Gowing & Langdon (2015) Thinking-The-Unthinkable-Report.
<http://thinkunthinkable.org/downloads/Thinking-The-Unthinkable-Report.pdf>
Executive leadership at the highest levels of corporate, public service and political life faces new vulnerabilities that few in these positions are willing to talk about publicly. In 2016, they are greater than at any time in recent history, and the implications are deeply troubling. This study heard that growing evidence for what were claimed to be 'unthinkables' did often exist. But often blind eyes were turned, either because of a lack of will to believe the signs, or an active preference to deny and then not to engage. The core leadership challenge is how to lead a company and government departments through the speed and nature of fundamental change that threatens the very conformity which has allowed the current leadership cohort to qualify for the top.

5.4 SUMMARY - Background

CURRENT RESEARCH	
TECHNICAL	
HUMAN	Organizational culture and the role of leader as crucial factors in the change process.
ORGANISATIONAL	Development of the model 'changing as three steps' came to be understood as the foundation of the fledgling subfield of change management and to influence change theory and practice to this day; The effectiveness of Theory Planned Behaviour-based interventions. Interventions conducted in public and with groups were more successful than interventions in private locations or focusing on individuals. Also, gender and education as well as behavioral domain as moderators of the interventions' effectiveness.
REGULATORY	

STATISTICS	
TECHNICAL	
HUMAN	The content of change management is reasonably correct, but the managerial capacity to implement it has been underdeveloped.
ORGANISATIONAL	Companies have made large investments in tools, training, and thousands of books. However, most studies still show a 60-70% failure rate for organizational change projects.
REGULATORY	

REPORTS	
TECHNICAL	
HUMAN	The speed and nature of fundamental change can threaten the very conformity which has allowed the current leadership cohort to qualify for the top.
ORGANISATIONAL	Increase the organisation's effectiveness by leveraging these lessons learned, common success factors, and mistakes to avoid when implementing change management
REGULATORY	

6 Current Policies

6.1 Current policies

- Change management is engaged in systematically changing organizations and individuals within organizations.

<http://www.ubsbusiness.nl/kennisbank/change-management/>

Within change management, we distinguish three aspects: adapt to change, control of change, and execution of change. Important concepts and approaches within change management are:

- Increase efficiency
- Restructuring and Improving Business Process Management
- Improve the functioning of human beings in organizations

Within the field of change management, change can be implemented in a planned way or in a spontaneous way. Scheduled change can be done from a design model or a development model. A design model is usually centralized, used for a high level of control and based on established work instructions. A development model is usually decentralized and depends on the creativity of people and the ability of the organization to adjust themselves. The development model is more focused on sense of responsibility and trust than on control. In spontaneous change, the change is not controllable, but the change is self-evident in the organization. Spontaneous change has interfaces with chaos theory, complexity thinking and the self-organizing ability of organizations.

- Resistance: a constructive tool for change management

<http://www.emeraldinsight.com/doi/full/10.1108/00251749810232628>

Traditionally, resistance has been cast as adversarial - the enemy of change that must be defeated if change is to be successful. While it is apparent that classical management theory viewed resistance in such a manner, recent literature contains much evidence that suggests resistance may indeed be useful and is not to be simply discounted. Present day suggestions and prescriptions for managing resistance have evidently disregarded this research and left little room for utility in resistance. This paper argues that the difficulty of organisational change is often exacerbated by the mismanagement of resistance derived from a simple set of assumptions that misunderstand resistance's essential nature. It is suggested that management may greatly benefit from techniques that carefully manage resistance to change by looking for ways of utilising it rather than overcoming it.

6.2 SUMMARY – Current policies

<i>Current policies</i>	
TECHNICAL	
HUMAN	Improve the functioning of human beings in organizations
ORGANISATIONAL	Increase efficiency, restructuring and Improving Business Process Management
REGULATORY	Using HRM and national law on labor

7 Current Practice

7.1 Current practices

- Organisational change management: A critical review
<http://www.tandfonline.com/doi/abs/10.1080/14697010500359250>

It can be argued that the successful management of change is crucial to any organisation in order to survive and succeed in the present highly competitive and continuously evolving business environment. However, theories and approaches to change management currently available to academics and practitioners are often contradictory, mostly lacking empirical evidence and supported by unchallenged hypotheses concerning the nature of contemporary organisational change management. The purpose of this article is, therefore, to provide a critical review of some of the main theories and approaches to organisational change management as an important first step towards constructing a new framework for managing change. The article concludes with recommendations for further research.
- The Strategic Management of Corporate Change
<http://journals.sagepub.com/doi/abs/10.1177/001872679304600801>

To investigate the controversy between universal and contingent approaches to corporate change, a study was undertaken of 13 service sector organizations. The study used the Dunphy/Stace contingency model of organizational change strategies, developing measures to place the organizations within the model. Results indicate that universal models of change management are inadequate to describe the diversity of approaches actually used by these organizations. In particular, the traditional Organizational Development model is unrepresentative of how change in many contemporary organizations is actually made. The traditional OD model prescribes incremental change combined with a participative management style but most organizations in the study made rapid transformative change using a directive leadership style. The OD model is also inadequate as a prescriptive model because very different change strategies, some dramatically different from OD, resulted in successful financial performance. Four case studies are presented to illustrate how each of the major contingencies in the model can operate to create effective organizational performance.
- Reflections: our Journey in Organizational Change Research and Practice
<http://www.tandfonline.com/doi/full/10.1080/14697010902879079>

This commentary summarizes research and practice on the topic of organizational change over the past 30 years. The purpose in preparing this commentary is to explain how the effort of the authors accumulated over this period to produce the questions they addressed, the answers the findings revealed, and the direction of future efforts. The authors summarize their journey thus far relative to six signposts, namely: (a) the identification of five key beliefs underlying change recipient motivations to change; (b) an emphasis on change recipient active participation in the change effort; (c) the importance of diagnosis; (d) the importance of creating readiness for change; (e) the identification of strategies for influencing the five beliefs throughout the change process; and, (f) the assessment of reactions to organizational change. To give an idea of where the journeys will take us in the future, they identify five trips to make: (a) examine the relative

importance of the five key beliefs for influencing change recipient support; (b) expand our cognitive view of change motivation to include emotional reactions to change; (c) investigate the relationship between change recipient characteristics (such as regulatory focus) and reactions to organizational transformation; (d) explore the relationship between internal contextual variables (relations with local change agents and co-workers) during organizational change; and (e) focus on ethics in organizational change.

- Integrated change management unit

<https://www.google.com/patents/US7356482>

An integrated system for managing changes in regulatory and non-regulatory requirements for business activities at an industrial or commercial facility. Application of this system to environmental, health and safety activities, and to food, drug, cosmetic, and medical treatment and device activities, are discussed as examples. The system: provides one or more databases that contain information on operations and requirements concerning an activity or area of business; receives information on regulatory and non-regulatory changes that affect operations of the business; converts these changes into changes in data entry forms, data processing and analysis procedures, and presentation (by printing, electronic display and/or distribution) of data processing and analysis results to selected recipients, without requiring the services of one or more programmers to re-key and/or reformat the items affected by the change; and implements receipt of change information and dissemination of data processing and analysis results using the facilities of the Internet

- A change management process: Grounded in both theory and practice

<http://www.tandfonline.com/doi/abs/10.1080/714042520>

There exists in the literature a number of change models to guide and instruct the implementation of major change in organisations. Three of the most well-known are Kotter's strategic eight-step model for transforming organisations, Jick's tactical ten-step model for implementing change, and General Electric (GE)'s seven-step change acceleration process model. This paper introduces a framework that draws from these three theoretical models but is also grounded in the reality of the change process at a Fortune 500 defence industry firm. The purpose of the paper is to provide guidance to the practitioner leading an organisational change process. This guidance is grounded in both theory and practice. The guidance is further enriched by the demonstrated use of such methodologies as mind mapping, lessons learned, storytelling and metaphors.

7.2 SUMMARY – Current practice

TECHNOLOGY	Using methodologies as mind mapping, lessons learned, storytelling and metaphors. Using facilities of the Internet.
HUMAN	Incremental change combined with a participative management style but most organizations can made rapid transformative change using a directive leadership style.
ORGANISATIONAL	Theory and practice in practitioner leading an organisational change process. emphasis on change recipient active participation in the change effort, the importance of diagnosis, the importance of creating readiness for change, the identification of strategies for influencing the five beliefs throughout the change process and the assessment of reactions to organizational change.
REGULATORY	To align universal and contingent approaches to corporate change with engaging mechanism from theory and practice. Define relationships between change recipient characteristics, such as regulatory focus

8 'THOR' Summary

Change Management	
TECHNICAL	<ul style="list-style-type: none"> • The role of technology, innovation, social media as used in (the response to) safety and security issues and criminal procedures
HUMAN	<ul style="list-style-type: none"> • Engaging stakeholders in the safety and security domain • The relevance of trust and legitimacy • The relevance of organisational identity for change success • Understanding and using change resistance • Exploring and applying group wisdom, in peer coaching sessions
ORGANISATIONAL	<ul style="list-style-type: none"> • Social costs of organisational change and downsizing • Unintended side-effects of change: implications for employees and external stakeholders • Planning for complex change projects and determining the feasibility of change plans • Evaluating change success: defining adequate success criteria and analysing complex interdependencies • Change leadership • Planning and implementing change communication between public-, private- and other relevant stakeholders in the security domain. • Communication skills for change management • Get a project started on the right path using those best practices learned from both successful and unsuccessful projects.
REGULATORY	<ul style="list-style-type: none"> • Human Resources law • Labor and Employment law • International labour law

Annex 2

CO-CREATION & CROWDSOURCING

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 Co-Creation and Crowdsourcing Module

Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 Co-Creation and Crowdsourcing Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V02
Date:	
Authors:	INITIATIVES, RSM and Estoril
Document description:	Desk based analysis for Co-Creation and Crowdsourcing

1. Module Descriptor

Module Name	Co-Creation and Crowdsourcing
Module Aim	This module will provide insight in Co-Creation and Crowdsourcing. It will provide tools and offers hands-on models and methodologies to harvest their potential.
Learning Outcomes	
LO1	Understand the role and impact of leadership in co-creation and crowdsourcing
LO2	Understanding the changing role of leadership in safety and security as well as the changing role of safety and security in society
LO3	Applying new knowledge to co-creation and crowdsourcing and problem based competencies for targeting operational as well as strategic challenges.
Indicative Content	<ul style="list-style-type: none"> • Designing co-creation initiatives • Setting performance management indicators for external collaboration • Emerging trends in safety and security and the role of co-creation and crowdsourcing in mitigating these risks • Trust and confidentiality • Driving change for impact in multistakeholder initiatives • Planning and delivering in cross-sectoral programs • Communicating internally and externally in partnerships.

2. Desk Based Research component

Horizon Scanning including 'THOR' Summary

The co-creation and crowdsourcing module should be based on a problem-based methodology with casework that targets emerging trends (e.g. automation, migration, ageing etc) and technologies (e.g. AI, space, block tech, data science). In order to establish the required evidence base for this co-creation and crowdsourcing module and to establish a uniform and manageable approach, the following typology of content was considered as a baseline for this task. However, while these areas represent key considerations for this module it may be the case that additional or different topics will be pertinent to this module and we will continue to seek out relevant information, if this is the case. At the core of this Horizon Scanning task is the identification of appropriate sources which will form the basis of the analysis defined under the tasks defined under WP2. These sources include materials such as, but not excluded to:

- **Current Courses**
 - Including; existing masters courses (Inc. content, structure and accreditation)
 - Practitioner CPD courses (requirements, standards and content)
 - Professional training (current practices and requirements)
- **Stakeholder perspectives**
 - Government / institutional bodies (EU / UN)
 - Private industry
 - Law enforcement

- **Background**
 - Current research (concerns, issues, requirements, including reviews of academic literature)
 - Reports

3. Master programmes

3.1. *Specific courses (as current courses)*

- MSc Business Design. (Domus Academy, Postgraduate School of Design. Milan) Italy <http://www.domusacademy.com/en/master/master-in-business-design/>
- MSc Strategic Leadership towards Sustainability. (Blekinge Institute of Technology, Department of Strategic Sustainable Development, Karlskrona Sweden) <http://www.msls.se/>
- MSc Business Development and Entrepreneurship. (Utrecht University, The Netherlands) <https://www.uu.nl/masters/en/business-development-and-entrepreneurship>
- MA Creative Practices and Direction. University of Surrey, UK <https://www.surrey.ac.uk/postgraduate/creative-practices-and-direction-2017>
- MSC Enterprise and Business Creation. (Norwich Business School, UK) <https://www.uea.ac.uk/documents/5212420/0/Enterprise+and+Business+Creation+final.pdf/2a8a3b99-7438-457d-9ff5-6878ef21f3d9>
- Course Crowdsourcing. (University of Tilburg, The Netherlands) <https://mystudy.uvt.nl/it10.vakzicht?taal=n&pfac=FGW&vakcode=880504>
- Masterclass Crowdsourcing. (SRM The Netherlands) http://www.opleidingenberoep.nl/ts/ob/cursus-opb-25975-Masterclass_Crowdsourcing.html

3.2. *Main topics outlined (Master programmes and Professional courses):*

- The role of co-creation and crowdsourcing in a connected society
- Multistakeholder engagement
- Co-Creation as Problem Solving
- Emerging trends and the role of co-creation and crowdsourcing
- Co-Creation in Change Management
- How to design large scale co-creation initiatives
- Co-Creation for Global Impact
- Performance Metrics in Co-Creation
- Innovation through crowdsourcing
- Co-Creation and Innovation practices
- Competencies and capabilities in Co-Creation
- Innovation through Partnerships and Co-Creation

3.3. SUMMARY – Current courses

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • The role of technology to support co-creation and crowdsourcing matters such as idea generation, progress reporting, knowledge sharing and inspiration. • Technology, innovation, social media
HUMAN	<ul style="list-style-type: none"> • Focusing on specific co-creation-related issues and challenges of international security • Understand how co-creation differs from other forms of engagement • Learn problem re-framing as foundation for engaging other stakeholders • Understand the role of design thinking and human-centered practice in co-creation • Applying human-centred design research as practiced in the context of international security • Mapping spoilers and enablers for co-creation initiatives and planning accordingly Multi-stakeholder engagement • Partnerships and Co-Creation • Networks and partnerships • Competencies and capabilities for multistakeholder engagement
ORGANISATIONAL	<ul style="list-style-type: none"> • Multi-stakeholder engagement • Co-Creation pipeline • Crowdsourcing and IPR • External engagement and internal robustness • Strategic Partnerships • Designing for crowdsourcing • Collaboration and Competition • Organizational design for external engagement • Human Resources in times of external engagement • Conduct value potential and impact analysis for future partners • Developing organisational platforms for multi-initiatives engagement • Learning practical implications from real life co-creation initiatives in a safety and security context from an educational point of view • Understand difference between co-creation, crowdsourcing, partnerships, innovation projects ect. • Inter-organisational planning and communication • Setting targets in multi-stakeholder initiatives
REGULATORY	<ul style="list-style-type: none"> • Regulatory and legal affairs in designing and driving external partnerships • Public tenders • Data protection regulation

PROFESSIONAL COURSES	
TECHNICAL	How to exploit technology for co-creation and crowdsourcing
HUMAN	Human aspects of strategic partnerships, co-creation and crowdsourcing relate to the changing mindset in the organization for bringing in other competencies and capabilities in relation to specifically trust, competition and organizational politics. This refers to employees, specialists and to leadership in the organization.
ORGANISATIONAL	There are very few professional courses that relate to the organizational aspects of co-creation and crowdsourcing. However, co-creation and crowdsourcing are essential elements in organizational courses that deal with new business models, disruptive markets and startup approaches to business. These include culture, organizational design and organizational structure and change in relation to the need for co-creation and crowdsourcing in organizations.
REGULATORY	Regulatory and legal are essential to co-creation, crowdsourcing and external partnerships. Such external collaborations require that both regulatory and legal as well as csr are integrated into the core of the agreements and design of such initiatives. This is the case for private as well as public and private-public initiatives.

4. Stakeholders perspective

- **Harvard Business Review: Creating Shared value**
<https://hbr.org/2011/01/the-big-idea-creating-shared-value>
- **Book: The Co-creation paradigm. 2014, Stanford University Press.**
- Journal of Design, Business & Society: How to design for large-scale multi-stakeholder co-creation initiatives – reframing crime prevention challenges with the police in Denmark
<https://www.intellectbooks.co.uk/journals/view-Article,id=19161/>
- Journal of Strategic Marketing: The mechanisms of value co-creation
<http://www.tandfonline.com/doi/abs/10.1080/0965254X.2012.671339>
- Strategy & Leadership: A ten-year perspective on how the value co-creation revolution is transforming competition
<http://www.emeraldinsight.com/doi/full/10.1108/SL-07-2013-0058>
- Journal of Business Research: Stakeholder co-creation during the innovation process: Identifying capabilities for knowledge creation among multiple stakeholders
<http://www.sciencedirect.com/science/article/pii/S0148296315002106>
- Strategy & Leadership: Strategy and co-creation thinking
<http://www.emeraldinsight.com/doi/full/10.1108/SL-07-2013-0053>
- European Business Review: The meanings of co-creation
<http://www.emeraldinsight.com/doi/full/10.1108/09555341311287754>
- European Business Review: Value co-creation: theoretical approaches and practical implications
<http://www.emeraldinsight.com/doi/full/10.1108/09555341311287718>

A summary of all end-user engagement activities identified the following areas of priority or particular challenge:

4.1. Enhancing awareness on Co-Creation and Crowdsourcing

Shaping innovation and driving impact through co-creation and crowdsourcing is a premise for safety and security organizations today.

Security professionals experience increasing expectations from citizens and politicians, increasingly complex crime patterns at the same time as demands for efficiency optimization and cost cutting. Therefore, we need to tap into resources outside of the police to constantly innovate with the same or less resources at hand while catering to the increasing demands from society.

Co-Creation and crowdsourcing are essential in targeting emerging trends and tendencies within space, 5G, AI, block chain and other technological advancements.

The needs for co-creation, crowdsourcing and partnerships are not just results of insufficient internal resources. Tapping into these approaches also enables security professionals of innovative practices that would not be possible if all resources were in-house. For example when working with community resilience in vulnerable neighbourhoods or influencing technology providers such as mobile companies to reduce smartphone theft from citizens, which would not be possible as internal initiatives regardless of how many resources were available.

Furthermore, tapping into external resources to innovate and drive impact opens up for a speed and agility. With the specialization and dynamic nature of crime patterns today, it would be too time consuming for security professionals to source and train specialists for new emerging criminal specialties before these crime patterns will have changed again.

4.2. Context of Co-Creation and the Changing Role of Leadership for Security Professionals

The changing role of security professionals and the cultural consequences provide a leadership challenge in addressing these cultural aspects. However, roles are changing not only in safety and security. The roles of citizens are changing, the roles of private corporations are changing and the roles of other public institutions are changing as well. Citizens want to be engaged. They want insights and influence in not just domestic issues but also in police related challenges. Historically, security professionals have depended on the public and on citizens as sources of information. Today, citizens want to be engaged far beyond being passive informers and with today's social technologies, citizens can prove to be an enormous capacity when providing the necessary platforms.

Private businesses have been providing resources to local society based challenges during the past decades through corporate social responsibilities (CSR). This has been valuable for many security related initiatives. However, many private businesses are changing their efforts for society by moving from CSR to being engaged in specific initiatives in which they can utilize their specialties and competencies rather than giving funds.⁴ Public authorities experience the same changing roles. They also strive towards a higher degree of cross-sectorial collaboration. However, a major challenge in cross-sectorial collaboration between public institutions lies in conflicting targets and performance metrics when dealing with safety and security related challenges that are by nature cross-sectoral and international.

4.3. Applying new knowledge to Co-Creation and Crowdsourcing

Communication skills for external communication; cross-sectoral partnerships; Metrics in multi-stakeholder impact; change management in cross-organizational initiatives;

⁴ See the text Porter and Cramer, 2010.

Methodologies for co-creation; Methodologies and technologies for crowdsourcing; Tools for designing Multi-Co-Creation

4.4. SUMMARY - Stakeholders' perspective

STAKEHOLDER PERSPECTIVES	
TECHNICAL	Technology is essential harvesting the potential of co-creation and crowdsourcing approaches to safety and security challenges. To ensure external engagement, technology in the forms of SOME and performance technologies.
HUMAN	Capabilities and competencies across the organization are pivotal in transforming the organization to an outreach outside of the organization. Human capabilities pipeline identify leadership competencies, specialist requirements and general knowledge and capabilities for co-creation and crowdsourcing. These include culture, strategic partnerships, innovation and engagement.
ORGANISATIONAL	Organizational design and organization structures are mainly designed for internal processes. Therefore, organizational challenges and opportunities of co-creation and crowdsourcing are necessary to address. Such organizational concerns relate to – but are not restricted to – structure, performance, work processes, leadership processes, and strategy.
REGULATORY	Regulatory and legal aspects of external collaboration when targeting essential challenges and opportunities require a professional focus from the outset. This is both due to the risks of confidential information, IPR issues, but not least to ensure trust from the starting point.

5. Background

5.1. Current research

- Co-Design international journal of : Co-creation, Prevailing Streams and a Future Design Trajectory
[http://research.cbs.dk/da/publications/cocreation-prevailing-streams-and-a-future-design-trajectory\(6fc0db8e-1eaa-46b4-b7be-fc2b2bfc1c8a\).html](http://research.cbs.dk/da/publications/cocreation-prevailing-streams-and-a-future-design-trajectory(6fc0db8e-1eaa-46b4-b7be-fc2b2bfc1c8a).html)
- Bidar, R., Watson, J., & Alistair, B. (2017) Classification of service co-creation systems: An integrative approach
<http://ieeexplore.ieee.org/abstract/document/7890109/keywords>

5.2. Reports

- Open Government Partnership. (2016). Co-Creation Guidelines.
http://www.opengovpartnership.org/sites/default/files/Co-creation-guidelines_Sept2016.pdf
- European Public Sector Information Platform. (2016). Co-creating Public Policies or Ways to Bring Citizens into the Process.
https://www.europeandataportal.eu/sites/default/files/2016_co_creating_public_policies_or_ays_to_bring_citizens_into_the_process.pdf

5.3. SUMMARY - Background

CURRENT RESEARCH	
TECHNICAL	Specifically aimed at tech for co-creation and crowdsourcing through SOME and IT platforms as well as performance management .
HUMAN	Competencies and capabilities for external collaboration and partnerships requires a structured approach to the capability pipeline.
ORGANISATIONAL	Partnerships, co-creation and crowdsourcing are external to the organization, whereas organizational structures are designed for internal quality assurance and management. Therefore, organizational design plays a pivotal role and requires structural change when emphasizing co-creation and crowdsourcing.
REGULATORY	IPR, confidentiality and not least trust are essential in co-creation and crowdsourcing. Therefore, regulatory and legal aspects are high on the agenda from day one.

6. 'THOR' Summary

Change Management	
TECHNICAL	<ul style="list-style-type: none"> • The role of SOME, technology, innovation, social media as used in (the response to) safety and security issues and criminal procedures
HUMAN	<ul style="list-style-type: none"> • Multi-stakeholder approaches in the safety and security domain • Competencies and capabilities for external outreach and impact • Leadership in strategic partnerships, co-creation initiatives and crowdsourcing
ORGANISATIONAL	<ul style="list-style-type: none"> • External focus in organizational design. • Performance management in external partnerships • Work processes across organizations • Leadership processes when including other organizations, authorities and individuals.
REGULATORY	<ul style="list-style-type: none"> • IPR • Confidentiality • Trust

Annex 3

INTERNATIONAL SECURITY COOPERATION

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 International Security Cooperation Module

Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 International Security Cooperation Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V01
Date:	September 2017
Authors:	FORMIT
Document description:	Desk based analysis, THOR summaries and module descriptor

1. Module Descriptor

Module Name	Cross-border Security Cooperation
Module Aim	This module will provide trainees with a general overview on the main international issues related to security in parallel with relevant actors and related procedures to deal with such emerging threats through structured cooperation initiatives of different type.
Learning Outcomes	
LO1	Current and emerging challenges related to security at international level
LO2	Role of the main bodies acting in Europe (national, European and International)
LO3	Interagency cooperation: from the technical, human, organizational and regulatory perspective
Indicative Content	<ul style="list-style-type: none"> • LO1 - Description of current security trends and growing threats (e.g. CBRNe and hazardous material trafficking, and psychological effects of terrorism) • LO2 - EUROPOL, INTERPOL, UN, CEPOL, OSCE, Eurojust, Frontex, national authorities and agencies and their roles and responsibilities • LO3 - EU planning response cooperation; modified roles and responsibilities; decision making; LEAs scene management/emergency services (including medical services and triage).

2. Current Courses

2.1. *Masters Courses*

- Strategy and Security
- International Defence and Security
- International Security Studies
- Law and Politics of International Security
- Global Cooperation and Security
- Security, Intelligence and Strategic Studies
- Intelligence & International Security
- International Security
- International and European Security
- Intelligence and Security Studies
- Terrorism, International Crime and Global Security
- Security Management
- International Conflict and Security
- International Security and Global Governance

2.2. *Professional courses (as current courses)*

- Managing International Cooperation and Development
- International Security
- Rapid Expert Assistance and Cooperation Teams for Conflict Prevention, Crisis-Management and Post-Conflict rehabilitation

2.3. *Main topics outlined (Master programmes and Professional courses):*

- Security, Collaboration and Competition
- Transnational Crime, Terrorism, and Insurgency
- Governance, State Weakness, and Human Security
- Comparative National Security Policies
- International relations theory
- Global, national and human security trends
- Post-conflict security and international interventions
- Geopolitical trends and implications for state security sectors and sub-regional efforts to promote peace and security
- Key actors, roles and responsibilities across the international, regional and subregional security communities
- International law and international relations
- UN system of collective security
- International terrorism
- Building of security communities
- Arms control and disarmament
- European and international security strategies

- International security & strategic thought
- Security and technology
- Peacekeeping and peacebuilding
- International Issues and Institutions
- International Security, theories & concepts
- International relations
- International organizations
- Foreign policy making & analysis
- Governance, security and development extra-UE countries
- EU Politics and Governance
- Foreign policy
- Security policy
- Global Strategy and Regional Issues

2.4. SUMMARY – Current courses

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • Security and technology
HUMAN	<ul style="list-style-type: none"> • Transnational Crime, Terrorism, and Insurgency • Global, national and human security trends • Geopolitical trends and implications for state security sectors and sub-regional efforts to promote peace and security • International terrorism
ORGANISATIONAL	<ul style="list-style-type: none"> • Security, Collaboration and Competition • Governance, State Weakness, and Human Security • Comparative National Security Policies • International relations theory • Post-conflict security and international interventions • Key actors, roles and responsibilities across the international, regional and sub-regional security communities • UN system of collective security • Building of security communities • Arms control and disarmament • European and international security strategies • International security & strategic thought • Peacekeeping and peacebuilding • International Issues and Institutions • International Security, theories & concepts • International relations • International organizations • Foreign policy making & analysis • Governance, security and development extra-UE countries • EU Politics and Governance

	<ul style="list-style-type: none"> • Foreign policy • Security policy • Global Strategy and Regional Issues
REGULATORY	<ul style="list-style-type: none"> • Law and Politics of International Security • International law and international relations

PROFESSIONAL COURSES	
TECHNICAL	Technology mainly refers to tools that may be used to support communication between the different actors involved in interagency cooperation.
HUMAN	Human aspects of interagency cooperation mainly refer to trends and local procedures that would constitute the basis to build an effective joint strategy.
ORGANISATIONAL	Many of the modules are relate to organisational factors. In particular, creating effective global strategy, involving several international actors, as well as creating general awareness and adopting best practice techniques by incorporating positive experiences from previous situations.
REGULATORY	Regulatory factors play a fundamental role in the interagency cooperation at international level. Participant must gain understanding of laws pertaining to Security Policy, International directives and cooperation protocols. Additionally, statutes, regulations and case law affecting the international security framework more widely are included.

3. Stakeholders perspective

A summary of all end-user engagement activities identified the following research topics (areas of priority or particular challenge):

3.1. *Enhancing awareness on Security policies*

Introduction to Transnational Crime, Terrorism, and Insurgency, Governance, State Weakness, and Human Security; definition of main International relations theories; identification of global, national and human security trends; national and international efforts to promote peace and security; Identification of international law and international relations already implemented; analysis of UN system of collective security, as well as European and international security strategies; introduction to peacekeeping and peacebuilding; discussion on governance, security and development extra-UE countries; differences between Global Strategy and Regional Issues.

3.2. *Cooperation and information exchange*

Public / private and inter-agency: Identification of the legal framework and mechanisms to incentivise and secure cooperation between private and public sector to improve resilience of all stakeholders; establishment of trust and cooperation that synthesises the protection of citizens; create, support and maintain partnerships across sectors, jurisdictions and boundaries for more efficient information sharing and to overcome jurisdictional issues; establishment of robust communication lines and contact points between public and private sector; fostering the environment of shared responsibility and trust; interagency bodies at an International

level; enhancing the capability of responders on information sharing and communication among different agencies; improvement of information requesting processes between LEAs both nationally and internationally; strong understanding of legal issues associated with interagency cooperation; assessment of the information-sharing ecosystem in order to analyse the complexities of the actors, requirements and governance structures; sharing of threat intelligence; Key actors, roles and responsibilities across the international, regional and subregional security communities.

International Cooperation: Establishment of political agreements that frame and cover the work of agencies all over the world; Understanding of legal differences and international cooperation approach; specifically a priority for cooperation between international intelligence agencies regarding security issues; assessment of different international approaches including legislation and policy towards harmonisation of existing methods, especially between member states and EU agencies; need to minimise the impact on LEAs due to geographical jurisdiction, which disempowers responders; identification of key stakeholders; networking and sharing of best practices between countries; empowerment of collaboration/centres of excellence; clarification of international bodies' role as facilitators of improved cooperation as well as of mechanisms that are currently being undertaken, and could be realistically undertaken in the future by organisations such as EUROPOL and Interpol to foster improvement in this areas. Enhancement of Centres of excellence; Create, support and maintain partnerships across sectors, jurisdictions and boundaries, for more efficient information sharing and to overcome jurisdictional issues; sharing threat intelligence

3.3. International legislative system

Establishment of bilateral/trilateral agreements; Arm control and non-proliferation treaties; Public health and environment regulations; International treaties to fight Terrorism and Organized crime; endorsement of law compatibility in establishing international inclusion; improvement of trans-border access to relevant information. Identify main requirements for policy and legislation to integrate the current framework and mechanisms into practice. Preliminary assessment for the harmonisation of the application of laws across member states; improving the availability of specialist legal expertise; fostering international cooperation, with specific regard to national and international policing and security strategies.

Data protection and confidential information: identifying and implementing the balance between the right to confidentiality and LEAs requirements for data sharing in order to improve investigation effectiveness; consideration on data protection in information sharing mechanisms, the integration of international approaches and the balance between protecting the confidentiality of data and meeting the information sharing requirements of LEAs; establishment of international best practices based on the assessment of existing international approaches.

3.4. Awareness, education and training

Organization of conferences/forums to allow decision makers in discussing emerging issues; identification of clear frameworks, training activities, financing opportunities and prioritization at international, national and policy levels for cooperation; correct training programme for responders at high level; joint educational activities; produce policy-relevant research on international security problems; deep understanding of the global emerging security issues; increasing the awareness and education of stakeholders; increasing education and awareness not only in a public environment, but also across private sector organisations; increasing awareness of reporting procedures to support cooperation at all levels, from

citizens, to large private-sector organisation; standardisation and accreditation of training for LEA members, judicial experts, the private sector and citizens; identification of clear education an awareness requirements and objectives that can be identified as part of government strategies.

3.5. *Technological evolution*

Development of platform for information sharing; assessment on the impact of technology in the suitability and applicability of laws, especially consideration of privacy and data protection; ensuring public confidence in data and information sharing mechanisms and the impact of technological advancements on public data protection requirements; development and/or improvement of tools and methods to increase the information sharing between international security actors;

3.6. *SUMMARY - Stakeholders' perspective*

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<p>Implementation of tools to foster information sharing is considered relevant; Development of technological means to enhance communication between relevant actors/institutions involved to deal with the same issues.</p> <p>Technological evolution involves both risks and benefits; Security considerations on transmission of information are necessary.</p>
HUMAN	<p>Humans represent a key factor to enhance cooperation among agencies; Cooperation and information exchange requires trust to be established between institutions and people; The roles and responsibilities of individuals needs to be ascertained as well as improved governance of practices is required; both the nature and behaviour of delegates and responders must be accounted for.</p> <p>Awareness raising and education represents one of the most important pillar to support the process. All stakeholders should be aware of benefits from cooperation aiming at increasing resilience at all levels.</p>
ORGANISATIONAL	<p>Enhance communication procedures and information sharing through a more vstructured reporting mechanisms, including a clear and harmonised classification of concepts and assessment and evolution of policies.</p> <p>Avoid that cultures within organisations would form barriers to effective cooperation. Roles of main international actors need to be assessed to provide all the agencies with a clear framework. The organized cooperation between international institutions is a significant factor to be assessed. Organisations need to review their networks and data streams and develop strategies for their analysis and protection. Organisations bear a responsibility to train and raise awareness among employees and to set and maintain standards so that a culture of awareness can be established.</p>
REGULATORY	<p>The legal implications arising from cooperation and information exchange need to be considered; Differences in legislation and policy prevent effective cooperation. Data protection, classified information, and internal restrictions are the most relevant aspects. Policies for classifying documents also need to be reviewed to prevent delay or blocking access to information. Removal of jurisdictional barriers. Development and implementation of policies specifically related to cooperation and information sharing.</p>

4. Background

4.1. Current Research

- The RAND Corporation is a research organization that develops solutions to public policy challenges to strengthen public policy through research and analysis. RAND research on Security Cooperation have provides policymakers with essential information on how best to forge new defense cooperation agreements and strengthen old alliances to counter emerging security threats.
- The paper “Walking Point for Peace: An Irish view on the state of UN peacekeeping, Center On International Cooperation” describes an example on how *...the International cooperation is ever more necessary in meeting the security challenges. The International Cooperation is fundamental to enhance international responses to conflict, insecurity, and scarcity through applied research and direct engagement with multilateral institutions and the wider policy community.*
- The paper “*Engagement on Development and Security: New Actors, New Debates*” underlines the essentiality of multilateral effort among countries to deal with emergencies and security challenges. Organization of international response around early support to economic recovery, livelihoods, and services. Bilateral and multilateral agreement to manage core political, security, economic, and humanitarian issues.
- The paper “*A New Form of Security Cooperation and Collective Conflict Management in the Post Cold War International System*” analyses new forms of security cooperation necessary to deal with post-cold war emerging threats, such as nation-state intervention, regional organizations, international agencies and non-governmental organizations involvement.
- The paper “*Parliaments and European Security Policy: Mapping the Parliamentary Field*” analyses the central importance of the European parliament to ensure the democratic quality of European Security and Defence Policy (ESDP). It underlines that although national parliaments are of central importance due to the intergovernmental nature of decision-making, both international cooperation among executive actors and military integration represent an added value to aspire. For instance, the European Parliament and various forms of inter-parliamentary cooperation complement the work of member state parliaments.

4.2. Reports

- The final report on “EU Justice and Home Affairs Agencies’ cooperation in 2016” highlights that Justice and Home Affairs (JHA) Agencies, working with their network partners, should step up cooperation to identify opportunities where their specialization can be put to further use to support the implementation of EU policies in a timely and effective manner. They should increase their efforts to share and utilise each other’s tools and promote each other’s work to raise awareness of common issues across respective mandates, making every effort to share relevant information with each other. Developing specialist networks of expertise, can be an asset to increase specialist knowledge and operational work.
- The “*Second Report from the Commission to the European Parliament, the European Council and the Council on the operationalisation of the European Border and Coast Guard*” underlines that protecting the external borders of the European

Union is one of the key pillars of the comprehensive European policy on migration. In this regard, the European Border and Coast Guard follows the concept and principles of integrated border management and brings together a robust European border agency with the border guard authorities of the Member States. The report also states that this joint investment and engagement in ensuring the European border agency becomes fully operational as quickly as possible is a practical expression of the commitment of Member States to share responsibility and demonstrate solidarity in the common interest.

- Inter-Agency Security Management Network (IASMN) provides several reports of its annual meetings, pertaining to the entire United Nations security management system. Each report makes an update on the network review on existing and proposed policies, procedures and practices of the United Nations Security Management System.

4.3. SUMMARY - Background

CURRENT RESEARCH	
TECHNICAL	
HUMAN	Responses to conflict, insecurity, and scarcity through applied research and direct engagement with multilateral institutions. New forms of security cooperation necessary to deal with emerging threats, such as nation-state intervention, regional organizations, international agencies and non-governmental organizations involvement.
ORGANISATIONAL	Essentiality of multilateral effort among countries to deal with emergencies and security challenges. Bilateral and multilateral agreement to manage core political, security, economic, and humanitarian issues.
REGULATORY	Central importance of the European parliament to ensure the democratic quality of European Security and Defence Policy (ESDP).

REPORTS	
TECHNICAL	To increase common efforts in sharing and utilising each other's tools and promote each other's work to raise awareness of common issues across respective mandates, making every effort to share relevant information with each other.
HUMAN	Developing specialist networks of expertise, can be an asset to increase specialist knowledge and operational work.
ORGANISATIONAL	Joint investments and engagements of Member States in ensuring the activation of a European border agencies represents a practical expression of the commitment of Member States to share responsibility and demonstrate solidarity in the common interest of security.
REGULATORY	Cooperation to identify opportunities where their specialization can be put to further use to support the implementation of EU policies in a timely and effective manner.

5. Current Policies

5.1. Government & Institutions

- European Neighbourhood Policy (ENP) to foster stabilisation, security and prosperity, in line with the Global Strategy for the European Union's Foreign and Security Policy. The implementation of the ENP is a joint endeavor that requires action on both sides, by neighbours and by the EU in order to build more effective partnerships in political, socio-economic and security terms.
- According to the Global Strategy for the European Union's Foreign and Security Policy, it is fundamental to promote the prosperity and safeguard democracies. Strengthening security and defence policy in full compliance with human rights and the rule of law, the main purpose is to translate each commitment to mutual assistance and solidarity into action, and contribute more to Europe's collective security through tailored lines of action.
- The European Security Strategy consists of a high-level briefing to examine the impact of changes in the security environment of Europe. It argues in favour of an ambitious new security strategy, describing the massive changes in Europe's Security environment since 2003, mapping new threats and the changing nature of the conflict.
- According to all the EU institutions, the European Agenda on Security requires an effective and coordinated response at European level. While respecting national responsibilities for upholding the law and safeguarding internal security, all relevant EU and national actors need to work together to tackle cross-border threats, aspiring to implement an EU area of internal security where individuals are protected in full compliance with fundamental rights. The Agenda aims to drive better information exchange, increased operational cooperation and mutual trust, drawing on the full range of EU policies and tools.

5.2. Industry

- Both the U.S. and EU promote a multi-layered strategy to combat terrorism and enhance security. The U.S.-European Collaboration on Security Standardization Systems aims at coordinating with partner nations to identify viable areas for cooperation and partnering; developing strategic priorities with other Federal agencies in support of the homeland security mission; matching U.S. entities engaged in homeland security research with foreign counterparts so that they may partner in cooperative research activities; engaging international partners to participate in the DHS Centers of Excellence program and encouraging U.S. institutions to partner with academic institutions abroad; cooperating with partner nations on development and implementation of standards for key areas such as border security and supply chain security.
- European Standards offer an accessible and affordable means for businesses to comply with relevant European legislation. By making the correct use of harmonized standards, businesses and other organizations can ensure that they comply with the requirements of EU Directives, for example with regard to the safety of a particular product or service. Institution such as CEN-CENELEC support standards development through a process of collaboration among stakeholders in which those are approved and published by recognized standardization bodies. Regulations and other types of legislation are adopted by

governments at national or regional level, or by supranational and/or inter-governmental organizations such as the European Union.

5.3. *Law Enforcement*

- Europol Strategy aim at reinforcing Europol as a trusted partner of law enforcement authorities, strengthening criminal information sharing and cooperation as the European criminal information hub and realising its role as a principal provider of operational support and expertise to Member States (MS) investigations. The new strategy laid EUROPOL to one based on full-scale delivery of operational service and impact, focusing its effort on consolidating all its capabilities and expertise to deliver the most effective support to MS investigations.
- The inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area represents a fundamental point to the EU Directorate General for Internal Policies. Complementarity, consistency and a good articulation between the different EU agencies and bodies (i.e. Europol, Eurojust, the European Judicial Network, the European Anti-Fraud Office and the future European Public Prosecutor’s Office) are crucial to establish an area of Freedom, Security and Justice (AFSJ) that has a multidisciplinary approach to crime. Main recommendations include not only proposals to improve bilateral relations, but also proposals of a cross-cutting nature, addressing political and operational concerns.
- Transnational crime can only be countered by cross-border cooperation, with police, customs, border guards and other authorities working together. There has already been considerable progress in implementing training on cross-border matters in the EU. For instance, more than 300 exchange programmes between law enforcement officers across the EU were organized, while new learning methods, such as CEPOL’s “webinars” were used by more than 3000 participants in 2012. Participation in EU training is growing, with more than 5000 enrolled at CEPOL and 3000 at Frontex last year. According to that, the European Commission’ Communication proposes a European Law Enforcement Training Scheme to equip law enforcement officers with the knowledge and skills they need to prevent and combat cross-border crime effectively through efficient cooperation with their EU colleagues. (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions)

5.4. *SUMMARY – Current policies*

Government & Institutions	
TECHNICAL	
HUMAN	The implementation of the European Neighbourhood Policy is a joint endeavor that requires action by neighbours and by the EU in order to build more effective partnerships in political, socio-economic and security terms. To promote the prosperity and safeguard democracies. New security strategies, describing the massive changes in Europe’s Security environment since 2003, mapping new threats and the changing nature of the conflict.
ORGANISATIONAL	While respecting national responsibilities for upholding the law and safeguarding internal security, all relevant EU and national actors need to

	work together to tackle cross-border threats, aspiring to implement an EU area of internal security where individuals are protected in full compliance with fundamental rights. To implement a multi-layered strategy to combat terrorism and enhance security.
REGULATORY	To foster stabilisation, security and prosperity, in line with the Global Strategy for the European Union's Foreign and Security Policy. Strengthening security and defence policy in full compliance with human rights and the rule of law, to contribute more to Europe's collective security through tailored lines of action. The European Agenda on Security aims to drive better information exchange, increased operational cooperation and mutual trust, drawing on the full range of EU policies and tools.

INDUSTRY	
TECHNICAL	
HUMAN	Institution such as CEN-CENELEC support standards development through a process of collaboration among stakeholders in which those are approved and published by recognized standardization bodies.
ORGANISATIONAL	Support initiatives such as U.S.-EU Collaboration on Security Standardization Systems to foster coordination between partner nations to identify viable areas for cooperation and partnering.
REGULATORY	European Standards offer an accessible and affordable means for businesses to comply with relevant European legislation. Regulations and other types of legislation are adopted by governments at national or regional level, or by supranational and/or inter-governmental organizations such as the European Union.

LEAs	
TECHNICAL	
HUMAN	Strengthening criminal information sharing and cooperation. Main recommendations include not only proposals to improve bilateral relations, but also proposals of a cross-cutting nature, addressing political and operational concerns. Transnational crime can only be countered by cross-border cooperation, with police, customs, border guards and other authorities working together.
ORGANISATIONAL	Europol Strategy aim at reinforcing Europol as the principal provider of operational support and expertise to Member States (MS) investigations. Complementarity, consistency and a good articulation between the different EU agencies and bodies are crucial to establish an area of Freedom, Security and Justice (AFSJ) that has a multidisciplinary approach to crime. Make progress to implement training on cross-border matters in the EU. Establishment of a European Law Enforcement Training Scheme to equip law enforcement officers with the knowledge and skills they need to prevent and combat cross-border crime effectively through efficient cooperation with their EU colleagues.
REGULATORY	

6. Current Practice

6.1. Europe

- Euro Lex provides EU Communications on Police and customs cooperation, including joint investigation teams; exchange of information between EU police and customs; international conventions; and the European Union Agency for Law Enforcement Cooperation's role and responsibilities.
- EMSA provides a list of current agreements and partnerships at the European level.
- The Organization for Security and Co-operation in Europe (OSCE) delivers research and analysis on several topics mainly related to Security and cooperation to provide the security community with relevant contents and useful insight on the matter.

6.2. International

- UNICRI fosters the Public-Private Partnerships (PPPs) for the protection of vulnerable targets against terrorist attacks. The need to increase promising partnership with the private sector has been outlined, requiring both to align private sector incentives with engaging in counter-terrorism strategies and adopting guidelines and mechanisms to make such a form of partnership possible and effective.
- The International Permanent Observatory on Security during Major Events (IPO) is a clear example of security cooperation in which relevant experts shared their knowledge about security issues to assist national authorities in dealing with emerging challenges. As the main result of this process, the IPO Security Planning Model is a tool available to public bodies responsible for, or otherwise involved in, planning the provision of security at a major event. The document is grounded on international experience and best practice gathered and collated by UNICRI.

6.3. National

Spain

- The Spanish National Security Strategy reflects the risks and threats that need to be addressed in a world undergoing profound and constant change. It takes a broad view of the concept of security, in accordance with these global changes which affect the State and citizens' daily lives. According to the National Strategy: *"Global challenges and threats must be addressed with global solutions developed in an international community where cooperation and multilateral action are established as basic organisational principles. In this sense, the UN continues to be the lead organisation for peace keeping and worldwide cooperation and international security"*. Moreover, *"Both national and multilateral cooperation are required to respond to the risks and threats which compromise security in this day and age. Unilateral and isolated responses, as they are incomplete and partial, are not effective against challenges which require a multidisciplinary approach and joint action."*

Italy

- The Italian White Paper for International Security and Defence intends to set short-to-medium term objectives, criteria and actions, providing the country with

an updated defence capacity able to safeguard the national interests in cooperation with all the other national and international instruments. Close cooperation between the Defence and industry, as well as universities and research centres, at both national and international level, will be the keystone of future action, hopefully also in view of the European integration process. With regards to cooperation between the institutions, it appears necessary to investigate how to improve communication with regional and local authorities as well as with international bodies involved in the Security domain.

6.4. SUMMARY – Current practice

EUROPEAN	
TECHNOLOGY	
HUMAN	Joint investigation teams; exchange of information between EU police and customs; international conventions; and the European Union Agency for Law Enforcement Cooperation' s role and responsibilities.
ORGANISATIONAL	Research and analysis related to Security and cooperation to provide the security community with relevant contents and useful insight.
REGULATORY	List of current agreements and partnerships at the European level.

INTERNATIONAL	
TECHNOLOGY	
HUMAN	Relevant experts to share their knowledge about security issues to assist national authorities in dealing with emerging challenges.
ORGANISATIONAL	Public-Private Partnerships (PPPs) for the protection of vulnerable targets against terrorist attacks. The IPO Security Planning Model is a tool available to public bodies responsible for, or otherwise involved in, planning the provision of security at a major event.
REGULATORY	To align private sector incentives with engaging in counter-terrorism strategies and adopting guidelines and mechanisms to make such a form of partnership possible and effective.

NATIONAL	
TECHNOLOGY	
HUMAN	Both national and multilateral cooperation are required to respond to the risks and threats which compromise security in this day and age. Unilateral and isolated responses, as they are incomplete and partial, are not effective against challenges which require a multidisciplinary approach and joint action. Investigate how to improve communication with regional and local authorities as well as with international bodies involved in the Security domain.
ORGANISATIONAL	Global challenges and threats must be addressed with global solutions developed in an international community where cooperation and

	<p>multilateral action are established as basic organisational principles. The UN continues to be the lead organisation for peace keeping and worldwide cooperation and international security. Close cooperation between the Defence and industry, as well as universities and research centres, at both national and international level.</p>
REGULATORY	

7. 'THOR' Summary

TECHNICAL	<p>Technical/technological considerations should be understood in terms of:</p> <ul style="list-style-type: none"> • Tools that may be used to support communication between the different actors involved in interagency cooperation. • Implementation of tools to foster information sharing. • Risks and benefits related to technological evolution. • Security considerations on transmission of information. • Increasing common efforts in sharing and utilising each other's tools and promoting each other's work to raise awareness. • Interoperability issues
HUMAN	<p>Human factors play a fundamental role in cooperation between different actors, primary regarding to trends and local procedures that would constitute the basis to build an effective joint strategy.</p> <p>Humans represent a key factor to enhance cooperation among agencies since cooperation and information exchange requires trust to be established between institutions and people.</p> <p>The roles and responsibilities of individuals needs to be ascertained as well as improved governance of practices is required. In this regard, both the nature and behavior of delegates and responders must be accounted for.</p> <p>All stakeholders should be aware of benefits from cooperation aiming at increasing resilience at all levels.</p> <p>New forms of security cooperation are necessary to deal with emerging threats, such as nation-state intervention, regional organizations, international agencies and non-governmental organizations involvement.</p> <p>Developing specialist networks of expertise can be an asset to increase specialist knowledge and operational work as well as to assist national authorities in dealing with emerging challenges.</p>
ORGANISATIONAL	<p>Organisational considerations should be understood in terms of:</p> <ul style="list-style-type: none"> • Enhanced communication procedures and information sharing through a more structured reporting mechanisms, including a clear and harmonized classification of concepts and assessment and evolution of policies. • Roles of main international actors need to be assessed to provide all the agencies with a clear framework. • Review of networks and data streams to develop strategies for

	<p>analysis and protection.</p> <ul style="list-style-type: none"> • Roles of responsibility to train and raise awareness among employees and to set and maintain standards so that a culture of awareness can be established. • Multilateral effort among countries to deal with emergencies and security challenges. • Joint investments and engagements of Member States in ensuring the activation of a European border agencies. • Implement a multi-layered strategy to combat terrorism and enhance security. • Respect national responsibilities for upholding the law and safeguarding internal security. • Need of EU and national actors to work together to tackle cross-border threats, aspiring to implement an EU area of internal security where individuals are protected in full compliance with fundamental rights. • Support initiatives on Security Standardization Systems to foster coordination between partner nations to identify viable areas for cooperation and partnering. • Reinforcing Europol as the principal provider of operational support and expertise to Member States (MS) investigations. • Make progress to implement training on cross-border matters in the EU. Establishment of a European Law Enforcement Training Scheme to equip law enforcement officers with the knowledge and skills they need to prevent and combat cross-border crime effectively through efficient cooperation with their EU colleagues. • Establishment of Public-Private Partnerships (PPPs) for the protection of vulnerable targets against terrorist attacks. • Global challenges and threats to be addressed with global solutions developed in an international community where cooperation and multilateral action are established as basic organisational principles.
<p>REGULATORY</p>	<p>Regulatory factors play a fundamental role in the interagency cooperation at international level and in particular:</p> <ul style="list-style-type: none"> • Security Policy, International directives and cooperation protocols and agreements to enable police/agencies cooperation, safeguarding rights, and ensuring standards. • Differences in legislation and policy that may limit effective cooperation. • Policies for classifying documents that need to be reviewed to prevent delay or blocking access to information. • Development and implementation of policies specifically related to cooperation and information sharing. • International Cooperation as fundamental action to identify opportunities where specialization can contribute to support the implementation of EU policies in a timely and effective manner. • Fostering of stabilisation, security and prosperity, in line with the Global Strategy for the European Union's Foreign and Security Policy as well as strengthening security and defence policy in full compliance with human rights and the rule of law, to contribute

	<p>more to Europe's collective security through tailored lines of action.</p> <ul style="list-style-type: none">• Alignment of private sector incentives with engaging in counter-terrorism strategies and adoption of guidelines and mechanisms to make such a form of partnership possible and effective.
--	---

Annex 4

PUBLIC SAFETY

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 Public Safety Management Module

Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 public Safety Management Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V04
Date:	
Authors:	RSM
Document description:	Desk based analysis carried out by DLC and RSM

1. Module Descriptor

Module Name	Public Safety challenges Management
Module Aim	The module integrates knowledge from various disciplines with a focus on how public and private organisations can respond to the opportunities and challenges offered by safety and security. It brings together history, sociology, politics, international development and crisis management as a foundation for a better understanding of the governance of public safety. The focus is specifically on public policy-making, enhanced commitment of the private sector and the broader implications of safety and security.
Learning Outcomes	
LO1	Understand the issues and problems faced by leaders in the public and private sectors.
LO2	Understanding the context of change public safety management in various disciplines.
LO3	Applying new knowledge how public and private organisations can respond to the opportunities and challenges offered by safety and security
Indicative Content	<p>The management of government and other public organisations is subject to increasingly high demands. A changing society confronts the government with new challenges to which it must respond and new conditions it has to meet. We define different roles for the concepts of security architecture and of security auspices and providers. The first role is only public while the others are mixing public and private bodies. The challenge is to articulate these roles. Finding answers in terms of policy and fulfilling the conditions in terms of democracy, effectiveness and efficiency test the internal performance of public organisations, particularly their management. To successfully complete its tasks, management has to integrate the various aspects of performance and ensure that work is carried out in a professional manner. Consequently, there is a growing need for multidisciplinary managers. The module Public Safety Management offers a multidisciplinary, analytical and creative approach to the issues and problems faced by managers in the public and private sectors.</p> <p>The module provides a forum of students and other security executives whose combined expertise will be utilized in a synergistic manner in developing, organizing, assimilating, and sharing knowledge within security disciplines for the ultimate purpose of enhancing professional and business standards.</p>

In this document we have listed the learning outcomes and indicative content of Public Safety Management, using the ‘THOR’ framework and a simple module descriptor outlining key learning outcomes. Another task within WP2 is the Stakeholder validation.

This module is closely related with the topics Change Management and Co-creation & Crowdsourcing. The last two have to be seen as the management part of the course while public safety, organized crime as well as cybercrime and terrorism are relevant to what may be called threat assessment. Because the threat assessment refers to the wide scope of security, the Public Safety Management block will include a comprehensive approach of the security field. This gives a leadership dimension that encompasses the assessment and response to more specific threats.

2. Master programmes

2.1. Current courses

- MSc Criminal Justice (Rochester Institute of Technology USA)
<http://www.rit.edu/programs/criminal-justice-ms>
The master of science degree in criminal justice emphasizes a multidisciplinary approach to urban studies with a focus on public safety. The program stresses training in policy analysis and practice, particularly as it is relevant to community and urban issues. The program builds on a foundation of locally relevant policy research by providing students with the critical skills to carry out such work and the experience to assure success in employment or in pursuit of further graduate studies. The program provides students with a strong foundation in criminological, criminal justice theory, and social scientific research skills, thus enabling graduates to have successful careers in the policy analysis arena or to be prepared to pursue advanced study beyond the master's degree.
- MSc Crisis and Security Management (Leiden University)
<https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management>
During this multidisciplinary master's programme students become familiar with the political and social dimensions of the governance of (in)security and crisis. The students study contemporary security challenges from both local and global points of view and gain deep understanding of the 'wicked problem' of security and crisis topics in a complex and globalising world. The combination of theory, practical insights and analytical skills prepares students for work in public or private organisations.
- MSc Crime, Violence and Prevention (London Metropolitan University)
<http://www.londonmet.ac.uk/courses/postgraduate/crime-violence-and-prevention---msc/>
The master's course encourages students to look critically at public protection, a key practitioner concept for professionals working in socially responsible professions. There is a special emphasis on gaining a sound grasp of the relevant academic literature, including substantial use of key scholarly journals in the field of criminology and criminal justice. There is also a focus on how theory relates to and enhances good practice. The course provides academic context to understand and evaluate the complexity of, and reciprocity between, varied agencies, departments and policies related to crime, criminology and criminal justice.
- MSc Advanced Policing Studies (Liverpool John Moores University)
<https://www.ljmu.ac.uk/study/courses/postgraduates/advanced-policing-studies>
Advanced Policing programme develops the skills increasingly required by forces as policing moves further towards an evidence-based approach. The programme addresses the quantitative research skills gap identified in policing. This course is for serving officers and those about to embark on their policing or academic career. It will learn evidence-based learning skills.
- MSc International and Transnational Policing (Liverpool John Moores University)
<https://www.ljmu.ac.uk/study/courses/postgraduates/international-and-transnational-policing>
The International and Transnational Policing MSc looks at the implications of policing across geographical and political boundaries. Students discover how policing is carried out across geographical boundaries and explore policing issues arising from differing jurisdictions, policies and procedures.
- MSc (Universiteit van Twente) – Public Management

www.utwente.nl/en/education/master/programmes/public-management

This programme for professionals is a part-time study for those who have a career in Public Management and has completed a higher education study. The degree programme addresses a crucial aspect of public management with such themes as organisational management, financial management and policy management, the second year Information management, human resources management, politics and management

- MSc (Erasmus Universiteit Rotterdam) Int. Public Management and Policy
www.eur.nl/english/master/programmes/international_public_management_and_policy
Public policy has gone international: organisations such as the EU and the UN are growing in importance. Master the theories, concepts and skills you need to work effectively in this time of increasing internationalisation; tackle global issues such as international conflict, poverty, migration, environmental protection and corruption.
- MSc (Erasmus Universiteit Rotterdam) Governance of migration and diversity
https://www.eur.nl/english/master/programmes/public_administration/governance_migration_diversity/
This specialisation focuses on migration and diversity as challenges in politics, policies and organisations. This includes but is not limited to understanding the development of migration and migrant incorporation policies per se. Migration and diversity have become highly politicized issues that play a much broader role in contemporary politics in many countries. Furthermore, migration and diversity are topic that are highly debated in media, which can have a broader impact on policy and politics as well. A key issue in the Public Administration-track of the 'Governance of Migration and Diversity' master is how broader development of welfare state regimes affect issues of migration and diversity. This programme will provide students a better understanding of what policies can be developed towards migration and diversity, how and why specific policies have been developed in cities and countries across the world, and what role migration and diversity play in broader political debates, media portrayals and welfare state regimes.
- MSc (Universiteit van Utrecht) Global Criminology
www.uu.nl/masters/en/global-criminolog
Old and new forms of global crime are rapidly expanding, as are the means to control it. The Netherlands serves both as a major crossroad in the illegal flow of goods, people and services and as a key host for international organisations such as Europol, Greenpeace and the International Criminal Court. Drug trafficking, human trafficking, international terrorism, corruption, environmental harm, financial and corporate crime and conflicts over natural resources all have global dimensions. Tackling these issues requires modern instruments that transcend national boundaries.
- MSc (Universiteit van Leiden) Global conflict in Modern Era
<http://www.mastersinleiden.nl/programmes/global-conflict-in-the-modern-era/en/programme>

In the Global Conflict in the Modern Era master programme students will explore the patterns of war and peace in the modern world from a multidisciplinary angle, incorporating history, political and social science and area expertise. The programme examines the core concepts and dominant approaches to the study of war, as well as more recent and critical takes on these phenomena. Students also study the theoretical and empirical explanations for war and peace that have been offered by the academic scholarship

- BS in security management John Jay college of criminal Justice

<http://www.jjay.cuny.edu/security-management-bs>

The major in Security Management concentrates on the analysis of security vulnerabilities and the administration of programs designed to reduce losses in public institutions and private corporations. The program prepares students for careers as managers, consultants and entrepreneurs

- MSc in protection management John Jay college of criminal Justice

<http://www.jjay.cuny.edu/master-science-protection-management>

The Master of Science in Protection Management Program provides advanced professional education in theory, design, management and operation of fire and security protection, and emergency management systems. Programs and procedures, and their practical application, are explored in a variety of public, commercial and residential settings.

2.2. *Main topics outlined (Master programmes and Professional courses):*

- Multi-level focus: dealing with public management and public policy on the national, EU and international levels.
- Risk analysis including security vulnerabilities and exposures and the administration of programs designed to reduce harm in public institutions and losses in private corporations
- Theory, practical insights and analytical skills of security and crisis topics
- Multi-disciplinary approach: organization of law enforcement practitioners, educators, researchers, private security specialists, technology experts and other professionals dedicated to improving criminal and social justice through the professionalization of policing and security

2.3. *SUMMARY – Current courses*

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • Policy analysis and practice • Criminological skills • Criminal justice theory • Risk and strategic analysis • Theory, practical insights and analytical skills of security and crisis topics • The quantitative research skills gap identified in policing • Information management • Theory, design, management and operation of security protection

	and emergency management systems.
HUMAN	<ul style="list-style-type: none"> • Community and urban issues • Implications of policing across geographical and political boundaries • Deviance and criminology • Human resources management
ORGANISATIONAL	<ul style="list-style-type: none"> • Social scientific research skills • Internationalization: Impact of global issues such as international conflict, poverty, migration, environmental protection and corruption • Prevention and response • Multidisciplinary approach • Contemporary security challenges • Local and global crime • Public protection • How theory relates to and enhances good practice. • Organisational management, • Financial management • Policy management • Politics and management • Migration and diversity as challenges in politics, policies and organisations • Public administration • Governance of migration and diversity • Modern instruments that transcend national boundaries • Core concepts and dominant approaches to the study of war
REGULATORY	<ul style="list-style-type: none"> • Political and social dimensions of the governance of (in)security and crisis • Understand and evaluate the complexity of, and reciprocity between, varied agencies, departments and policies related to crime, criminology and criminal justice. • Explore policing issues arising from differing jurisdictions, policies and procedures

3. Stakeholders perspective

3.1. Stakeholder perspective general

Exposure of interest is the risk for many stakeholders. Security will be increased when exposure of the interest is reduced. But there is always a tension between the interest (business/profits) and the security of the interest: on one hand it can facilitates movement, but at the same time security of the interest demands low profiling. Security is the balance between facilitations and low exposure, the balance between prevention and response with voluntary strategies; delay repression to get time to adjust response: prevention can delay but cannot fully stop threat.

With respects to stakeholders, the division between public and private should comprise the division between auspices and providers.⁵ Indeed stakeholders have also to be seen between auspices who are in charge of security and have an interest to protect and the providers who are delivering the necessary services to ensure this protection.

The latter are working on behalf of the former who defines missions, resources and style. However, the providers remain responsible about deployment of techniques and tactics to use with respect to the instructions and procedures of the auspices. This search for the right balance is the challenge both stakeholders need to face with authorities that desires to manage on a micro level and provider who could try to influence, or even manipulate in order to control their mission.

This duality has to be kept in mind with the following four roles. This will be done according to the usual threats to be found in the field of public safety. Additionally a specific attention should be given to the citizen. As an individual he can be a private auspice for himself and a private provider for himself and others. As a taxpayer and an elector he is a public auspice.

Most individual factors in the scope of public safety have limited impact and produce minor consequences. However their repetition can have a broader impact and produce heavy consequences because they carry on the assumption according to which everyone can be hit. In that case any individual case becomes a social issue that has to be addressed as such.

3.2. Public safety and the field of security

Public safety is a part of the global field of security, together with public order/institutional life, organised crime and national security which differentiates public safety from other areas.

One major difference is related to threat. Public Safety concerns perpetrators with limited organization structure and therefore limited impact. These actors are commonly motivated by immediate benefits (either immaterial or material) and they operate on a random basis. However, repetition of petty offenses could become a major issue. They have no aim attacking society, neither the institutions nor the nation. This is a huge difference with organised crime, public order, terrorism, foreign interferences or other threats, which do have these specific goals.

The potential confusion is that at first glance most of organized crime activities, terrorist attacks and even some of national security aggressions, could look as a matter of public safety and addressed initially as such by the relevant public safety police agency. An example is a theft of cargo from a parked truck caused by a local thief operating randomly or caused by a network of organized crime with specific aim to target this truck to fulfill the demands of an illicit trade network. At first glance they look the same but investigation could establish the real nature of that threat.

Additionally the nature of the multidisciplinary role of the public safety police agencies that derives from their first line position has increasing that confusion. This has been the case in most European countries where resources of public safety police agencies focus mostly on terrorism and therefore abandoning some of their public safety duties, while even this focus is mostly on consequences and not on the causes of the offense committed

⁵ e.g. David H. Bayley, D.H. & Shearing, C.D. (2001). *The new structure of policing*. Washington

3.3. *Antisocial behaviour*

Antisocial behaviour (ASB) has been a key part of public safety for a long time. Initially antisocial behaviour was defined around property, compliance with social rules and religion. Therefore tramping, begging as well as some form of social unrest by working classes were seen as antisocial behaviour.

Today things have changed and antisocial behaviour covers a wide range of activities in the public space. This can be activities that are disturbing public life and activities which are perceived by citizens as harming and threatening, even if they cannot be defined as a crime. Among the most common are noisy behaviour (often linked to alcohol), drugs, gangs, garbage throwing, petty destruction, aggressive attitudes and more generally all types of petty street disorders.

Antisocial behaviour is a strong concern for the citizens and is often stressed by elected community leaders, to respond to these activities in order to stop them. In some cases, especially in Nordic countries, citizens feel entitled to interact with the badly behaving individual in order to stop the unwanted behaviour. In other countries, like USA or South America, citizens are keener to protect their properties within gated communities where they call the service of the private security industry (e.g. fences, CCTV, guards.).

ASB is a major concern for all kinds of organisations that request a peaceful and secure atmosphere, shopping, restaurant, entertainment especially when dealing with luxury services and product and with upper and middle class customers. Such companies will either stress the elected community leaders and law enforcement agencies to stop ASB in public places or they will act as auspices and look for private security industry service providers if the ASB occurs in the private space they manage.

3.4. *Violence*

Violence covers the wide range of aggressions that could target individuals from pure verbal ones to serious physical attacks including (this differs from organised crime as the latter is not a one to one action) It is bound to sociocultural features. Some societies are known as violence oriented while others are not. For example the murder rate ranges from 1,1/100 000 inhabitants in France, but with a 7/100 000 in Corsica, to 4,5/100 000 in the US and 24/100 000 in Mexico (average figures '2010-2015) or even 90/100 000 in Honduras.

Violence can be isolated from other crimes but could also be linked. This is what makes the difference between a burglary and a robbery. It is very common to use violence in combination with other crimes (trafficking of all types, property crime...). Violence can also reflect a great proximity between the aggressor and the victim. For example in France 18% of murders occurs within the family. In Switzerland this is 55%. With these figures, it is more likely for a woman to die under the attack of her partner than under a terrorist attack.

Because violence has a direct impact on the physical integrity of the individual it is a major concern for public safety. The public generally refused violence and asks (local) community leaders, to address the issue. For private companies violence, or at least a climate of violence, has a negative impact on the business either through employees or customers being threatened by violence. Therefore, private companies have also here a strong interest to reduce violence.

3.5. *Property crime*

Traditionally the protection of property is secondary to the protection of individuals. The mission of public safety -and more generally of policing- is however and very often said to protect individuals and goods.

Property is any asset that carries a certain value, either material or immaterial. Consequently any action that entails the theft of property has to be seen as a loss. It is however necessary to differentiate the different natures of loss.

With respects to individuals, loss can be both material and psychological and sometimes even highly emotional. Individuals can experience different kind of theft, from street pickpocketing to burglaries. In case of burglary, the theft becomes an aggression, a violation of privacy and intimacy. For that reason, even if the material loss is low, most victims, as well as potential victims, ask for more protection with the political leaders, law enforcement and policy makers. The people with good resources also address their sense of insecurity and need for protection to the private security services (armoured doors, captors and alarms or even security guards).

Individuals can also be victims of large-scale organised crime activities. Because these crimes are at first not seen as serial cases, but as individual cases, they are initially and improperly addressed within the framework of public safety. (E.g. burglaries, credit card frauds).

When it goes to private companies the situation is more material and less emotional. Property crime is seen first through its impact on the balance sheet. Second it is seen quite often as a factor of disruption when the stolen item is part of a process that could be at least disturbed and at worst interrupted. Such a disruption could impact the company image when it cannot deliver in time or when the stolen products are associated to street level illicit trade. Some organisations, especially those with attractive and high priced products (fast moving consumer goods: FMCG), experience more victimhood than others. Physical thefts and frauds are the most common types of property crime that impact private business. Shoplifting, employee diversion, burglary of storage facilities and theft or even sometimes robbery of cargo in transit, are the most common types of physical theft. When these property crimes are random, they belong to the field of public safety. But they can also be manifest in a more structured approach, in case we speak of organised crime.

These property crimes are seen as a financial loss. Consequently the private companies have to found solutions to reduce this loss. They can try to do it at no cost just by lobbying public authorities and law enforcement agencies. In a more preventive approach they can also make the crime more difficult. In that case they behave as security auspices and task the private security industry to provide a wide range of services: security guards for access control, CCTV in shops and storage area or truck parking, tags to ensure traceability of products.... The creativity of the security service and equipment providers has not limitation to address the diversity of needs of the private sector. It can be assumed that the bulk of the security industry is committed to the protection of private property.

The property crime introduces an additional stakeholder with the insurer. This one has to be seen as an auspice that set standards and rules for the protection of goods. The insurer is in a position to have private companies complying with these standards and rules because this compliance is a condition to benefit from the insurance and get good rates. Compliance covers not only the use of services and equipment but also the performance standards of these.

3.6. Trafficking

Trafficking consists of two levels criminal activity. The upper level is supply is: by nature an organised crime activity, mostly international that facilitates movement of huge shipments of goods and large numbers of persons over long distances and across borders.

At the lower level there is retail, a street level crime and disorder. This used to be mostly a physical appearance with pawn-shops, street dealing and suspicious places. Nowadays it is

more and more using the internet either through dedicated websites that offer trafficking products or through social media where illicit salesmen contact potential consumers.

Trafficking could be articulated around persons, illicit and licit goods.

- Trafficking of persons deals with three different types of criminal activity: sexual exploitation, forced labour and/or illegal immigration. Criminals make profit either during the transfer of persons or at the end of the process. At street level and with respects to public safety it could be prostitutes and immigrants in the street, it could be forced labourers in fields or clandestine workshops or as maids in the homes of “honourable citizens”.
- The trafficking of persons is hurting the sensibility of most citizens. If it does not receive any response this creates a feeling of insecurity because citizens experience that a serious crime is not tackled and that consequently, other crimes including those that directly harm them, will not be punished too. They will push political leaders and law enforcement agencies to do something. Similarly private companies will see a degradation of their business environment and would also stress public authorities to react.
- The trafficking of illicit goods is mainly made of drugs and weapons. In the field of public safety it has to be seen at the level of street level deal (drugs) or as a potential increase of violence in public space. Once more this is being very negatively perceived by the citizens and by the private companies that both press the public authorities to re-establish a safer public environment.
- The trafficking of licit goods and services for illicit purposes is the basis for illicit trade, a fast growing criminal activity that is passing over drugs and other illicit trafficking. WEF 2014 estimate is over 650 Bn \$ going up to 2 000 Bn \$ by including financial flows. In economic terms this would make illicit trade a G8 member. Illicit trade could come from theft, frauds, counterfeiting and contraband. It could also come from incompliance (breaking health, physical security, technical standards, environment, UN embargos) or from breaking commercial rules (contracts, practices, trademarks). Illicit trade creates grey markets. These ones could feed and mix with organised crime for large supply. At retail level it could disrupt peace and order at street level and here again citizens and business leaders will stress public authorities. In order to support their claims the private companies task private security to monitor these markets to identify illicit trade activities.
- The trafficking persons as well as of both of illicit and licit goods is now using the internet either directly on the open way or in a more discreet way by using the dark net or social media. This creates new spaces of illegality that are not easy to tackle. Public authorities are concentrating their efforts on the trafficking of persons and consequently private companies have to use the security industry to monitor the markets to identify illicit trade.

3.7. *Large scale public events*

The management of large-scale public events is seen as a major irregular but high-risk public safety duty. Such events are questioning public safety through two dimensions. The first one is to have criminal activities that could occur during such events. The scope is quite wide ranging from pickpockets, drunken disputes to looting or terrorist attacks. Crowd movements make a more serious threat with people becoming unmanageable and crushing themselves along fences or in narrow lanes. It is generally the responsibility of the organizer to take charge of public safety during such events. For what is taking place in the private space it is to the organizer to act as an auspice and to task private security to provide the necessary services (access control, CCTV, stadium stewards, setting fences, etc.). However public authorities are in a role of secondary auspices because they issue the regulations the private sector has to comply and generally oversee how these are respected. When it goes to the public space it could be split between private security and police forces. With respects to the later the private organizer could be charged with a specific fee. In any case public authorities have a specific role in terms of regulation or clearance.

3.8. *Natural and technological hazard*

To be discussed: Do we take non threats (no human action) into account? Defining public safety

3.9. *Traffic and road security*

It is very common to include traffic and road security in the public safety area. Traffic and moving on public road are part of the daily life. Any observation and common wording of what happens on the roads uses the same concepts as public safety: anti-social behaviour, violence, property crime, etc. Therefore traffic and road security can be seen a part of public safety.

Traffic and road security is important for citizens and mostly with respects to physical security issues. There have been worldwide dramatic efforts to improve road security on the roads. Over the last fifty years and despite a huge increase of the traffic the death toll has been reduced from six to one in France as an example.

For private companies the key interest is beyond the physical security of employees. It is a question of lean flows of cargo. First traffic jams can cause delays; if a truck misses an aircraft departure in Europe this can disrupt a key commercial event in Asia meaning the company can lose major business opportunities. The same can be said if the shipment is stolen on a motorway parking lot. As auspices, chartering companies as well as insurer have set in Europe a scheme of safe parking where security (guards, CCTV) is provided by the security industry.

4. Stakeholders Perspective

A key source for trends, threats and issues in public safety can be found on the websites on a few institutions that have regular publications, usually annual assessment and reports. Among them are:

- the British “her majesty’s inspectorate constabulary and fire services”
<https://www.justiceinspectors.gov.uk/hmicfrs/publications>

The purpose of these studies is to review existing knowledge of the police role in responding to crime and, on the basis of the available evidence, to propose priority areas of focus for forthcoming inspection.

- Her majesty inspectorate constabulary “public views of policing in England and Wales”
<https://www.justiceinspectors.gov.uk/hmicfrs/publications/public-views-of-policing-in-england-and-wales-201617/>

In 2015, Ipsos MORI published the results of a survey, commissioned by HMIC, into public perceptions of policing in England and Wales. In 2016, HMIC commissioned a follow up survey. This report sets out the results of this survey.

- Her majesty inspectorate constabulary “Living in fear the police and CPS response to harassment and stalking” <https://www.justiceinspectors.gov.uk/hmicfrs/publications/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking/>

In 2016/17, HMIC and HM Crown Prosecution Service Inspectorate (HMCPIS) carried out the first inspection into the police and the Crown Prosecution Service (CPS)’s response to harassment and stalking crimes. Harassment and stalking are crimes of persistence. It is the unrelenting repeat behaviour by the perpetrator experienced in its totality, which seems inescapable and inevitable, that has such a detrimental effect on the victim.

- Her majesty inspectorate constabulary “State of policing in England and Wales 2016”
<https://www.justiceinspectors.gov.uk/hmicfrs/publications/state-of-policing-the-annual-assessment-of-policing-in-england-and-wales-2016/>

This report on the efficiency and effectiveness of policing in England and Wales in respect of the inspection year 2016. This reporting period has seen the second complete cycle of PEEL (police effectiveness, efficiency and legitimacy) inspections, which consider the effectiveness and efficiency of police forces, and assess the legitimacy of how they discharge their obligations (that is, how they behave and treat people). These inspections provide a comprehensive analysis of the way in which each police force in England and Wales has performed, and will continue to do so on an annual basis.

- Her majesty inspectorate constabulary “police effectiveness 2016”.
<https://www.justiceinspectors.gov.uk/hmicfrs/publications/peel-police-effectiveness-2016/>

As part of our annual inspections of police effectiveness, efficiency and legitimacy (PEEL), HMIC assessed how effective police forces are at keeping people safe and reducing crime. This inspection focused on five areas of policing: (1) How effective are police forces at preventing crime, tackling anti-social behaviour and keeping people safe? (2) How effective are forces at investigating crime and reducing re-offending? (3) How effective are forces at protecting those who are vulnerable from harm, and supporting victims? (4) How effective are forces at tackling serious and organized crime? (5) How effective are the forces’ specialist capabilities? This report presents a national overview of themes identified in inspections of all 43 police forces in England and Wales. The national overview report is accompanied by separate reports on each force, based on inspections carried out from September to December 2016, and data provided by forces.

- Her majesty inspectorate constabulary “police legitimacy 2016”
<https://www.justiceinspectors.gov.uk/hmicfrs/publications/peel-police-legitimacy-2016/>

The inspection looked at (1) the extent to which forces treat people with fairness and respect, (2) the extent to which they ensure their workforces act ethically and lawfully; and (3) the extent to which those workforces themselves feel they have been treated with fairness and respect by the

forces. The national overview report is accompanied by separate reports on each force, based on inspections carried out from March to July 2016, and data provided by forces.

- Her majesty inspectorate constabulary “ police efficiency 2016”
<https://www.justiceinspectors.gov.uk/hmicfrs/publications/peel-police-efficiency-2016/>
The inspection examined how well forces understand the demand for their service and how well they match their resources to that demand; Also they provide an assessment of their efficiency. The national overview report is accompanied by a separate report on each force, based on inspections carried out from March to July 2016, and data provided by forces on their spending plans for future years. The efficiency reports will be followed by reports on legitimacy in December 2016 and effectiveness in early 2017, which together make up the three pillars of the annual PEEL assessment.
- The US national institute of Justice that gather all US government funded research in public safety policing : <https://www.nij.gov/Pages/welcome.aspx>
A recent NIJ-funded study found that computer learning may provide a new avenue for creating tools to identify financial exploitation among elderly adults. Researchers sought to determine if computers can “learn” how to distinguish between financial exploitation and other forms of elder abuse, including physical abuse or neglect. The research results showed that computer models were effective in identifying financial exploitation and its subtypes
- European Forum for Urban security (EFUS) : <https://efus.eu/en/>
Efus is a network of some 250 members – cities, other local elected governments and associated institutions and partners – who share a. Its common commitment to work at a European level on crime prevention and urban security policies members come from 16 countries.
- Police futurist: <http://www.policefuturists.org/>
The Society of Police Futurists International (PFI) is an organization of law enforcement practitioners, educators, researchers, private security specialists, technology experts and other professionals dedicated to improving criminal and social justice through the professionalization of policing. Futures Research (long-range planning and forecasting) is the pivotal discipline that constitutes the philosophical underpinnings of PFI. The tools and techniques of this field are applied in order to more accurately anticipate and prepare for the evolution of law enforcement ten, twenty, and even fifty years into the future. Futures Research offers both philosophical and methodological tools to analyze, forecast, and plan in ways rarely seen in policing in the past. The strength of PFI lies in the participation of it's members as they engage in dialogue and collaborate on research on the future of the policing profession.
- European association of security service enterprise : <http://www.coess.org/>
The main objective of CoESS is to represent and support the growth of an industry that delivers solutions of high quality and professionalism, focused on the selection and development of qualified staff and technology. The core values of CoESS are Quality, Safety, Compliance and Trust.
- Transnational alliance to combat illicit trade <http://www.tracit.org/>
Illicit trade has grown well beyond the capabilities of individual governments and individual companies, and now demands a sustained, coordinated response. TRACIT is a private sector initiative to mitigate the economic and social damages of illicit trade by strengthening government enforcement mechanisms and integrating supply chain controls across industry sectors most impacted by illicit trade.

TRACIT draws from industry strengths and market experience to build habits of cooperation between business, government and the diverse group of countries that have limited capacities for regulatory enforcement. Connecting and mobilizing businesses across industries, sectors and national borders makes it possible to achieve results more effectively than any single actor can accomplish alone.

- International security management association <https://isma.com/>
ISMA is a premier international security association of senior security executives from major business organizations located worldwide. ISMA's Mission is to provide and support an international forum of selected security executives whose combined expertise will be utilized in a synergistic manner in developing, organizing, assimilating, and sharing knowledge within security disciplines for the ultimate purpose of enhancing professional and business standards.
 - European Corporate security association <https://www.ecsa-eu.org/>
ECSA's Objectives are to provide its members with a trusted forum for sharing common issues, experiences, information and education. The main goal is to liaise and to promote synergy with relevant Academic, Research, Scientific, Public & Private Organizations and Associations and stimulate Public-Private Cooperation
 - Perpetuity research <https://perpetuityresearch.com/>
Perpetuity Research is a leading research company with wide expertise in both quantitative and qualitative approaches. They have been involved in evaluating 'what works' (and what does not). Their work has involved helping their clients to understand people's behaviours, perceptions and levels of awareness and in identifying important trends. Their mission statement is 'committed to making a difference', and much of the work has a practical application in terms of informing decision making and policy formulation.
- Transport Asset Protection association <http://www.tapaonline.org/>

4.1. SUMMARY - Stakeholders' perspective

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<ul style="list-style-type: none"> • Computers learn how to distinguish between financial exploitation and other forms of elder abuse • Identifying public safety offenses on the internet and in social media • Using modern technology to identify and report the commission of offenses • Information sharing • Surveillance equipment
HUMAN	<ul style="list-style-type: none"> • Review existing knowledge of the police role in responding to crime • Public perceptions of policing • Police response to harassment and stalking crimes. • Police act fair with respect • Public safety policing
ORGANISATIONAL	<ul style="list-style-type: none"> • Public safety policing • Balance between prevention and response with voluntary strategies. • Efficiency and effectiveness of policing (how effective police forces

	<p>are at keeping people safe and reducing crime)</p> <ul style="list-style-type: none"> • Police efficiency • Multi-disciplinary: common commitment to work at a European level on crime prevention and urban security policies. • Private sector initiatives to mitigate the economic and social damages of crime • Public-Private Cooperation • Organizing public (police) and private security bodies (auspices and providers) to address public safety separately from other areas of the security sector
REGULATORY	<ul style="list-style-type: none"> • Police legitimacy • Police act ethically and lawfully • Protection of privacy and personal data • Quality • Safety • Compliance and Trust • Decision making and policy formulation. • Differentiating the roles of (i) auspices that are responsible to organize the protection of persons and goods and of (ii) security providers who have to deliver the services and equipment that will ensure security • Differentiating offenses that relate to public safety from those that relate to other areas of the security sector (OC, national security, public order) • Differentiating anti-social behaviour and crime • Adjusting penal law to new type of offenses • Social and ethical engagement of companies, market driven and policy driven, taking care of security with respect to regulations and rules of law

5. Background

5.1. History

Public safety is quite often seen as policing. This was may be true at the early stage

To ensure the security of individuals and of their belongings is a social demand that is as long as mankind. In the western world it started with the medieval cities and the feudal world with local brotherhoods (mostly merchants) and local lords being entitled to organize a form of public safety within their communities.

Nevertheless a modern form of public safety emerged in big cities as soon as the seventeenth century in Paris with the first lieutenant of police. The most advanced form of public safety was defined and implemented in London by Robert Peel who was at that time minister of Interior. Even if there is some doubts about the origin of what is called “Robert Peel nine principles”, either by Robert Peel or by one of the first London police commissioners these principles that had been issued in 1829 have been the basis of public safety by emphasising the service to the citizen, by promoting the importance of prevention. The first of these

principles is very clear: *“The basic mission for which the police exist is to prevent crime and disorder.”*

Over the second part of the nineteenth century most of the western countries set up public safety police agencies mostly in towns and these were called city or municipal police to be managed under the auspices of the city mayor or council and funded by the city. Some countries used a military model of gendarmerie to ensure security in the countryside and in small cities. This was the case in southern and central Europe as well as in Latin America. In the USA the sheriff offices played a similar role.

5.2. Policing models

Until the end of the twentieth century public safety has been implemented according to two different models. The first one is called law and order while the second one is oriented on the service given to the citizen. At that time there was a clear distinction between public safety police that operates in uniform in the street and investigation or national security services that worked in plain clothes.

The law and order model of policing aims to ensure a stable social order. Therefore public safety sees the police as maintaining the established order with dominant and dominated social classes. This model has been predominant in Southern and Central Europe. Usually it emphasises the response over the prevention. With this model policemen uses to carry weapon and most of the time in a visible way to establish a hierarchy of power between the police and the citizen. This model had been present in authoritarian regimes either conservative like the Spain at the time of Franco or communist like in the Soviet block.

The service-oriented police relies on a closer relationship between the police and the public. This is reflected in Robert Peel seventh and ninth principles: *“Police, at all times, should maintain a relationship with the public that gives reality to the historic tradition that the police are the public and the public are the police”* and *“The test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with it. Unlike the law and order model the police service oriented one relies on ownership of the police by the citizen. This is reflected by the concept of “policing by consent” and by participative practices like neighbourhood watch. One could also say that the police that ensure public safety is not an instrument of the state power but a representation of the public interest, something Robert Peel said as “Police, at all times, should maintain a relationship with the public that gives reality to the historic tradition that the police are the public and the public are the police; the police being only members of the public who are paid to give full-time attention to duties which are incumbent on every citizen in the interests of community welfare and existence.”*

5.3. Organizational models

Over time the organization that are in charge of public safety have been defined along the following features: centralized versus decentralized and civilian versus military. Such features reflect not only the organizations meaning the security service providers but also the governance and consequently the security auspices.

In a decentralized model like Switzerland, Belgium, the UK the public safety is decentralized. Public safety auspices are elected local authorities, cantonal councillor in Switzerland, Mayors in Belgium, and elected commissioners in the UK. The public safety service providers are local police services, Swiss cantonal police, local police force in Belgium, county constabulary in the UK. This model is also the model that exists in Northern America.

In a centralized model like the public safety auspices are usually the ministries of Interior and at local level their representatives the so called “prefects” or Governors. Similarly the public safety security providers are national police forces. Centralized models exist in Western Europe, France, Italy but also in most of the world (Turkey, South America, Central Asia, Africa...).

The last feature is military versus civilian. This applies mainly to the level of service providers but also sometimes to the level of the auspices. It is not just a question of status; the differentiation has deeper signification. As said before a military model is linked to a law and order model of public safety. It is generally part of a centralized organization of the public safety. It also reflects the emphasis that is given to sovereignty either because the state has to control large pieces of territory or because it has to strengthen the central power. The military model was formalized by Napoleon with the gendarmerie. It has weakened over time in Western Europe where gendarmerie disappeared in many countries (Austria, Belgium, Germany...) but remains very present in South America and has even been established as a new police force in China with the armed people’s police.

More recently and for various reasons there has been a militarization of traditionally civilian public safety police organizations. This has occurred at the level of the service providers. This is translated in ranks and uniform like in France or in equipment like in the US where military surplus equipment and combat weapons are issued to local police forces.

The differentiation is not always as clear and there are very often some mixed models. This is usually the consequence of history with different organizational layers like in Spain where one can found civilian and military police forces at national level and regional and municipal civilian police forces at local level.

6. Background

6.1. Current research

- Boin, A. & ‘t Hart, P. (2017). The politics of crisis management. Public Leadership under pressure. <https://books.google.nl/books?hl=nl&lr=&id= HqJDgAAQBAJ&oi=fnd&pg=PA1&dq=public+safety+management&ots=8Qm8tzHyO7&sig=PyrjKbRlfh0hfktRWefJ6RKma0#v=onepage&q=public%20safety%20management&f=false>
- Bercovitch, J. & Lee, S. (2003) Mediating international conflicts: examining the effectiveness of directive strategies. http://www.jstor.org/stable/41852891?seq=1#page_scan_tab_contents. Interventions in international conflicts.
- Rand corporation “public safety research” <https://www.rand.org/topics/public-safety.html>
- The US national institute of Justice that gather all US government funded research in public safety policing : <https://www.nij.gov/Pages/welcome.aspx>
- CrimeSolutions.gov website www.crimesolutions.gov/ is a resource to help practitioners and policymakers understand what works in justice-related programs and practices. Research on the effectiveness of programs and practices.

6.2. Statistics

The reliability of security statistics is questionable. For a long period the figures of reported crimes have been used as indicators, the so called crime rate. Nevertheless the integrity of these figures has been challenged by different factors over the last decades. First victims can avoid to report crimes due to fear of retaliation, limited loss or unavailability of police.

Second, the police itself can refuse to register reported crimes to keep good figures. Last, new forms of crime like frauds, cybercrime are not well defined in statistical books and are either ignored or aggregated with other offenses in a sense it is difficult to have an accurate picture of the situation. Furthermore this gap between figures and reality is called the dark figure of crime and therefore of security. Such a gap exists in official public statistics as well as in private ones because even the members of professional bodies that are dedicated to security are reluctant or have no time nor resources to fill statistical forms.

Recently new methodologies have been developed to measure crime and consequently security. The first one is made by large-scale surveys; these addresses groups of several tens of thousands of persons or organizations that are asked about crimes and losses they have suffered. Another methodology that asks robust protocols is to question offenders or population of potential offenders - under condition of anonymity - about the offenses they have committed. Still in the field of statistics European police forces - unlike American ones - have never built statistics on losses (e.g. theft, frauds).

To conclude statistics have to be used very carefully; any change of conditions could biased the figures. Furthermore comparisons in different environments could be tricky.

- Global Homeland Security & Public Safety Industry, Technologies & Markets – 2017-2022.

<http://homelandsecurityresearch.com/2016/11/global-homeland-security-public-safety-industry-technologies-markets-2017-2022/>

15 years have passed since 9/11, and the global Homeland Security & Public Safety technologies and markets are forecasted to go through major shifts. Counter terror and security markets formerly dominated by the U.S. are now moving to Europe and Asia-Pacific. New and maturing counter terror technologies, such as big data & data analysis, advanced sensors, big data-based cybersecurity, video analytics and TETRA & LTE emergency communication, will create new market segments and fresh business opportunities. According to the “Global Homeland Security & Public Safety Industry, Technologies & Markets – 2017-2022” report, the market will go through a growth period, sustaining a 2016-2020 CAGR of 5.7%. This growth is driven by the following dynamics:

- The European terror and migration crisis
- The turmoil in the Arab world, the ongoing conflicts in Iraq, Syria and Yemen, and the Shia-Sunni conflict
- President Donald Trump promised, throughout his campaign, a tough fight against Islamist extremism terror at home and abroad, and to invest in physical security and counter terror
- Climate warming-related natural disasters growth
- Organized crime
- The “We Will Invest Whatever It Takes” approach of autocratic governments (e.g., China and Saudi Arabia) to avoid regime change
- Cybercrime and cyberterrorism threats

This HLS market report is a comprehensive review of the global physical security market. The objective of this counter terror market forecast is to provide a detailed, time-sensitive and reasoned intelligence analysis.

6.3. Reports

- EENA. (2016). Public Safety Answering Points – global edition.
http://www.eena.org/download.asp?item_id=217

EENA's annual publication 'PSAPs in Europe' (112 Emergency Services are handled in PSAP.) has become one of the most anticipated documents in the emergency services field. A comprehensive guide to understanding PSAP structures in different countries. This first edition includes 53 country profiles. You can find details about PSAPs' functioning, understand the complexity of the different national structures, as well as the context in which PSAPs operate. Moreover, questions about Advanced Mobile Location and drones have been added so that you get the latest information on new technologies and developments from emergency services around the world. Many case Study documents and Technical Committee publications in de annexes

6.4. SUMMARY - Background

CURRENT RESEARCH	
TECHNICAL	<ul style="list-style-type: none"> Deploying more and more technical solutions
HUMAN	<ul style="list-style-type: none"> Interventions in international conflicts. Civilian and military status for police
ORGANISATIONAL	<ul style="list-style-type: none"> Public leadership Evidence-Based Programs and Practices Effectiveness of directive strategy Differentiating the organizational competencies according to the different areas of the security sector. Balancing centralized/decentralized organisational models Public monopoly of security
REGULATORY	<ul style="list-style-type: none"> Balancing local versus national competencies.

STATISTICS	
TECHNICAL	<ul style="list-style-type: none"> intelligence analysis on counter terror forecast National Statistics on crime
HUMAN	
ORGANISATIONAL	
REGULATORY	

REPORTS	
TECHNICAL	<ul style="list-style-type: none"> Advanced Mobile Location and drones
HUMAN	
ORGANISATIONAL	<ul style="list-style-type: none"> PSAP structures in different countries
REGULATORY	

7. Current Policies

Over the last fifty years there has been dramatic changes in the field of public safety. This is the consequence of major social changes that have both asked for a new organization of the security sector and for a new style of public safety. It is necessary to grasp the whole security sector to be able to understand what is going on about public safety.

7.1. *Security sector*

The buildup of the security sector is by nature a national matter. It has been a key attribute of states from the early time along Justice when it became necessary to protect people inside the country. For that reason policies are purely national. However when it became necessary to rebuild failed states or to support the buildup of newly created states a security sector reform policy was initiated within the international community. Another exception to national competency in the security covers road safety and traffic safety. This is the case within the EU with the road safety and Tispol initiatives. Last, even if their sovereignty is respected states can be bound by international conventions.

7.2. *National policies*

Until the First World War the security sector in Western countries was quite simple. There was a public safety area with auspices and providers that were able to address almost all the security challenges of the daily life of citizens and companies. Specific needs were addressed on an ad hoc basis. Aside there was a national security service that was in charge of protecting institutions and national interest. Ultimately and for major events, emergency and crisis the public auspices could rely on the military.

Over half a century the security sector has faced dramatic changes in Western countries where it has been fully restructured. Dominique Montjardet (“Ce que fait la police”, Odile Jacob, Paris 1995) has described the new security sector on the basis of the interests that have to be protected. Consequently he differentiated different security areas that reflect different policies:

- Public safety to protect the physical life and the properties of the citizen and other private bodies
- Organised crime to protect the society against gangs that disrupt the society and the economy while intending to build a social and economic alternative (mafia threat)
- Institutions and public order to ensure a fair political and social life: political debate, elections, public expression and demonstrations (avoiding extremism and radicalism)
- National security to protect the key interest of the nation: critical infrastructure for economy and public services; border and immigration for sovereignty and national identity; intelligence for sovereignty and national independence against external interferences and terrorism.

Initially the reform of the security sector paved the way to specialised bodies. It also reinforced the centralisation of security bodies because responses in the field of organised crime, institutions and national security have demanded to be nationally centralized. For that reason decentralized countries had to create central bodies to address national security. This why in the field of organised crime the US set up the Federal Bureau of Investigation (FBI)

as early as 1908 and the UK the Serious and Organised Crime Agency (SOCA) more recently in 2006 that became later in 2013 the National Crime Agency (NCA).

For a while the four areas were separately addressed and both auspices and providers were separated and operated separately. Most of the time the security sector reform has been implemented incrementally quite often in a reactive way like the creation of the US Homeland security department in 2001 after 9/11. Sometimes a comprehensive reshaping could occur that fully reorganize the security sector as it was the case in Northern Ireland when the Royal Ulster Constabulary was transformed to become the Northern Ireland Police Service or in Belgium when all police services were merged to create the two level police service.

Over the last two decades two major constraints have pushed for integration.

- Financial constraints have limited resources available for the public security sector and it became obvious for political leaders that horizontal reinforcement should be achieved from some areas to the others when needed especially in case of crisis. This is the reason for which public safety police services are regularly committed to duties outside the public safety area. This creates some confusion for the public and for the security governance especially when decentralized and locally funded public safety services are requested by state authorities to work in public order or national security areas. This was the case when Margaret Thatcher used the police against the coal miners' strike. This is now the case in many Western countries to prevent terrorism by establishing a strong deterring police presence on the ground.
- A second factor that pushes for a form of integration is the management of information. The security information is like a puzzle. It is the assembly of all pieces of information that provides a comprehensive picture. The tendency (coming from the military) is to aggregate all information within a centric network system in order to give everyone a common operational picture. For the moment this is a tendency but at national level every state is working on a national policy for security information and quite often "prestigious services" try to preserve their information autonomy.

7.3. *International policies*

Over the last two decades the international community has had to support peace and development in countries that either were failed states or were in a situation where security institutions have been disbanded or at least proved to be unable to work. Over that period and more especially from 2005 two major policies have emerged.

- The OECD drives the first one. It aims to create a safe environment for development especially with an economic perspective. It focuses on the governance of the security sector with a systemic approach. It is presented in the OECD manual "Security System Reform and Governance" that was issued in 2005.
- THE UN manages the second set of SSR policies. The peacekeeping operations department within the general secretariat does this. The UN approach intends to help and support UN missions and UN police forces that operate in a wide range of countries (18 at the present time) to implement the relevant Security Council

mandates they are given. The UN has published a wide range of documents on that topic.

Later the EU issued a policy to support its ESDP missions. It did that in a similar way to the UN. This policy that is based on the OECD work is described in the document “EU Concept for ESDP support to Security Sector Reform (SSR), issued in July 2016.

7.4. Public safety policies

Community policing

The concept of community policing has emerged in the US in the 80s. It is very close to the Robert Peel approach (cf. supra § 21). J.Q Wilson and Kelling have highlighted it in the famous “*broken window theory*“ scientific article in 1982 that gave way to a specific policing model. Briefly, the model focuses on the importance of disorder (e.g., broken windows) in generating and sustaining more serious crime. Disorder is not directly linked to serious crime; instead, disorder leads to increased fear and withdrawal from residents, which then allows more serious crime to move in because of decreased levels of informal social control.

The police can play a key role in disrupting this process. If they focus in on disorder and less serious crime in neighbourhoods that have not yet been overtaken by serious crime, they can help reduce fear and resident withdrawal. Promoting higher levels of informal social control will help residents themselves, meaning the community, to take control of their neighbourhood and prevent serious crime from infiltrating.

The concept was widely used by police forces in the US. Chief Bratton who had been police chief in Boston, New York, Los Angeles and again in NY has been a key advocate of that concept. This one later extended to other countries worldwide where it faces local adaptation like “proximity policing” or “daily security policing“ in France.

Community policing has been said to be the key factor of crime reduction and improved security environment in the US. This point is however discussed and there are arguments that point other factors that in fact helped to reach these achievements.

The community policing policy has widely relied on the human factor. On one hand it has emphasized the interaction between the police and the citizens. On the other hand it has concentrated police manpower on hotspots to stop and deter street crime. However and with a view to optimise the use of the human resource the community policing has developed a surveillance policy. Using CCTV and now video analytics and facial recognition, automated number plate recognition it intends to ensure an early identification of suspicious behaviours. When connected with police records and information analysis it drives to predictive policing order. In that perspective public safety interacts with public order when technology helps to catch disorders and with organised crime when it offers evidences.

Standardisation

Western countries have adopted a set of policies to “standardize behaviours and environment” with a view to prevent offenses and reduce vulnerabilities. A specific attention has been given to the following topics for which various sets of regulation has been put in place in many countries:

- Road safety and traffic: speed limitation, use of alcoholic beverages and drugs when driving, mandatory use of security items (safety belts, traffic lights...)

- Private spaces open to the public: technical norms to house and evacuate the public, restriction of access (football hooligans, prohibition of alcoholic beverages)
- Organization of public events: norms to provide security services (security steward, control room, MoU with police and fire and emergency ...)

7.5. *International policies*

Even if public safety within the framework of community policing remains a national competency it has a strong connection with democracy and human rights. This is why some international bodies that in fact are defining a policy can address community policing.

- In Europe the Council of Europe (CoE) is addressing policing and police in the field of public safety around two main topics. The first one is about police accountability that provides guidance for the governance of community policing even if at an institutional level it has a wider impact on the governance of the security sector. The second one is about police behaviour in dealing with the citizen. Both accountability and police behaviour are included in the CoE code of police ethics that was issued in 2001 and has been regularly updated through CoE police declarations since.
- Another set of international policies is provided by the European Forum of Urban security that is a European network of public authorities in charge of large cities. EFUS is working to assemble local initiatives into comprehensive approaches that can be presented as policies.
- Last and as mentioned previously the EU is initiating policies that are addressing the mobility of citizen with respects to public safety. First it is about of road safety and this includes anti-social behaviour on the road (cf. TISPOL). Second it is about football hooliganism and the relevant policy support police cooperation against that phenomenon, intelligence sharing, exchange of officers, common monitoring of supporters movement. Last is the Schengen Convention that facilitates local public safety police cooperation in border areas.

7.6. *Private security*

As mentioned, public safety and more generally security remain under a tight national competency. This is the case for private security. Looking at private security service providers it is obvious that over the last thirty years these have become major security actors. Consequently the previous policies that dealt with private guards in factory or on agricultural premises no longer were able to match the reality of the situation. This reality is made by huge players like G4S with a yearly turnover of 12 Bn\$ and a total staff of 620 000 employees. It is also clear that from the end of the 90s the private security sector has more staff than the public law enforcement agencies. It has also become clear that the private security industry has now both private and public missions in the field of public safety but also in other areas mostly national security (air transport, critical infrastructure).

To address the new nature of the private security service provider several countries have developed policies that generally intend to organize and oversee the activities of what is

generally called the private security industry. This allows public authorities to control the security service providers and to have a framework for technical exchanges. Key topics of such policies are about licensing (of companies and employees), training, carrying guns, mixing with Defense activities etc. Examples of such policies are reflected by the UK Security industry Act of 2001 that creates the Security Industry Agency and by the French LOPSSI 2 that created the CNAPS as an agency to oversee security industry. It should be noted that both UK and French policies are funding the public agencies (SIA and CNAPS) through fees that are paid by the security industry itself.

Aside organising and ensuring the control of the security industry the public policies in the field of security also define the role of the private security industry. There has never been any doubt to have the private security industry operating on private premises private in to ensure the protection of private interests. More recently different policies in many countries have both allowed and tasked the security industry to play a greater role in the public space with respects to public safety. This could include the safety of public events, the protection of public buildings and other missions that were previously completed by the police.

However there are huge differences among European states about the role and the size of the private security.

7.7. SUMMARY - Policies

CURRENT RESEARCH	
TECHNICAL	<ul style="list-style-type: none"> • Developing a wider use of the technology for surveillance
HUMAN	<ul style="list-style-type: none"> • Training people
ORGANISATIONAL	<ul style="list-style-type: none"> • Reorganizing the security system and governance • Implementing security norms (staff, building)
REGULATORY	<ul style="list-style-type: none"> • Protecting human rights and privacy • Preventing disrupting behaviours • Differentiating public safety competencies from other areas of the security sector • Organizing the security competencies

8. Current Practice

8.1. Prevention and response to call

The demand for public safety services is split between a need to permanently feel safe and a need to have every incident, every security issue being immediately addressed. This division is reflected into two different police and security industry practices.

The first practice is about prevention. Public safety uses two types of prevention. The first one is called situational prevention. It aims to make the violation of the law less attractive and less rewarding. It is based on the commitment of the potential victims to reduce vulnerabilities. In this framework it is the role of the police and of the private security industry to bring information and advice based on the knowledge they have the threat trying to go through vulnerabilities. The second one is called social prevention and it intends to deter offenders to

commit crime. It relies on a visible and active presence with techniques such as stop and search, checks either random or with fixed checkpoints. I could also include surveillance. Prevention practices whatever they are can be seen as what is called problem solving policing because they address the roots and not the consequences of crime. These practices demand for a close and continuous relationship with the public and therefore they have a cost/benefit ratio that is difficult to measure. Expenses can be very accurate but benefits are not easy to assess even with a comparative approach. Ultimately perception and feelings can be evaluated; this is accepted by citizens and communities but less by the business world that has to see prevention through a balance sheet template. Last it is worth to stress that a preventive model is very often bound to community policing even if this model is also used by authoritarian states to ensure a tight social control and a strong public order.

The second practice is about responding to call, in fact addressing an immediate response to security incidents. There are two ways for doing so. One is to have response team regularly deployed and present on the field for other purposes but able to abandon them to immediately move to the scene of the incident. The second one is to have responders waiting at a central place to move to the location of the incidents. In both cases there is a need for a centralized management of the resource. In both cases the use of technology (geolocalisation, software to optimize the deployment, central control room) should bring more efficiency.

Both police forces and private security industry use these two services trying to find the most appropriate balance to get efficiency.

8.2. *Police services*

The prevention versus responding to call differentiation directly impacts the model of police services both in terms of organization and of process of work.

Preventive services will be organised in order to keep a close contact with public. This would rely on small and autonomous police stations that are easy to access, feet patrols and wide initiative powers given to the officers, regular meetings with the public, presence of policemen and women coming from minorities.

The response to calls for duty demands a different model of police service with a more centralized organisation to optimize the resources, dispatch and coordinate the operational engagement. Surveillance and geo-localisation have lowered the need for a human knowledge of the area.

Police services could be structured with differentiated units, could have jack of all trade units or could emphasize one model over the other.

8.3. *Neighbourhood, local communities, citizen commitment*

Preventive and community policing as well as problem solving policing all converge to have the public, meaning the local communities, the neighbourhood and the individual citizen more committed. This approach has elaborated several practices.

- A first practice is of a local governance nature. It is to associate the local community and its citizen to the orientations of the public safety with a view to define what has to be done by the community and what remains to be done by the police. This provides guidance to the police and consequently facilitates police accountability. The business community can be part of the scheme.
- A second practice could be to promote a more active role of the citizen and more generally of the community including business: this can be done through

neighbourhood watch, citizen chain to report incidents, citizens patrols...and even community demonstrations against crime.

8.4. Private security

The private security companies combine the same features as the police services with respects to prevention and response. Prevention use advice and monitoring to reduce vulnerabilities and deter aggressors. Response will come most of the time from an alarm issued by sensors and the private security role is limited to confirm the reality of the aggression and to assist the police who are the only ones to be able and allowed to arrest people and to use physical force and weapons.

8.5. Public private partnerships

Public private partnerships are part of the preventive approach. They rely on information sharing both on a strategic level to build solutions that are implemented jointly and to an operational level to address a concrete case provided there had been some preliminary joint planning.

8.6. Surveillance and predictive policing

Surveillance and predictive policing (that includes intelligence led policing) are practices that first fall somewhere between prevention and response and second have introduced advanced technologies in the area of public safety.

As preventive instruments surveillance and predictive policing help to identify (weak signals) and warn about coming incidents. Therefore they could help to anticipate and to work on the causes of the problems. As instruments to support the delivery of the response they help to adjust the response with respects to the nature of the service to deliver, the place and the time to have it delivered.

The use of technology for surveillance and predictive policing is just at an early stage. Facial recognition, artificial intelligence and self-learning software will dramatically change the nature of surveillance by moving from the reporting of facts to the automated identification of crimes and of criminals. Similarly predictive policing will go farther than the clues that are provided by current analytics and could cover the profiling of potential offenders. This however could raise legal issues with respects to the presumption of innocence and could question a police tendency to pre-emptive measures.

9. Current Practices

- Group value and intention to use — A study of multi-agency disaster management information systems for public safety

<http://www.sciencedirect.com/science/article/pii/S0167923610001776>

The theory of information systems success in the context of large-scale disaster management (DM) for public safety. In the recent past, various evaluation reports on DM efforts have concluded that information quality and system quality are major hurdles for efficient and effective multi-agency DM and are critical antecedents for information systems (IS) success. This research develops and empirically tests a model that explains IS usage intention as a reflective measure of IS success in the public sector DM domain. In this paper, the effects of the expected value of IS for the entire group of collaborating DM agencies, task support, user satisfaction, and three specific information/service quality dimensions on usage intention are examined. The

results of the data analysis revealed that expected group value is a key determinant of intention to use in the public sector DM domain. The data analysis also showed that perceived task support only has an indirect effect, through user satisfaction, on the usage intention. These findings imply that previously suggested IS success models for business environments are likely to fall short in their explanatory power and applicability for highly volatile complex disaster environments that require immediate coordinated responses from a large number of organizations.

- Partnerships, information and public safety: Community policing in a time of terror
<http://www.emeraldinsight.com/doi/full/10.1108/13639510210437023>
Congress has expressed concern that the Homeland Security agency might lack the power necessary to prevent future terrorist attacks. This paper argues that it is less likely to be a lack of police power and more likely the misapplication of those powers that undermines the war on terror. Until one learns to police in ways that build trust within those communities least likely to willingly assist the police, no amount of additional funding or legal authority will increase the capacity of the police forces to gather the information needed. For neighborhood policing this means partnering with those most victimized by crime. For the war on terror, this means partnering with Arab-American communities. This examination of partnerships provides a basis for understanding how likely it is that current neighborhood policing practices will support a successful war on terror.
- Risk management in a dynamic society: a modelling problem
<http://www.sciencedirect.com/science/article/pii/S0925753597000520>
In spite of all efforts to design safer systems, we still witness severe, large-scale accidents. A basic question is: Do we actually have adequate models of accident causation in the present dynamic society? The socio-technical system involved in risk management includes several levels ranging from legislators, over managers and work planners, to system operators. This system is presently stressed by a fast pace of technological change, by an increasingly aggressive, competitive environment, and by changing regulatory practices and public pressure. Traditionally, each level of this is studied separately by a particular academic discipline, and modelling is done by generalising across systems and their particular hazard sources. It is argued that risk management must be modelled by cross-disciplinary studies, considering risk management to be a control problem and serving to represent the control structure involving all levels of society for each particular hazard category.
Furthermore, it is argued that this requires a system-oriented approach based on functional abstraction rather than structural decomposition. Therefore, task analysis focused on action sequences and occasional deviation in terms of human errors should be replaced by a model of behaviour shaping mechanisms in terms of work system constraints, boundaries of acceptable performance, and subjective criteria guiding adaptation to change. It is found that at present a convergence of research paradigms of human sciences guided by cognitive science concepts supports this approach. A review of this convergence within decision theory and management research is presented in comparison with the evolution of paradigms within safety research.
- Research on Urban Public Safety Emergency Management Early Warning System based on Technologies for the Internet of Things
<http://www.sciencedirect.com/science/article/pii/S1877705812032468>
Urban public safety emergency management early warning system based on technologies for the Internet of Things (IOT) can realize the function of omni-directional monitoring and control,

accurate prediction and efficient disposal. The rescue mechanism of a unified command, complete function and response sensitivity, and operate efficient be formed by the system. And improve the city's ability to withstand to public emergencies have great significance. In this paper, the current research situation for Internet of Things application in the field of public safety is introduced. The characteristic, structure and constitution are expatiated in details with illustration. Then the software and hardware platform, and the system function are analyzed. The key technologies and the technical research routes of the system are expounded.

- LTE for public safety networks

<http://ieeexplore.ieee.org/abstract/document/6461193/>

In recent years the public safety community, more particularly first responders, has watched with envy the growing wireless multimedia capabilities offered to consumers by new 3G technologies. Although some first responders make use of WiFi in the interference-prone unlicensed spectrum, the majority of first responders linger in a 2G world. Global attempts at garnering support for additional spectrum or reshuffling existing spectrum, the keys to broadband deployment have not always been successful because of hindrances such as commercial stakeholders' interests and budget constraints. However, nowhere was the effort to enhance public safety communications as sustained as in the United States post 9/11.

- Rapid Deployment of Wireless Ad Hoc Backbone Networks for Public Safety Incident Management

<http://ieeexplore.ieee.org/abstract/document/4411144/>

This paper studied a problem of deploying wireless ad hoc relay devices in real time by public safety first responders at an incident scene without pre-planning so that a wireless communication backbone network can be rapidly established at the scene. A collaborative deployment method is proposed to enable mobile devices carried by first responders to exchange control information and make deployment decisions based on such information. Simulation results show that the proposed method efficiently establishes a reliable ad hoc backbone network at an incident scene.

- Modelling of safety management systems

<http://www.sciencedirect.com/science/article/pii/S0925753597000349>

Management systems for safety and environment and audits for assessing them have been a major research topic of the last few years. This attention has been fuelled by increasing emphasis in European directives on auditable safety management systems (SMS) 1 and by the increasing interest in their certification following the principles of the ISO 9000 series of standards. This paper reviews briefly the literature on this topic and presents a framework within which the total activity of an SMS can be presented using a consistent descriptive language. The framework can be used to describe and evaluate an SMS or to assess the completeness of audit tools designed for SMS evaluation. It can also be used as a didactic framework for safety practitioners and managers and as a tool for accident analysis. The framework combines the following principles:

- safety management seen as a set of problem solving activities at different levels of abstraction in all phases of the system life cycle;
- safety related tasks are modelled using the Structured Analysis and Design Technique (SADT). This shows the inputs, resources and criteria/constraints necessary to produce the required outputs;
- risks are modelled as deviations from normal or desired processes.

The framework emphasises the dynamics of safety management as a process. It aims to provide an abstract ordering of the field which can clarify and specify research and policy needs for the future. It also provides a clear definition of safety culture.

- Spectrum considerations for public safety in the United States
<http://ieeexplore.ieee.org/abstract/document/1580930/>
Since the inception of mobile radio, public safety agencies have relied on wireless communication systems to coordinate day-to-day and emergency operations. The decentralized and autonomous nature of the various public safety agencies in the United States has led to the deployment of a variety of systems operating in a fragmented spectrum, ranging from lower VHF to upper UHF. Due to the narrowband technologies used in public safety communications systems, public safety agencies have been limited primarily to voice services and low-speed data transfer on their private networks. In contrast, the commercial cellular sector now offers a large portfolio of services that include voice, messaging, email, Web browsing, picture transfer, video streaming, and other wideband services. In this article, some of the factors driving the expansion of spectrum allocated to public safety agencies are described.
- Perpetuity research: criminal Justice, Crime prevention and community safety :
<https://perpetuityresearch.com/criminal-justice-crime-prevention-community-safety-research/>
Criminal justice, crime prevention and community safety are essential components for maintaining a safe and secure society. At Perpetuity we have extensive experience of working on such diverse topics as reducing reoffending, evaluating crime prevention initiatives, and researching gang crime, knife crime, domestic violence, violent crime, serious acquisitive crime, and drug and alcohol related offending to name a few. This organisation is about providing comprehensive research using a combination of scholarly examination and practical expertise to support local and national work in understanding and preventing crime.
- Perpetuity research “ improving the local response to frauds
<https://perpetuityresearch.com/improving-the-local-response-to-fraud/>
Perpetuity and the Police foundation are working together on a two-year project investigating the UK response to fraud. This work is founded on previous research carried out by the teams which found that a disproportionate amount of fraud is organised and that it is highly prevalent. The work showed, for example, that between a third and nearly half of all frauds occurring locally in our sample of two police force areas were linked to Organised Crime Groups, which is at least twice previous Home Office estimates. The research also found that despite the significant and sometimes very damaging impact fraud has on communities it is not a priority for many local police forces and largely falls outside the responsibility of many agencies, including the police. This new project seeks to understand how the local response to fraud can be improved. The research covers three key areas that will be examined alongside one another in order to understand how local resources should be balanced:
 - Perpetrators of fraud
 - Victims of fraud
 - Protecting the public from fraudThis research aims to provide an overview of the current response to fraud, to understand the roles of relevant local agencies, and their relationships, and to provide recommendations for improving the response. The project will investigate:
 - How information relating to fraud is gathered, shared and analysed to understand the crime, including organised fraud and cyber-enabled fraud.

- How fraudulent activity is identified, assessed and prioritised with police forces and across other agencies.
- The powers, roles and responsibilities of relevant agencies in the public, private and third sectors around tackling fraud and how these bodies work together effectively (or not).
- The resources deployed by particular agencies, how effective are these and what good practice looks like.
- Centre étude et sociologie des institutions pénales
www.cesdip.fr/publications/penal-issues/
The revisiting of crime-based insecurity is based here on new data. However imperfect, they do enable us to document the various aspects of insecurity and above all, to track the current trends. Indeed, the development of victimisation surveys, repeated at regular intervals, allows for more systematic study of feelings of insecurity

9.1. SUMMARY – Current practice

CURRENT RESEARCH	
TECHNOLOGY	<ul style="list-style-type: none"> ● Information systems in the context of large-scale disaster management ● Socio-technical system involved in risk management ● Urban public safety emergency management early warning system based on technologies for the Internet of Things (IOT) ● First responders use of wireless multimedia capabilities by new 3G technologies ● Wireless communication systems to coordinate day-to-day and emergency operations ● Management systems for safety and environment ● Audits for assessing the management systems ● Responding to call efficiently (control room, geo-localisation, asset management) ● Profiling potential places and authors of offenses
HUMAN	<ul style="list-style-type: none"> ● Neighborhood policing (partnering with those most victimized, other communities) ● Examination of partnerships ● Stakeholders: legislators, managers, work planners, system operators. ● Public expectations and public satisfaction
ORGANISATIONAL	<ul style="list-style-type: none"> ● Risk management: modelled by cross-disciplinary studies ● System-oriented approach based on functional abstraction ● Public safety communications ● Response to fraud ● Comprehensive research using a combination of scholarly examination and practical expertise to support local and national work in understanding and preventing crime. ● Development of victimisation surveys, repeated at regular intervals ● Organizing processes and structures to deliver response and closely liaise with the communities/citizens

REGULATORY

- Changing regulatory practices and public pressure
- Defining legally pre-emptive measures to support predictive policing

10. Legal Factors

10.1. *Human rights and privacy*

National laws in each country define the protection of human rights and privacy. However these should comply with the international law namely the UN Universal declaration of Human rights and by the European convention of human rights (for countries that are signatories to this convention).

An administrative bodies that regularly update and provide guidance about the legal interpretation support UN (UN Council for human rights) and European (Council of Europe general assembly and general secretariat) legal framework. At European level this is complemented by the rich jurisprudence of the European Court of Human Rights.

The key points of human rights with respects to public safety are mostly addressing the police behaviour and especially the use of force or weapons. Most principles have been defined for a long time. When it goes to privacy it is highly impacted by development of technology and the jurisprudence is still in a buildup phase. Technology has been mainly in the field of communication but recently extended to unexpected area like aerial surveillance by drones.

10.2. *Commercial and penal fraud*

In the field of public safety a large part of the property crimes are linked to frauds. However frauds do not fall within the scope of the penal law and appears more relevant to commercial meaning contractual law. For the victims, individuals or private companies, there is a tendency to look for a penal framework. On the same time and to avoid to be overwhelmed by such case the prosecution and courts are eager to decline their competencies and to argue that these are civil cases.

The number of such conflicts is increasing due to the complexity of trade operations (sales and payment) especially at consumer level. In some country there is a tendency to look for some form of administrative litigation as it is the case in France for private bankruptcy.

Another situation is that of illicit trade at retail level. If illicit trade is defined by the violation of the law the violation itself suffers a weak legal framework. This is especially the case of incompliance with regulation that deals with health, physical safety, environment, technical specifications. Specific skills are needed to proceed such cases and as far as there is no serious harm, public authorities and judiciary tend to ignore these, until illicit trade disrupts deeply social and economic areas.

10.3. *Criminalisation, prosecution and trial*

When it comes to penal matters the law has to be mitigated with prosecution and court practices. The law offers the legal basis but the implementation of the law falls in the hands of the prosecutors and judges. Consequently it is necessary to take into account their practices, especially with respects to (1) the gap between the law and the current social practices and (2) the inaccuracy of the law.

In one sense when the law looks obsolete, the gap between the law and the social practices could make that prosecution and courts are more lenient. This is for example the case for

begging that could be a still existing XIXth century law nobody would like to sentence. It is the basis of the discussions about the use of marijuana despite that is no longer punished in several countries, while it is still prohibited by the International Vienna Convention of 1967. In another sense the legal practice could be very tight when the law appears to be light-handed as it had been the case in some countries for sexual crimes before the law was revised to be tougher.

Last the legal factor has normally to be seen through individual cases according to the basic principle of human rights. However and especially in the area of public safety mass litigation is a serious issue. The usual judicial proceeding cannot be used without paralysing the judiciary but offenses have to be punished. This is where there is a development of police tickets with police officers issuing a fine on the spot and therefore closing the case. This has been used for a while for traffic violation where it even includes automated judicial responses now (e.g. speed radar, red light crossing). Now the tendency is to use that practice for public safety (use of drugs, illicit sale on the street, prostitution, petty violence). This raises a serious debate on how far is it possible to proceed and with which guarantees before entailing human rights principles.

Therefore to assess the impact of the legal factors in the area of public safety, it is necessary to assess not only the law but also the prosecution practices and the court jurisprudence.

10.4. SUMMARY - Legal factors

<i>CURRENT RESEARCH</i>	
<i>TECHNICAL</i>	<ul style="list-style-type: none"> • Technology to process mass offenses
<i>HUMAN</i>	<ul style="list-style-type: none"> • Peoples expectation for human rights and privacy
<i>ORGANISATIONAL</i>	<ul style="list-style-type: none"> • Transferring competences from the judiciary to the police
<i>REGULATORY</i>	<ul style="list-style-type: none"> • Adjusting penal code to new • Managing the gap between criminalisation and prosecution

11. 'THOR' Summary

MASTER'S COURSES Public Safety Management (LCI and RSM)	
LEADERSHIP	<ul style="list-style-type: none"> • Understanding the nature of security and the different areas of the security field, the stakes, games and players • Addressing the public safety issues in your organization multidisciplinary, creative and analytical and outside with various stakeholder. • Learning to have the overall responsibility of security (global protection) develop and implement a strategy, manage tasks and assess internal and external security providers, etc. • Personal transformation: being able to operate as a professional executive in the field of security • Obtaining a systematic approach and provide solutions from a systems perspective, integrating different angles • Develop, support, and enhance writing and verbal communications skills • Weigh and assess common areas of occupational proficiency for security executives: data protection, emergency planning and response, homeland defense, and legal liability. • corporate social responsibility, compliance and integrity
TECHNICAL	<ul style="list-style-type: none"> • Using electronic technology: Access control, tracking and surveillance • Deploying Information systems: intelligence, alarms and guidance • Deploying traceability and markers to prevent loss prevention • Discern and differentiate concepts of situational crime prevention, rational choice theory, and criminological tenets to understanding crime and to evolving countermeasures for the control of harm, loss and disorder.
HUMAN	<ul style="list-style-type: none"> • Driving security Staff (management and providers) • Developing general staff security role and capacity (skills, training) • Managing human resources and creating a protective climate (harm prevention and confidence) • Security/protective culture
ORGANISATIONAL	<ul style="list-style-type: none"> • Organising leadership: hierarchy and security management line including compliance (job definition) • Protecting assets : capital and physical, brand and image, IP and know how • Ensuring safety of people: customers, partners, staff and their relatives • Ensuring safety of operations: R&D, production, sales and procurement, logistics • Developing organizational resilience (crisis management model) • Contracting/tasking private security service providers • Coordinating with law enforcement agencies • Mobilizing partners and developing public private partnerships with a focus on local communities • Discover and apply tools to be effective in achieving those goals, particularly in areas where current practices are deficient, such as information protection, security technology, legal justice, and safety services.

	<ul style="list-style-type: none"> Evaluate the origins and current structure of security management within corporations, not-for-profit institutions, and government.
REGULATORY	<ul style="list-style-type: none"> Ensuring Property laws Compliance and vigilance requirements Respecting privacy (staff and customers/providers) Learning about differences in legal systems and how to deal with it Various laws that stress the responsibility of companies
METHODS	<ul style="list-style-type: none"> Implementing risk analysis (threats, natural and technological hazards, vulnerabilities and interests to be protected) Completing Strategic analysis (likely and impact, needs and capacities) to assess priorities and define strategic actions Developing Strategic responses (core, crisis, routine/repetitive and anecdote) Elaborating Strategic planning (action and support) Balancing situational prevention vs operational strike response
THREAT	<ul style="list-style-type: none"> Identifying and measuring the impact of petty aggressions (physical, verbal, psychological) Identifying and measuring the impact of petty theft (shoplifting, employees diversion) Identifying and measuring minor voluntary destructions and disruptions of business activities (fires, tags, garbage, power cuts,) Taking into account the management of groups and crowds in case of incidents and large scale events Identifying and measuring the potential natural and technological hazards and their consequences Identifying and assessing the consequences of public disorders (disputes, anti-social disorders, hooliganism) and of social unrests (demonstrations; looting) on business activities, staff and customers
ENVIRONMENT	<ul style="list-style-type: none"> Understanding public safety policies (state, local communities) Liaising with similar organisations and professional bodies that face the same challenges to assess situation and elaborate responses Raising local partnerships with local authorities and the local business community

Reference list

- “The handbook of security” , Martin Gill, Palgrave Mac Millan, 2016
- “The future of policing” , Schafer, Buerger, Myers, Jensen, CRC Press, 2017
- “Ce que fait la police “ D. Monjardet, Odile Jacob 1995
- “Policing 2020” J A Schafer, Police futurist 2007
- “The new structure of policing” D H Bayley and C D Shearing , National Institute of Justice 2006
- “The review of Policing”, Ronnie Flanagan, Her Majesty Inspectorate Constabulary, 2008
- “ Future Trends in policing” Police executive research forum , 2014

Annex 5

ORGANISED CRIME

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 Organised Crime Module

Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 Organised Crime Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V0.1
Date:	February 12 th , 2018
Authors:	LCI
Document description:	Desk based analysis carried out by DL and HP

1. Module descriptor

Module Name	Organised Crime: “crime which involves individuals , normally working with others, committing serious crime on a continuing basis “ (Home Office 2012)
Module Aim	The module integrates knowledge from various disciplines with a focus on how public and private organisations can respond to the challenges introduced by organised crime (. It brings together history, sociology, politics, and international relations as a foundation for a better understanding of the governance of responses to organized crime. The focus is both on public policy-making on one hand and enhanced awareness and commitment of the private sector on the other.
Learning Outcomes	
LO1	Understand the issues and problems faced by leaders in the public and private sectors with respects to organised crime.
LO2	Understanding the context of change in various disciplines with respects to new forms of organised crime.
LO3	Applying new knowledge how public and private organisations can respond to the challenges offered by organised crime
Indicative Content	<p>The management of government and other public organisations is subject to increasingly high demands especially when it comes to emerging challenges that carry what is perceived as threat both for individuals and for the society. Globalization and the development of transportation and communication in the wider context of the e-society have dramatically changed the forms of organised crime. Finding answers in terms of policy and fulfilling the conditions in terms of democracy, effectiveness and efficiency test the internal performance of public and private organisations, particularly their management. To successfully complete its tasks, management has to integrate the various activities and impacts of organised crime with respects to the daily social, administrative and economic life. Consequently, there is a growing need for multidisciplinary approach. The module “organised crime” offers a multidisciplinary, analytical and creative approach to the issues and problems faced by managers in the public and private sectors.</p> <p>The module provides a forum of professional students and other security executives whose combined expertise will be utilized in a synergistic manner in developing, organizing, assimilating, and sharing knowledge and experience for the ultimate purpose of enhancing professional and business standards.</p>

2. Master programmes

2.1. Current courses

- MSc Criminal Justice (Rochester Institute of Technology USA)
<http://www.rit.edu/programs/criminal-justice-ms>
The master of science degree in criminal justice emphasizes a multidisciplinary approach that encompasses OC. The program builds on a foundation of locally relevant policy research by providing students with the critical skills to carry out such work and the experience to assure success in employment or in pursuit of further graduate studies. The program provides students with a strong foundation in criminological, criminal justice theory, and social scientific research skills, thus enabling graduates to have successful careers in the policy analysis arena or to be prepared to pursue advanced study beyond the master's degree.
- MSc Crisis and Security Management (Leiden University)
<https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management>
During this multidisciplinary master's programme students become familiar with the political and social dimensions of the governance of (in)security and crisis. This encompasses OC issues.
- MSc Crime, Violence and Prevention (London Metropolitan University)
<http://www.londonmet.ac.uk/courses/postgraduate/crime-violence-and-prevention--msc/>
The master's course encourages students to look critically at public protection, a key practitioner concept for professionals working in socially responsible professions. There is a special emphasis on gaining a sound grasp of the relevant academic literature, including substantial use of key scholarly journals in the field of criminology and criminal justice. There is also a focus on how theory relates to and enhances good practice. The course provides academic context to understand and evaluate the complexity of, and reciprocity between, varied agencies, departments and policies related to organized crime, criminology and criminal justice.
- MSc Advanced Policing Studies (Liverpool John Moores University)
<https://www.ljmu.ac.uk/study/courses/postgraduates/advanced-policing-studies>
Advanced Policing programme develops the skills increasingly required by forces as policing moves further towards an evidence-based approach. The programme addresses the quantitative research skills gap identified in policing. This course is for serving officers and those about to embark on their policing or academic career. It will learn evidence-based learning skills.
- MSc International and Transnational Policing (Liverpool John Moores University)
<https://www.ljmu.ac.uk/study/courses/postgraduates/international-and-transnational-policing>
The International and Transnational Policing MSc looks at the implications of policing across geographical and political boundaries. Students discover how

policing is carried out across geographical boundaries and explore policing issues including organized crime arising from differing jurisdictions, policies and procedures.

- MSc (Erasmus Universiteit Rotterdam) Int. Public Management and Policy
www.eur.nl/english/master/programmes/international_public_management_and_policy

Public policy has gone international: organisations such as the EU and the UN are growing in importance. Master the theories, concepts and skills you need to work effectively in this time of increasing internationalisation; tackle global issues such as international conflict, poverty, migration, environmental protection and corruption.

- MSc (Universiteit van Utrecht) Global Criminology
www.uu.nl/masters/en/global-criminolog

Old and new forms of global crime are rapidly expanding, as are the means to control it. The Netherlands serves both as a major crossroad in the illegal flow of goods, people and services and as a key host for international organisations such as Europol, Greenpeace and the International Criminal Court. Drug trafficking, human trafficking, international terrorism, corruption, environmental harm, financial and corporate crime and conflicts over natural resources all have global dimensions. Tackling these issues requires modern instruments that transcend national boundaries.

- MSc (Universiteit van Leiden) Global conflict in Modern Era
<http://www.mastersinleiden.nl/programmes/global-conflict-in-the-modern-era/en/programme>

In the Global Conflict in the Modern Era master programme students will explore the patterns of war and peace in the modern world from a multidisciplinary angle, incorporating history, political and social science and area expertise. The programme examines the core concepts and dominant approaches to the study of war, as well as more recent and critical takes on these phenomena. Students also study the theoretical and empirical explanations for war and peace that have been offered by the academic scholarship

- BS in security management John Jay college of criminal Justice
<http://www.ijay.cuny.edu/security-management-bs>

The major in Security Management concentrates on the analysis of security vulnerabilities and the administration of programs designed to reduce losses in public institutions and private corporations. The program prepares students for careers as managers, consultants and entrepreneurs

2.2. SUMMARY – Current courses

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • Policy analysis and practice • Criminological skills • Criminal justice theory
HUMAN	<ul style="list-style-type: none"> • Implications of law enforcement across geographical and political boundaries • Deviance and criminology, sociology of OC
ORGANISATIONAL	<ul style="list-style-type: none"> • Social scientific research skills • International: Impact of global issues, as trade globalization, migration, environmental protection and corruption • Awareness and response vs Contemporary OC challenges • Multidisciplinary approach • Local and global crime • Organizational management (incl financial and procurement), • Public administration
REGULATORY	<ul style="list-style-type: none"> • Understand and evaluate the complexity of, and reciprocity between, varied agencies, departments and policies related to crime, criminology and criminal justice. • Understand the regulations and mechanisms that are at work in public administrations and private organisations with respects to responsibilities and compliance. • Explore policing issues arising from differing jurisdictions, policies and procedures

3. Stakeholders Perspectives

Organized crime is a clever security threat that proceeds discretely until it gained enough power to control people and to offer a societal alternative that works outside the rule of law. Therefore it has to be seen either in a build up process when it has no full control of certain sectors or well established when it has already a sound basis to operate. Concretely organised crime is the fact of criminals who operate in groups to commit serious offenses on a continuous basis.

3.1. Stakeholder perspective general

Organised Crime is a political, social and economic alternative model that operates outside the rule of law. This means that (i) it does not respect the legal provisions

that are designed to protect legitimate interests, (ii) it solves disputes through violence and (iii) its leadership obeys tribal and patriarchal principles. It uses political, social and economic weaknesses and vulnerabilities to offer its members power and rewards.

3.2. Corruption and hostile take over

Corruption and hostile take over of organizations either private or public are both first tools and core objectives of organized crime. Corruption is initially implemented through bribery. Then when bribes have compromised the targeted officials these ones are blackmailed and have no other choices than to obey their criminal masters or to disclose their previous corruption. At that stage the organised crime has reached its objective of control. Such a control could cover the whole or just one part of the organization according to the needs of the criminals. For example if the organised crime ring want to embed illicit trafficking in a maritime container they will corrupt just the few key people, either public (customs, port authority) or private employees (logisticians) that will help them to hide their materials at loading and unloading places.

While corruption is an indirect control of organizations through the control of their officials the hostile take over is a direct control of the organizations where the criminals replace the regular officials. Such a replacement could occur through bribes or violence to have regular staff abandoning their position or through frauds to have criminals reaching position they would otherwise not be granted. In the private sector the hostile take over can be the outcome of a financial investment by using the proceeds of the crime. The huge profits that are generated by some criminal activities, especially the various types of trafficking, give OC organisations the financial resources they need. Usually this has to go first through a money laundering scheme where criminals could expect to get at best a 30% laundering rate, something that is seen as excellent to get a legitimate status.

Corruption and hostile take over are key for the strategy of criminal organisations. They offer an area, either a territory, an organisation or a community inside which they can extend, conceal and implement their activities freely. For that reason it is critical for those who are legitimately in charge of these same territories, organisations and communities to be able to detect organised crime activities at their early stage in order to block these activities.

3.3. Trafficking illicit goods and services

International conventions prohibit the production and trade of drugs as well as any type of sexual exploitation and forced labour. In many countries the law prohibits products such as weapons, alcohol beverages and services such as gambling and prostitution. Usually laws are a mix of morale, public order and health rationales to protect people and prevent a demand. Sometimes the consumer of such products and services can be prosecuted and sentenced.

Such a situation is a holy land for organised crime. On one hand there is a strong demand. On the other hand the demand is coming from consumers who know they are outside the law and ready to behave accordingly. Therefore they will never complain and are falling in the area where organised crime operates according to its own rules. Criminals could consequently fix their prices and solve complaints, as they like. Typically criminal markets obey economic rules and could be either a monopoly when criminal organizations are cartelized or an open market when criminal organizations are competing to access consumers. Generally organised crime ensures a safe and peaceful environment around market places to attract and please consumers. There is here a paradox that organised crime could ensure a good level of public safety. This contributes to strengthen the social control of organized crime on local communities and territories. Unfortunately blind or cynical politicians and public managers could accept this.

The trafficking of illicit goods and services generates huge profits but is generally highly risky. This is especially the case in the drug sector where policies are tight and law enforcement agencies motivated and well equipped sometimes with an incentive to use the seized crime money for their own budget. When looking at the cyber world the trafficking of illicit goods makes the greatest part of the darknet mostly in wholesale deals. Web sites and social media are used more and more for retail sales.

In some specific circumstances like war, embargo, crisis political leaders can welcome the trafficking of illicit goods by criminal organisations. There could be a type of collaboration. The trafficking of drugs could provide financial resources. The trafficking of weapons could help insurgents, militias and even terrorists to strengthen their military capacity on the ground.

3.4. Illicit trade of licit goods/illicit trade

The trafficking of licit goods is very similar to the trafficking of illicit goods. It is also called illicit trade the definition of which is the sale of goods and services to the public that violates the law. This definition opens a wide scope of illicit trade from the breach of (i) property laws (stolen and counterfeited goods), (ii) fiscal law (contrabands and tax avoidance), (iii) all regulations that prohibit the trading of goods that endanger health or physical security, breach the protection of environment or violate international regulations about the prevention of conflicts, the work of children...In all these cases a lack of compliance could trap public and private bodies. Last illicit trade could also come from the breach of commercial rules and contracts with parallel imports being a major threat for many manufacturing companies.

Illicit trade looks like a soft white-collar crime but has a huge social and economic impact because it offers an alternative to the existing social and economic system. Figures from OCDE and WEF are around several hundred billions dollars yearly therefore making illicit trade a member of the G8...Counterfeited goods have been for a while the bulk of illicit trade (460 Bn US\$ in 2016 OCDE). Illicit trade is combining

organised crime for large scale supply and petty crime that relates to public safety for retail and distribution. Organised crime has the capacity to move shipments of several containers across the world or to loot cargo on the road or in storage areas (8 Bn €/year in Europe). Petty criminals can sell products at street corner or on social media.

Criminal organisations are also bound to rogue politicians, terrorists and armed militias to operate illicit trade activities. This is mostly done through levying a toll to extract, produce or move the products of illicit trade. Blood diamonds, rare earths, crude oil as well as timber rhino horns or ivory are seen as financial resources by warlords and corrupted politicians. Mokhtar Al Mokhtar provides an iconic picture of that situation. This individual is a famous jihadist who operates in the Sahel region both is nicknamed Mr Malboro due to his involvement in cigarette smuggling and the leader of the In Amenas terrorist attack in Algeria (year 2016, 40 fatal casualties and 800 hostages for three days).

Individually the private companies are aware of the situation with respects to their business. They are working to mutualize their efforts especially with respects to counterfeited goods but have some difficulties to mobilize public authorities.

3.5. Frauds and money laundering

Large-scale frauds have always been part of organised crime activities. They have reached an industrial level and have to be seen as white collar crime; according to Kroll around 80% of CEO meet at least one fraud case a year. Some fraud scheme can target the public budget like VAT or subsidies frauds at European level. Other schemes could look after private organisations or even individuals (phishing). Because they harm confidence between economic actors they have a wider impact on the whole economy than the direct losses they produce.

Over the last years cybercrime has seen the fraudster moving away from forged documents to cyber attacks to catch money. Sophisticated frauds can manipulate stock values by using fake news (VINCI case France 2016) or by deploying a pump and dump approach.

Frauds by using payment tools like credit card have a dual impact. First they have a financial cost (1,16 Bn € for a total payment of 3 000 Bn € for credit card in Europe); this could look limited but is quite high when compared to the cost of operations. Second it questions the robustness and the integrity of the system therefore impacting confidence, something that is key for business.

A major cause of fraud inside companies but also in public organisations takes place in the procurement process where huge amount of moneys circulate. The basic scheme is to (over) pay for a product or a service that at worst does not exist or at best is substandard. According to the private investigation firm Kroll such frauds are quite often connected to OC groups and rely on internal connections. In all public and private organisation procurement is a critical stage where management has to pay a great attention. This is a place where corruption could be used by OC.

The sophistication of frauds is limited only by the creativity of the fraudsters. Rogue Russians cybercriminals, state sponsored ones are competing with Nigerian crooks to imagine how to get money illegally from private or public purses or from the financial markets.

Frauds are not the only financial activities of the organised crime. Money laundering to integrate the profits of crime in the real economy is also a key criminal financial activity. Money laundering is usually connected with regular economic activities like trade based money laundering and asks for the support of some legitimate economic actors who are either blind or corrupted.

3.6. Embedded and concealed operations

Organised crime activities especially all forms of trafficking have to be concealed. Criminals could operate undercover on their own but they have to build a cover something that is expensive and not easy especially in an environment that is not friendly. When it is possible it is better for them to embed their operations in an already existing operation. This could ask for some accomplice but it could be achieved at a low level. The transportation of goods is the best example of such a practice. A truck driver can be asked and could accept to take aboard his vehicle a full pallet of drugs for a few hundreds of euros. The transportation of individuals, trafficked persons, illegal immigrants, and fugitives can be organised similarly. If the employee can face a penal sentence the consequences for the employer could be heavy with the seizure of the vehicle, the disruption of the relevant logistic and the tarnished corporate image. Once more this is a matter where front line managers have to be vigilant.

Consequently the embedment of organised crime operations in regular business operations is a situation many companies can face that could engage their responsibility. In all cases that demands some form of complicity. For that reasons managers have to be very cautious to identify any suspicious event that can come from such embedment.

3.7. Business responsibility, due diligences and compliance

Over the last decades and following major private companies failures that harmed customers, shareholders, creditors and impact the public confidence in business regulations have been put in place. These regulations stress the responsibility of companies with respects to criminal activities they could be associated to. They cover a wide area from bribes to ensuring the integrity of providers and customers; they also ask for compliance with all rules that are linked to environment, health, physical security, international order, protection of vulnerable persons...

The consequence of that trend is the development of new practices by companies. The first one is the role of the compliance officer who has to ensure that all operations are complying with existing regulations. Companies that do not commit themselves in that sense are expose to public disapproval and quite often to

prosecution. The second consequence is the practice of due diligence with companies calling special investigation firms to ensure that their business relation match the criteria of honesty and integrity. This should help to prevent OC activities and also avoid company “blindness”. Similarly companies are expected to develop internal control to prevent internal fraud. This responsibility is the source of a major dispute between the French bank Société Generale and the French tax service: the bank asks for a 2 Bn € tax rebate due to an internal fraud while the tax claims the fraud could have been detected and prevented therefore stressing the company responsibility.

The responsibility of companies is not only to take preventive measures. It is also to report to authorities the detection of suspicious activities. Usually this goes through prosecution and specialised investigative services or public authorities with a capacity to regulate and sentence.

3.8. Violence and Racketeering

Violence and racketeering, namely aggressive intimidation to extort money or to accept OC activities, is inherent to organised crime. This is first the case inside and among criminal organization. Second this can extend to people who are in situation of weakness because they are corrupted or compromised by organised criminals.

Violence is used for intimidation through physical assault but ultimately can go through murder to eliminate foes and also to intimidate communities in a mafia style approach therefore ensuring the power of the criminal organization. Usually OC organization have some mitigation mechanisms but these do not work in some cases especially when newcomers are challenging established gangs.

3.9. Desk based research stakeholders perspective

A key source for trends, threats and issues in organised crime can be found on the websites of a few institutions that have regular publications, usually annual assessment and reports. Among them are:

- UNODC <http://www.unodc.org/unodc/en/organized-crime/intro.html> the UNODC organised crime web page gives a regular update on the OC situation worldwide
- Interpol <https://www.interpol.int/Crime-areas>
This page of the Interpol website gives a comprehensive view of organized crime and of its different forms.
- WCO <http://www.wcoomd.org/en.aspx> the WCO website presents a wide scope of information on frauds, contraband and illicit trade. This covers both WCO activities, policies, training operational coordination and studies.
- EUROPOL : <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>
Serious and organized crime threat assessment that is published yearly helps to understand the new forms and trends of organized crime. Aside the report

an academic review provides a more analytical view of the OC situation in Europe.

- FBI : <https://www.fbi.gov/investigate/organized-crime> like UNODC or Europol the FBI web page on organized crime gives an American view of organized crime but aims to offer a world vision
- NCA <http://www.nationalcrimeagency.gov.uk/crime-threats> like the previous listed websites the NCA website on crime threats presents a comprehensive detailed and analytical view of the different types of OC threats with respects to both the current situation and the current and emerging threats.
- The US national institute of Justice (NIJ): <https://www.nij.gov/Pages/welcome.aspx> gathers all US government funded research in organised crime
- Trans crime <http://www.transcrime.it/wp-content/uploads/2015/12/ocp.pdf> Trans crime a conducted a research on how illicit trafficking operates in Europe
- Transnational alliance to combat illicit trade (TRACIT) <http://www.tracit.org/> gives a view of the situation with respects to Illicit trade
- International security management association <https://isma.com/> ISMA offers a concrete and practical view of the organized crime situation and threat in the private sector
- European Corporate security association <https://www.ecsa-eu.org/> ECSA's Objectives are to provide its members with a trusted forum for sharing common issues, experiences, information and education. This includes OC issues
- Perpetuity research <https://perpetuityresearch.com/> Perpetuity Research is a leading research company with wide expertise in both quantitative and qualitative approaches. They have been involved in OC issues from a corporate point of view.
- Transport Asset Protection association <http://www.tapaonline.org/> TAPA focuses on cargo theft and offer a comprehensive view of the relevant activities of OC in this sector their website list substantial reference papers either studies or researches.

3.10. SUMMARY - Stakeholders' perspective

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<ul style="list-style-type: none"> • E-business introduces vulnerabilities to be used by OC • Identifying OC activities on the Internet and in social media • Using modern technology to identify and report the commission of offenses • Information sharing

HUMAN	<ul style="list-style-type: none"> • Review existing knowledge of the police role in responding to crime • Public and private perceptions of OC (early detection) • Police response to OC. • Preventive OC measures inside public and private organizations
ORGANISATIONAL	<ul style="list-style-type: none"> • Warning mechanisms about suspicious activities of OC nature • Preventive practices • Balance between prevention and response with voluntary strategies. • Efficiency and effectiveness of policing (how effective police forces are at fighting OC) • Multi-disciplinary: common commitment to work at a European level on OC Threats at least on a sectorial basis. • Private sector initiatives to mitigate the economic and social damages of crime • Public-Private Cooperation
REGULATORY	<ul style="list-style-type: none"> • Police legitimacy (acting ethically and lawfully) • Private organisation responsibility and duty of vigilance • Compliance and Trust • Decision making and policy formulation. • Adjusting penal law to new types of offenses • Social and ethical engagement of companies, market and policy driven, security with respect to rule of law

4. BACKGROUND

The development of OC is bound to the socio political environment. The history of OC is bound to a few major societal changes.

4.1. *Traditional mafias*

Traditional mafia have emerged as a form of social control when other forms are weakening. This is the case of the Italian Cosa Nostra that took over from the aristocratic social control in a context of weak state.

More recently a similar process took place in Latin America, namely in Colombia and in Mexico. In these places the drug cartels established a social order that controls the territory and the community by offering a rewarding economic model that competes with the legitimate society.

Sometimes a specific event that supports a strong demand for trafficking could increase the development of OC (cf. infra § 5.2).

4.2. Drugs and major trafficking

Major trafficking have played a key role in the development of OC since WW1. This is usually the combination of several factors.

First factor is a strong demand that has several causes. It was the demand of alcohol beverages that is the basic cause of OC development in the US at the beginning of the XXth century. It is the social changes that initiate a high consumption of drugs in the 70s in the Western world. IT is also the consumerism that pushed the recent illicit trade of stolen, smuggled and counterfeited goods since the 80s and 90s. Whatever these products or services are answering a real need or are the outcome of an addiction the consumers are ready to enter the illicit trade scheme as customers therefore becoming an easy target for organised crime.

The demand in fact motivates OC to trigger the first level of crime (theft, fraud, counterfeiting...) in order to feed illicit trade scheme to match the demand. This is a dramatic change. A century ago the robber was the initiator of crime and once theft had been committed he had to find a buyer. Today the fence is the initiator of crime because once he has identified a demand he has to trigger the relevant criminal activity to get the product or service that is demanded.

This demand faced a public response that is a mix of morale, public order, fiscal and health reasons to limit, tax or even prohibit the sale of goods like drugs, alcohol and services like sex and gambling. The outcome of the public policies is either a price that goes beyond what would be a fair market price or a reduced or even full market unavailability

Consequently there is an area where organised crime can develop (cf. 4.). An anti OC strategy could be to at least depenalize or even legalize the sale of these goods and products. This was what was achieved with the end of the US prohibition when it became obvious it was a failure. It is what is behind the current debate about marijuana in the US and to some extend in Europe. In that sense depenalization can be seen as a preventive measure against OC. It avoids opening vulnerabilities that can be used by OC. A similar observation can be developed in the field of electronic products where the real value lays in the services that are tightly technically controlled and where the physical possession has a very limited interest. Companies like apple have developed a strategy in that sense.

4.3. International organised crime

Immigration and trade have created the conditions of international organised crime over a century.

Immigration helps to connect criminal group across the world. Criminals could hide themselves and their activities inside expatriated communities that like all communities in a foreign environment have a natural tendency to close themselves and to protect their members whatever they do. Communities stemming from immigration cover a network of criminal immigration. This was the case of the Italian

mafia, it is now the case of the Latin American MS13 as well of the Chinese triads. Diaspora are now a major feature of the modern societies for the best and for the worst.

The globalization and the development of world trade also help to initiate and support international organized crime. Communication means facilitate coordination among criminal groups worldwide. Flows of merchandise help to conceal criminal activities especially trafficking: only one per cent of containers are usually searched and even if risk analysis could identify some suspicious ones there is still room for criminal ones.

Last the globalization and the easy transportation are bringing together the producers and the customers for illicit goods and services. Opiates produced in Afghanistan and t-in the Golden triangle, cocaine from South America, counterfeited goods, substandard products, trafficked women for sex, immigrants for forced labour can be distributed worldwide using failed or weak states, passing through free trade zones or just benefiting from lax control at all levels.

5. Background

5.1. *Current research*

- <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/mafia-structured-crime-areas-and-trends-groups-ocg> Europol regularly completes studies on OC group sociology
- <https://projects.exeter.ac.uk/RDavies/arian/scandals/mafia.html> a continuous research about OC
- <https://www.dur.ac.uk/research/news/thoughtleadership/?itemno=24781> the university of Durham research on the UK model of organized crime when compared to the Italian mafia model.
- <https://blogs.ucl.ac.uk/organised-crime/tag/mafia/> UCL (Jill Dando institute) completes a continuous research on the sociology and rationale of OC organizations worldwide
- <https://www.wilsoncenter.org/publication/the-criminal-diaspora-the-spread-transnational-organized-crime-and-how-to-contain-its> the Wilson center conducts a programme on transnational organised crime and diaspora in Latin and North America

5.2. *Statistics general view*

The reliability of security statistics is questionable. For a long period the figures of reported crimes have been used as indicators, the so called crime rate. Nevertheless the integrity of these figures has been challenged by different factors over the last decades. First victims can avoid to report crimes due to fear of retaliation, limited loss or unavailability of police. Second, the police itself can refuse to register reported crimes to keep good figures. Last, new forms of crime like frauds, cybercrime are not well defined in statistical books and are either ignored or aggregated with other

offenses in a sense it is difficult to have an accurate picture of the situation. Furthermore this gap between figures and reality is called the dark figure of crime and therefore of security. Such a gap exists in official public statistics as well as in private ones because even the members of professional bodies that are dedicated to security are reluctant or have either no time or no resources to fill statistical forms.

Still in the field of statistics European police forces - unlike American ones - have never built statistics on losses (e.g. theft, frauds). On the contrary professional bodies either manufacturers or service providers are usually collecting figures of an economic nature, value of thefts and frauds, losses, missed sales, impact on employment and paid taxes. Insurers are very vigilant on that and have developed their own databases.

To conclude statistics have to be used very carefully; any change of conditions could biased the figures. Furthermore comparisons in different environments could be tricky.

5.3. *Statistics sources*

The main statistical sources are the following:

- <https://www.unodc.org/unodc/en/data-and-analysis/statistics.html>
General thematic and geographical data and statistics with respects to organized crime worldwide
- <http://ec.europa.eu/eurostat/web/crime/overview>
European Union statistics on crime and criminal Justice
- <https://ucr.fbi.gov/>
uniform crime reporting to be offered by the FBI provides a statical view of organized crime in the US with figures and analysis
- <https://www.gov.uk/government/collections/crime-statistics>
crime statistics in the UK
-

5.4. *SUMMARY - Background*

CURRENT RESEARCH AND STATISTICS	
TECHNICAL	<ul style="list-style-type: none"> • Deploying more and more technical solutions • Adressing technical criminal innovation • Statistical tools incl analytics
HUMAN	<ul style="list-style-type: none"> • Immigration and diaspora. • Protective communities
ORGANISATIONAL	<ul style="list-style-type: none"> • Awareness of leadership • Evidence-Based Programs and Practic
REGULATORY	<ul style="list-style-type: none"> • Balancing local versus national competencies.

6. CURRENT POLICIES AND LEGAL FACTORS

Current policies are the outcome of a continuous process that was initiated at the beginning of the XX th century with Interpol and has really developed from the end of this same century. Policies helped to address specific crimes and to define strategic responses

6.1. *Organised crime*

The keystone of international policy against organised crime is the UN Palermo convention against transnational crime that both defines organised crime and the relevant responses (article 2 of the convention) and urges governments to implement its provisions (article 5 of the convention). The convention is the outcome of a three years process. A key advance is that the Convention includes the participation to an OC group as a crime in itself. In terms of policy this has to be seen as key step forward.

At European level the policy against organised crime is elaborated jointly at the EU level and at the level of the council of Europe. The EU policies are to address major OC threats with a view to ensure the security of the Union. This is achieved through multiannual programmes. At operational level the policy is to develop cooperation and to share information. This is mainly the role of Europol. The council of Europe is more in charge of ethical and human rights issues with a view to ensure efficiency of investigations/prosecution and respects of human rights and democratic values.

6.2. *Drugs, Human trafficking, Money Laundering*

International conventions that are elaborated under the auspices of the UN with the support of UNODC are the backbone of major policies to address OC. They are relayed by European instruments and generally reflected in national legislations. As said previously (cf. § 4.3) the rationale that is behind these policies is mixing morale, health, public order and, sometimes, geopolitical considerations. Therefore the relevant conventions have to be seen as highly politicized.

The main topics that have been addressed within this approach are:

- Drugs with an initial convention (Single Convention on Narcotic Drugs) in 1961 to be complemented in 1967 and 1971 (Convention on Psychotropic Substances) and totally refounded in 1988 (United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances).
- Trafficking of human beings for sexual exploitation or forced labour. This is mostly linked with immigration. The policy is reflected by the attached additional protocol to the UN transnational organised crime convention.
- Money laundering policy was initially designed as an indirect strategy to attack drug traffickers on a financial basis. It has been later extended to all benefits from crime. It is driven by the G8/G20 at international level and is generally

managed by the services of the ministries of finance and economy at national level. It relies on instruments like the intergovernmental financial action task force and by the Egmont group of national financial investigation units.

6.3. *Illicit trade*

Illicit trade policies have so far focused on the protection of intellectual property namely addressing counterfeiting and piracy. This is reflected by the trade related aspects of intellectual property rights (TRIPS). Under this international policy counterfeiting and piracy are considered as a serious crime.

Other forms of illicit trade than IP violations or physical property breaches are addressed on an ad hoc basis. This could be done through health, sanitation, and physical security regulations. This later could help to tackle the illicit trade of substandard goods.

Illicit trade is also addressed through some ad hoc international conventions or UNSRC decisions: this is the case for illicit trade of wildlife products or for the trafficking of extracted minerals and materials especially in conflict zones; the Kimberley process is an example of such a policy. It is clear that public authorities and private companies are involved in the fight against these forms of illicit trade.

6.4. *International police and judiciary cooperation*

Over time the need for international police and judiciary cooperation has become obvious. Initiatives have been taken to build the legal and operational framework for that both at international and national levels.

At international levels frameworks have been developed to exchange and more and more share police information with a view to support and drive joint investigations. This is the *raison d'être* of INTERPOL and EUROPOL it is also the rationale of some more limited initiatives like the South Eastern Europe cooperative initiative trans national organised crime centre or the Western Africa police information system (WAPIS) that is being build under the auspices of the ECOWAS.

In the field of judiciary cooperation both for penal and civil matters frameworks are generally built at a regional level or within bilateral agreements. EUROJUST, the European convention on judicial matters, the European arrest warrant are the tools of the European Union policy for judicial cooperation. The goal is to coordinate prosecution and trial with a view to have the criminals being sentenced across borders.

The EU has also a constant policy to integrate the fight against OC in all international agreements it concludes with foreign countries. Justice and home affairs and later security chapters have been present in all agreements of the enlargement policy, of the European Neighbourhood policy, of the development policy and of the stability policy (in post crisis countries). Usually this policy is reflected in the agreement by a joint commitment to address OC efficiently in a democratic way and by the EU

commitment to concretely support the building of institutional and organizational capacities in the beneficiary country.

At national level the initiatives to support international police cooperation rely either on a network of bilateral agreements or on the deployment of police attaches or liaison magistrates. The policy is to exchange information, coordinate investigation, train and support when necessary. A good example of such a policy is made by the FBI legal attaché (LEGAT in fact FBI agents) network and by the French police attaché network.

6.5. *Criminal asset seizure*

In parallel with the money laundering policy the international community and the national government have developed policies of criminal asset seizure. Like money laundering that aims at financial flows the criminal asset seizure aims at criminal assets that are stemming from the profit of crime.

Such policies include orientations about the use of the criminal asset. Generally the outcome of the seizure is shared between the state general budget and the police and the judiciary. Countries like France have established specialised agencies to manage the criminal assets. The French agency AGRASC has managed 920 millions euro over its first six years and is on growing trend.

6.6. *Sources*

- <https://www.un.org/ruleoflaw/thematic-areas/transnational-threats/transnational-organized-crime/> the UN general secretary has developed a general policy on organized crime.
- https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Ebook/The_International_Drug_Control_Conventions_E.pdf
- UNODC booklet to present the different drug control conventions
- http://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf
- UN Convention on transnational organized crime
- http://www.oecd-ilibrary.org/fr/commonwealth/governance/a-guide-to-international-drugs-conventions_9781848594395-en
- OCDE guide on drugs conventions
- <https://www.tni.org/en/collection/conventions-on-drugs>
- transnational institute analysis on the major drugs conventions
- <http://idpc.net/policy-advocacy/global-advocacy/global-drug-control-system/un-conventions-drug-control>
- International drug policy consortium debate on drugs conventions
- <https://www.imf.org/external/np/leg/amlcft/eng/aml4.htm>
- The IMF references for money laundering: context and specific instruments
- https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm
The WTO references about the regulations to protect intellectual property (namely the fight against counterfeiting and piracy)

- <http://www.consilium.europa.eu/en/policies/eu-fight-against-organised-crime-2018-2021/> the EU policy and multiannual programme against organised crime
- https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking_en The European Commission approach and view on OC policies
- <https://www.coe.int/en/web/cdpc> the Council of Europe view on organized crime
- <https://www.coe.int/en/web/transnational-criminal-justice-pcoc/home> the Council of Europe view on Judicial cooperation in criminal matters

6.7. SUMMARY - Policies and regulation

CURRENT RESEARCH	
TECHNICAL	<ul style="list-style-type: none"> • <i>Organizing information exchange/sharing</i>
HUMAN	<ul style="list-style-type: none"> • <i>Training people</i> • <i>Developing a culture of cooperation</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>Reorganizing the OC law enforcement system and governance</i> • <i>Implementing OC policy</i> • <i>Developing international cooperation for police and Justice</i> • <i>Managing change</i> • <i>Developing multidisciplinary approach</i>
REGULATORY	<ul style="list-style-type: none"> • <i>International Conventions Criminalizing major OC threats</i> • <i>Protecting human rights and privacy</i> • <i>Reflecting international conventions at national level</i>

7. CURRENT PRACTICES

The new forms of OC are a constant challenge for public authorities that have to enforce the law and for private companies that could be the victims or the involuntary accomplices of OC. Because the criminals are creative and innovative the public authorities and the private companies managers have to innovate and to imagine new responses to keep on OC. Like in the defence area there is a continuous race between the sword and the shield.

7.1. Undercover operations and controlled deliveries

The first adaptation of practices to the new forms of OC has been to penetrate the universe of organised crime in a discreet manner. This practice covers the undercover operations that allow police officers to penetrate criminal organizations

and even to take an active role inside these same organizations. This includes all criminal activities and especially the delivery of trafficked products. In this context it is necessary to develop a specific legal framework to exonerate the undercover agent from any penal responsibility while on the same time respecting the rights of defence of the criminals.

7.2. Surveillance and tracking

Unlike undercover operations that take place inside criminal organisations surveillance and tracking are observing the criminal activities from outside even if some techniques can be called intrusive they are always without human presence.

Surveillance will be used to monitor activities, movement, meetings, verbal or electronic exchanges and in fact any actions that can be seen, listened or that left a footprint. For a while surveillance has relied on individuals who operate as discreet observers. Now more and more it uses material asset and especially electronic equipment. Surveillance has extended from monitoring movements to monitoring communications. The strategy that lays behind is through the coordination mechanisms of crime to attack the whole criminal activity instead of just a few of its actions.

In the specific case of illicit trade or even in the embedment of criminal activities distant surveillance of movement of goods and even of individuals can rely the block chain technology. This is an innovative technique that is still at its early stage but it appears to have a bright future.

7.3. Private public cooperation

At this stage the public private cooperation has to be underlined.

First the criminal activities to monitor either from inside (undercover) or from outside (surveillance and tracking) would most of the time occur inside private organisations or private space. Consequently the private sector is very often associated to the law enforcement operations for help, assistance and support. Private sector is needed in many undercover operations where they can provide a robust coverture t the agents.

Second the investigation techniques in surveillance, tracking, monitoring of activities need some specialized equipment that are manufactured, provided and sometimes operated by the private sector. This is systematically the case for operations that are ordered by the private sector and this is more and more the case for public investigations. Within the security industry there is a growing number of service and equipment providers that are involved in the fight against organised crime on behalf of private organizations and private companies.

7.4. Criminal analysis

The achievement of a criminal activity has become a complex process inside which members of the criminal organization are playing different roles but with none of them being in a position to be fully guilty neither fully innocent. The adoption of new

regulations that incriminate just the participation to organised crime activities demand that judges, prosecutors and investigators know exactly what is the role of each criminal, how he interacts with others in the completion of crime.

For a while it was based on intuitive approaches. Since the 90s the technology has helped to offer a solution with computerised analytical tools, the most famous of them being IBM/I2 analyst notebook and Palantir. These tools help to identify the exact roles and responsibilities of each individual. They also help to understand the criminal process and to identify its weaknesses therefore providing clues to the investigators and orientations for preventive measures.

With the help of algorithms and artificial intelligence there could be soon dramatic progress in this sector.

7.5. Plea bargaining and cooperative witnesses

Plea bargaining and cooperative witnesses have been developed in the US a few decades ago. These practices are now common in many countries. They are developed at the level of the prosecution. They include the protection of witnesses that covers physical protection, relocation and even a new identity. Once more as discussed previously for undercover techniques the legal difficulty is both to protect the witnesses and to respect de defence rights.

7.6. Sources

- UNODC https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf UNODC manual for criminal analysis
- Interpol <https://www.interpol.int/INTERPOL-expertise/Criminal-Intelligence-analysis> Interpol view of criminal analysis
- UNODC https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf UNODC manual for the use of electronic surveillance in the investigation of serious and organized crime
- UNODC <https://www.coe.int/en/web/transnational-criminal-justice-pcoc/home> UNODC view on special investigative techniques of surveillance and tracking
- HMIC <https://www.justiceinspectores.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf> an HMIC comprehensive study of undercover operations in England and Wales

7.7. SUMMARY – Current practice

CURRENT RESEARCH	
TECHNOLOGY	<ul style="list-style-type: none"> • <i>Developing a wider use of the technology for surveillance and analysis</i> • <i>Make best use of new technologies (Block chains, artificial intelligence)</i>
HUMAN	<ul style="list-style-type: none"> • <i>Undercover operations and agents</i> • <i>Cooperative witnesses to be managed and protected</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>Management of new techniques and practices</i> • <i>Public private cooperation</i>
REGULATORY	<ul style="list-style-type: none"> • <i>Changing criminal procedures to allow new techniques and practices</i> • <i>Continuous respects of criminal's rights especially fair defense</i>

8. THOR' Summary

MASTER'S COURSES ORGANIZED CRIME (OC)	
LEADERSHIP	<ul style="list-style-type: none"> • Understanding the nature of OC the stakes, games and players • Addressing the OC issues in your organization multidisciplinary, creative and analytical and outside with various stakeholder. • Learning to have the overall responsibility of OC matters develop and implement a strategy, manage tasks and assess internal and external security providers, etc. • Personal transformation: being able to operate as a professional executive in the field of OC • Obtaining a systematic approach and provide solutions from a systems perspective, integrating different angles • Develop, support, and enhance writing and verbal communications skills • Weigh and assess common areas of occupational proficiency for security executives: awareness raising investigation and prevention and legal liability. • corporate social responsibility, compliance and integrity
TECHNICAL	<ul style="list-style-type: none"> • Using electronic technology tracking and surveillance • Deploying Information systems: intelligence, alarms and guidance • Deploying analytical tools.

HUMAN	<ul style="list-style-type: none"> • Driving security Staff (management and providers) • Developing general staff security role and capacity (skills, training) • Managing human resources and creating an OC protective climate (corruption free and responsible) • Security/protective culture
ORGANISATIONAL	<ul style="list-style-type: none"> • Organising leadership: hierarchy to integrate OC in the security line (job definition) • Protecting assets : capital and physical, brand and image, IP and know how • Ensuring safety of operations against OC threats especially in procurement, and logistics • Coordinating with law enforcement agencies • Mobilizing partners and developing public private partnerships • Discover and apply tools to be effective in achieving those goals, • Evaluate the origins and current structure of OC management
REGULATORY	<ul style="list-style-type: none"> • Ensuring Property laws • Compliance and vigilance requirements • Respecting privacy (staff and customers/providers) • Learning about differences in legal systems and how to deal with it • Various laws that stress the responsibility of companies
METHODS	<ul style="list-style-type: none"> • Implementing risk analysis (threats, natural and technological hazards, vulnerabilities and interests to be protected) • Completing Strategic analysis (likely and impact, needs and capacities) to assess priorities and define strategic actions • Developing Strategic responses (core, crisis, routine/repetitive and anecdote) • Elaborating Strategic planning (action and support) • Balancing situational prevention vs operational strike response
THREAT	<ul style="list-style-type: none"> • Identifying and measuring the impact of different forms of OC • Identifying and measuring the impact of corruption • Measuring the international dimension of OC
ENVIRONMENT	<ul style="list-style-type: none"> • Understanding international and national OC policies • Liaising with similar organisations and professional bodies that face the same challenges to assess situation and elaborate responses • Raising private public partnerships with authorities and the business community

Reference list

- “The handbook of security” , Martin Gill, Palgrave Mac Millan, 2016
- “The future of policing” , Schafer, Buerger, Myers, Jensen, CRC Press, 2017
- “Ce que fait la police “ D. Monjardet, Odile Jacob 1995
- “the handbook of policing” Tim Newburn , Willan publishing 2005
- “Traité de sécurité intérieureé M Cusson, B Dupont and Frederic Lemieux , cahiers du québec 2007
- “Policing 2020” J A Schafer, Police futurist 2007
- “The new structure of policing” D H Bayley and C D Shearing , National Institute of Justice 2006
- “The review of Policing”, Ronnie Flanagan, Her Majesty Inspectorate Constabulary, 2008
- “ Future Trends in policing” Police executive research forum , 2014
- “Dual Markets” Ernesto U Savona and others , Springer 2017

Annex 6

CYBERCRIME

EACEA Action Grants

Project reference No: 575734-EPP-1-2016-1-NL-EPPKA2-KA

International Security Management Knowledge Alliance (ISM-KA)

Addressing Security Challenges in an Interconnected World



Work Package 2

Cybercrime Module

Deliverable Form	
Project Reference No.	575734-EPP-1-2016-1-NL-EPPKA2-KA
Document Title	WP2 Cybercrime Module
Relevant Work package:	WP2 -
Nature:	Educational Guideline Report
Dissemination Level:	Restricted to the Consortium
Document version:	V01
Date:	July 2017
Authors:	Alison Lyle (CENTRIC)
Document description:	Desk based analysis for Cybercrime

1. Module Descriptor

Module Name	Cybercrime
Module Aim	<p>This module aims to provide the student with the knowledge and skills required to more effectively deal with cybercrime. Developed as a result of extensive research and collaboration with experts across a wide range of domains, this module encompasses identified gaps and specific challenges associated with addressing cybercrime.</p> <p>Rather than focusing on specific, technical capabilities, this module will create awareness and the ability to engage with the issues and principles that are essential to managing preventative measures and responses to cybercrime. Each learning outcome, and the content in relation to it, complements and interacts with others so that at the end of the module a comprehensive and solid knowledge-base is acquired through an iterative approach.</p>
Learning Outcomes	
Successful completion of this module will enable a student to:	
LO1	Understand the current legal landscape in respect of the various aspects of cybercrime and the impact of this.
LO2	Identify the human factors relating to cybercrime, including offenders, victims and investigators.
LO3	Apply digital investigation processes, incorporating best practice in terms of evidence management.
LO4	Employ the various tools, methods and capabilities for cross-jurisdictional working.
LO5	Recognise cybercrime threats and trends and prepare responses to these.
Indicative Content	<ul style="list-style-type: none"> • LO1 <p>The legal landscape in relation to cybercrime incorporates not only offence types, but the powers of investigators, rules relating to evidence, data protection and human rights. The principles and aims underlying these laws provide a holistic understanding of how, when and why they apply. Key European and International legal instruments will also be studied.</p>

	<ul style="list-style-type: none">• LO2 The human elements involved with cybercrime include those relating to carrying out various offences, the impact on and response of victims and the factors present in investigators' responses to this type of crime. The latest research outcomes and criminological theories, as well as an examination of real-life case studies will enable students to learn how to manage the effects of these behaviours. • LO3 The components that make up an investigation of cybercrime will be examined along with an overview of the purpose of these so that unique incidents can be managed effectively. Key components include legal constraints and powers, seizing and managing evidence, criminal justice processes, technical methods and exploiting various resources. • LO4 One of the main challenges in relation to cybercrime is the cross-jurisdictional nature compared to the jurisdictional nature of those dealing with it. This developing area encompasses technological, human, organisational and regulatory factors; the latest policy and practice in each of these areas will be studied. Real-life case studies will form part of this learning and experience. • LO5 The nature, type and purpose of a range of cyber-attacks will be studied. Ongoing horizon scanning feeding into this topic will facilitate analysis of relevant threats and understanding of the ways in which these develop. The modi operandi of the various actors will be studied, along with preventative measures in relation to these.
--	---

2. Current Courses

2.1. Masters Courses

- MSc (University of Portsmouth) Security Management
<http://www.port.ac.uk/courses/law-and-criminology/msc-security-management/>

- MSc (Coventry University) CyberSecurity Management
<http://www.mastersportal.eu/studies/161770/cyber-security-management.html>
- MA (Coventry University) Terrorism, International Crime and Global Security
<http://www.coventry.ac.uk/course-structure/arts-and-humanities/postgraduate/terrorism-international-crime-and-global-security-ma/>
- MSc in Cyber Security (University of Liverpool)
http://edu.university-liverpool-online.com/global/programmes/information-technology/msc-in-cyber-security?comm_code=4427200
- MSc (Walden University) International Security and Global Governance
<http://www.mastersportal.eu/studies/76413/international-security-and-global-governance.html>
- Master in International Security Studies (MISS) Charles University, Prague
<http://fsveng.fsv.cuni.cz/FSVEN-340.html>
- MA (University of Kent, Brussels School of International Studies) International Conflict and Security
<http://www.mastersportal.eu/studies/61896/international-conflict-and-security.html>
- MA (University of Groningen, Netherlands) International Security
<http://www.rug.nl/masters/international-security/>
- International Security Master's Universitat Autònoma de Barcelona
<http://www.mastersportal.eu/studies/34642/international-security.html>
- International Security MA Sciences Po, Paris
<http://www.mastersportal.eu/studies/152070/international-security.html>
- MA in Cybercrime Investigation University of Central Lancashire
http://www.uclan.ac.uk/courses/msc_cybercrime_investigation.php
- MSc Cybercrime and Digital Investigation Middlesex University London
<http://www.mdx.ac.uk/courses/postgraduate/cybercrime-and-digital-investigation>
- Master's in cyber security accredited by National Cyber Security Centre (part of GCHQ)
<https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0>

2.2. Professional Training

- ASIS certification for professional excellence (CPP, PCI, PSP)
<https://www.asisonline.org/Certification/Pages/default.aspx>
- ISMI - the International Security Management Institute and Certified Security Management professional (CSMP) Level 6 Diploma, accredited by Industry Qualifications (IQ)
<https://www.ismi.org.uk/csmp/the-ismi-professional-assessment-board.aspx#.WPdjhWIrJtR>
- Certificate in Security Management (BTEC level 3)
<https://www.security-institute.org/qualifications/certificate>
- Security Institute Diploma in Security Management (BTEC level 5)
<https://www.security-institute.org/qualifications/diploma>
- The Security Institute qualifications for practitioners in security
<http://www.perpetuitytraining.com/syisecurityinstitute.html>
- International Security Management Institute
[https://www.ismi.org.uk/membership/fellows-of-the-international-security-management-institute-\(fismi\).aspx#.WPfHqvnyuUI](https://www.ismi.org.uk/membership/fellows-of-the-international-security-management-institute-(fismi).aspx#.WPfHqvnyuUI)
- International Professional Security Association
<http://www.ipsa.org.uk/>
- College of Policing (UK) Digital forensics Managers' workshop
<http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-Forensics-Managers-Workshop.aspx>
- College of Policing (UK) Digital and Cybercrime Training
http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx
- CCL academy (UK, Middle East & Africa) CISI - Managing Cyber Security (for non-technical and managerial, suitable for all sectors (public and private)
<https://www.cclacademy.com/courses/96/cisi-managing-cyber-security/>
- CEPOL (European Union Agency for Law Enforcement Training) 25/2017 Cybercrime –
conduction forensic searches in various IT devices
<https://www.cepola.europa.eu/education-training/what-we-teach?page=16>

2.3. CPD Courses

- CISI (Chartered Institute for Securities and Investment) provide training and CPD programmes to support financial industry in fight against criminals.
<http://www.cisi.org/cisiweb2/cisi-website/misc-pages/Financial-Crime-and-Cyber-Security-CPD-Opportunities-for-you-and-your-Firm>
- ICAEW provide online courses in cyber security and CPD courses for accountants, unknown whether the two coincide
<http://www.icaew.com/en/technical/information-technology/cyber-resource-centre>
- Institute of Information Security Professionals
[https://www.iisp.org/imis15/iisp/About Us/Our Mission/iispv2/About us/Our Mission.aspx?hkey=9a43cc5c-8b71-4770-bfa9-d60e5c7b3ba9](https://www.iisp.org/imis15/iisp/About%20Us/Our%20Mission/iispv2/About%20us/Our%20Mission.aspx?hkey=9a43cc5c-8b71-4770-bfa9-d60e5c7b3ba9)

3. Stakeholder Perspectives

3.1. Institutional Bodies

- Legislative Systems & Data Protection
- Organisational and Societal Resilience
- Political agreements that frame and cover the work of agencies all over the world
- Appreciation of (international) legal framework to secure proper balance between privacy and security
- Sentences that reflect impact of crime (as a deterrent and to reflect investigation resources invested)
- Appropriate legislation
- Education of general public to provide understanding of how to avoid falling victim to cybercrime
- Create, support and maintain partnerships across sectors, jurisdictions and boundaries for more efficient information sharing and to overcome jurisdictional issues
- Development and implementation of policies related specifically to cybercrime
- International rules of engagement

- Legal framework is insufficiently equipped to create an effective deterrent
- Anonymity of cybercrime, compounded by cross-jurisdictional nature, causing confusion as to which is responsible for investigation and prosecution
- Legal differences and international cooperation
- Cybercrime is legitimised by various regimes as a political instrument. This creates moral and motivational ambiguity for authorities to address the problem.
- Critical infrastructures are also particularly vulnerable. Therefore, a close cooperation between the security authorities and the business and the scientific partners is very important.

3.2. Law Enforcement

- Enhancing the Capability of Investigators
- recruiting IT specialists; up to date relevant technology; up to date relevant knowledge; collaboration with external experts; technical attribution (IP address to suspect)
- Understand economic drivers to create effective deterrence measures
- Strong understanding of legal issues associated with cybercrime and gathering / presenting digital evidence
- Correct training of investigators and recruitment of capable personnel
- Collaboration / centres of excellence
- Sharing threat intelligence
- Future-proofing current technology and investing in new technologies
- Adapting as quickly as cybercriminals
- Significant economic drivers to cybercrime. Present low-risk; high-reward equation is an ineffective deterrent.
- Identify the potential harm and risk of offences and how much is at stake, in monetary terms.

- Development of cybercrime into large-scale, lucrative opportunity for complex cybercriminal networks to commit crimes on unprecedented scale. Involves experts; highly organised and calculated activities leaving limited room for errors.

3.3. *Businesses And NGOs*

- Facebook launching tools to tackle revenge porn
<https://www.theguardian.com/technology/2017/apr/05/facebook-tools-revenge-porn>
- Esteves, J; Ramalho, E; De Haro, G. 'To Improve Cybersecurity, Think Like a Hacker' *MIT Sloan Management Review* 58.3, Spring 2017, pp 71-77
<http://search.proquest.com/docview/1885859523?pq-origsite=gscholar>
- Awareness, Education and Training
- Technological Evolution
- Cooperation and Information Exchange
- Aggressive upskilling of ICT professionals to create competent workforce in order to create and reconstruct software, networks and systems that are robust and resilient to cyber attack.
- Overly complex software and systems, rushed to market, without due consideration of early and integrated security led to vulnerable systems, easily exploited.

4. Background

4.1. *Current Research*

- NATO Cooperative Cyber Defence Centre of Excellence - new study published April 2017 reveals vulnerabilities in the Most Widespread Network Security Solutions
<https://ccdcoe.org/new-study-reveals-vulnerabilities-most-widespread-network-security-solutions.html>
- CCDOE (2017) Hedgehog in the Fog: Creating and Detecting IPv6 Transition Mechanism-Based Information Exfiltration Covert Channels
<https://ccdcoe.org/multimedia/hedgehog-fog-creating-and-detecting-ipv6-transition-mechanism-based-information.html>
- Call for papers for 2017 International conference on cyber Conflict U.S. (CyCon U.S.) - deadline 10 July 2017. Conference on 7-8 November in Washington DC

<http://aci.event.com>

- 9th International CyCon (Tallinn 30 May - 2 June 2017) - international cooperation and conflict in cyberspace, technical challenges and requirements, legal frameworks, regulations and standards etc. General topic Defending the Core)
www.cycon.org
- Cyber Power Conference 2016 materials, focusing on theme of Cyber Power, now available as part of IEEE publication
www.cycon.org.
- Clark, R & Hakim, S. (eds) (2017) 'Cyber-Physical Security: protecting infrastructure at the State and local level' Switzerland: Springer International Publishing. (US perspective)
<http://www.fox.temple.edu/cms/wp-content/uploads/2016/08/Cyber-Physical-Security-PDF.pdf#page=197>
- RLD Pool & BHM Custers (2017) 'The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime' *European Journal of Crime, Criminal Law and Criminal Justice* Vol. 25, Issue 2, pp 123 - 144
<http://booksandjournals.brillonline.com/content/journals/10.1163/15718174-25022109>
- Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D & Apostolopoulos, T. 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of the Tallinn Manual' *Computers & Security* 12 April 2017
<http://www.sciencedirect.com/science/article/pii/S0167404817300822>

4.2. Statistics

- PriceWaterhouseCoopers 'Global Economic Crime Survey' 2016 study revealing extent of cybercrime
<http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html>
- RSA '2016: Current State of Cybercrime'
<https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf>
- UK Office for National Statistics 'Overview of fraud statistics: year ending Mar 2016'
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016>

- Crime Survey for England and Wales 2016
<http://www.crimesurvey.co.uk/SurveyResults.html>
- Cyber Security Breaches Survey 2017 (Ipsos MORI Social Research Institute)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf
- National Cyber Security Centre (part of the UK's GCHQ); Weekly threat reports.

4.3. Reports

- Cisco 2017 Annual Cybersecurity Report
http://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html
- UK National Cyber Security Centre 2017 report on criminal online activity
<https://www.ncsc.gov.uk/topics/cyber-attacks>
- European Union Serious and Organised Crime Threat Assessment 2017
<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>
- NCA (National Crime Agency) 'Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime'
<http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file>
- ETL 2016 (enisa current and emerging threat landscape report, published February 2017)
<https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2016-report-cyber-threats-becoming-top-priority>
- RUSI 'Financial Institutions and Cybercrime: Threats, Challenges and Opportunities' research paper July 2016
https://rusi.org/sites/default/files/2016_newsbrief_july_de_oliveira_and_stickings.pdf
- PPR Paralegal report: '5 Cyber Watchpoints for 2017: what's in store for cyber security around the world?' (Australia, Central South America, China, EU, Russia, United Arab Emirates, UK, USA)
http://www.lexology.com/library/detail.aspx?g=f0affac1-03bf-43e0-9dc9-dc7b9a790431&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+%20+General+section&utm_campaign=PPR+IOP+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2017-01-31&utm_term=

- Reform report: ‘Bobbies on the Net: a police workforce for the digital age’ (Report addressing issues around policing cybercrime)
<http://www.reform.uk/wp-content/uploads/2017/08/Bobbies-on-the-net.pdf>
- Information Age (website with many reports and surveys, carried out by various bodies and organisations, all related to cyber security)
<http://www.information-age.com/levels-scratching-surface-required-stem-skills-123467998/>

5. Current Policies

5.1. Governments & Institutions

- Global strategy on foreign and security policy for the EU
http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
- UN Security Council Resolution 2347 (2017) 24 March
[https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2347\(2017\)](https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2347(2017))
- United Nations: Inter-Agency Security Management Network (IASMN)
<http://www.unsystem.org/content/inter-agency-security-management-network-iasmn>
- EU Policy Cycle (EMPACT) - cybercrime is listed as one of nine 'priority areas'. Current policy cycle ends in 2017
<https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>
- Enisa 'Cyber Security Strategy 2014 - 2017'
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf
- CCDCOE (NATO cooperative Cyber Defence Centre of Excellence - Tallinn, Estonia)
<https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>
- Cybersecurity Strategy for the European Union
<https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>
- European Agenda on Security
http://europa.eu/rapid/press-release_IP-15-4865_en.htm
- UK Government: Policy Paper 5: A safe and secure cyberspace – making the UK the safest place in the world to live and work online

<https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online>

5.2. *Industry*

- Privacy Enhancing Technologies: Evolution and State of the Art (enisa document guiding developers and others to build and maintain PETs)
<https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art>
- SHIELD project proposing universal solution for dynamically establishing and deploying a virtual security infrastructure into ISP and corporate networks (EU funded H2020, began 2017)
<https://ec.europa.eu/digital-single-market/en/news/universal-security-infrastructure-isps-and-corporate-networks-using-nfv-enabled-technologies>
- Report prepared by European Commission's Energy Expert Cyber Security Platform Expert Group, proposing analysis of potential threats to cybersecurity within the EU and how to combat them, also encouraging EU energy regions to cooperate and share information about cyber risks
<https://ec.europa.eu/digital-single-market/en/news/cybersecurity-energy-sector>
- Outputs from 'Functional safety & cybersecurity workshop in Brussels, 16 March 2017 (stakeholder engagement workshop)
<http://www.cvent.com/events/functional-safety-cybersecurity/event-summary-15cbf692ff4748d2a291b3b1540d2b1d.aspx>
- GLACY (Global Action on Cybercrime) 'Strategic priorities for cooperation on cybercrime and electronic evidence in GLACY countries (adopted at close of GLACY project, Bucharest, October 2016)
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b57b4>

5.3. *Law Enforcement*

- Interpol 'Global Cybercrime Strategy'
<https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>
- University of Birmingham 'Cybercrime workshop: Better Policing Collaborative (BPC)' 27 March 2017 (Home Office, College of Policing, Higher Education Funding Council for England, Police Knowledge Fund, Better Policing Collaborative, Centre for Crime, Justice and Policing, University of Birmingham, University of Derby)

<http://www.birmingham.ac.uk/schools/business/events/2017/03/cybercrime-workshop-bpc.aspx>

- Europol - EMPACT policy cycle (2013 – 2017) Cybercrime is key priority
<https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>

6. Current Practice

6.1. EU

- Cyber Europe 2016 'stronger together' (cyber-security exercise - large scale, distributed technical and operational exercise involving 300 stakeholder organisations).
<https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016>
- European Audit Committee Leadership Network discussion in May 2015
http://www.tapestrynetworks.com/initiatives/corporate-governance/global-audit-committee-leadership-networks/upload/Tapestry_EY_EACLN_May15_View45.pdf
- Europol: 'Unique Police2peer Initiative Combats Child Sexual Exploitation and Abuse Online' (press release)
<https://www.europol.europa.eu/newsroom/news/unique-police2peer-initiative-combats-child-sexual-exploitation-and-abuse-online>
- European Commission Public-Private Partnership on cybersecurity (part of the EU cybersecurity strategy, signed in July 2016)
<https://ec.europa.eu/digital-single-market/en/cybersecurity-industry>

6.2. International

- United Nations General Assembly paper: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - indication of current issues (in 2015)
<https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf>
- International Code of Conduct for Information Security (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan) submitted to United Nations in 2015
<https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>
- Locked Shields 2017 (24-28 April) largest and most advanced international live-fire cyber defence exercise in the world. Reflecting on the key trends in cyber-security, emphasis on specialised systems. 800 participants from 25 nations taking part.
<https://ccdcoe.org/largest-international-technical-cyber-defence-exercise-world-takes-place-next-week.html>
- Interpol (including Global Complex for Innovation in Singapore; a cutting edge research and development facility, opened in 2014, leverages global cyber-expertise from law enforcement and key private sector partners)

directive

- The Budapest Convention (Council of Europe’s only legally binding cybercrime legislation)
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf
- Joint communication to the European Parliament and the Council, ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’ European Commission (High Representative of the Union for Foreign Affairs and Security Policy) Brussels, 13.9.17, JOIN(2017) 450 final
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&from=EN>
- The Rome Declaration (Joint statement of 4 objectives to achieve a safe and secure Europe)
http://www.consilium.europa.eu/press-releases-pdf/2017/3/47244656633_en.pdf
- Report from the Commission to the European Parliament and the Council on the evaluation of the European Union Agency for Network and Information Security (ENISA), Brussels 13.9.2017, COM(2017)478 final
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-478-F1-EN-MAIN-PART-1.PDF>
- Proposal for a Regulation of the European Parliament and of the Council on ENISA the “EU Cybersecurity Agency” and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”), Brussels 13.9.2017, COM(2017) 477 final, 2017/0225 (COD)
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF>
- Executive summary of the Impact Assessment accompanying the above document:
<https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-501-F1-EN-MAIN-PART-1.PDF>
- Communication from the Commission to the European Parliament and the Council; Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, Brussels 13.9.2017, COM(2017) 476 final
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-MAIN-PART-1.PDF>
- Annex to the above document:
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN->

[ANNEX-1-PART-1.PDF](#)

- Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Brussels 13.9.2017, COM(2017) 474 final
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-474-F1-EN-MAIN-PART-1.PDF>
- University of Essex (2017) 'EU-Japan Security Cooperation: Challenges and Opportunities' (A project co-funded by the University of Essex and the Erasmus+ Programme of the European Union)
http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf

7.3. International

- United Nations General Assembly *Resolution adopted by the General Assembly on 23 December 2015: 70/237 Developments in the field of information and telecommunications in the context of international security.*
<https://ccdcoe.org/sites/default/files/documents/UN-151223-ITIS.pdf>
- 'The Tallinn Manual 2.0' - launched in February 2017, this is the most comprehensive analysis of how existing international law applies to cyberspace. Authored by 19 international law experts, an influential resource for legal advisers dealing with cyber issues. Drafting of manual facilitated and led by NATO Cooperative Cyber Defence Centre of Excellence
<https://ccdcoe.org/tallinn-manual.html>

8. Current Courses

8.1. Master Programmes

- Identity & collective violence
- Gender & terrorism
- Science, technology and national security policy
- Protection of sensitive information
- Protection of information
- Video surveillance
- Introduction to cybersecurity
- Cybercrime
- Security architecture and network defence
- Cryptosystems and data protection
- Information risk management and governance
- Digital forensics

- Cyber intelligence and operations
- Cyber-physical systems
- Enterprise & cyber security
- Wide range of cyber security issues
- Advanced understanding of theories and protocols that underpin contemporary cyber security
- Develop ability to deploy effective solutions to real-world cyber security challenges
- Acquire knowledge to conduct effective investigations into suspected cyber attacks
- **Cybercrime investigation techniques**
- **Trends in cybercrime** (Develop ability to find and evaluate the value of cybercrime for criminals. Methods, techniques and emerging technologies of cybercriminals)
- **Behavioural dynamics of cybercrime** (Includes current understanding of offender and victim characteristics and associated investigative issues)
- **Digital forensic technology** (technical issues involved in the handling of electronic evidence)
- **Policing cybercrime** (Proactive and reactive investigation of cybercrime at local / national level; includes working with partners and alternative strategies to prosecution such as prevention, intervention and disruption)
- **Open source internet investigation**
- **Corporate compliance and financial crime prevention** (regulatory compliance and financial crime in corporate environments. Techniques to manage compliance, mitigate risks and investigate financial crime)
- **Cybercrime and society** (History, nature and patterns of cybercrime; theories relating to information technology and social harm)
- **Digital investigation and evidence management** (Evidence management, relationships between digital technology and investigation. Strategic approaches to investigations)
- **Researching cybercrime and legal frameworks** (Critical introduction to legal issues and contemporary methods in researching cybercrime)
- **Computer network and internet security**
- **Computer science for cyber security** (security fundamentals (principles of secure design, threats and attacks, cryptography, security architecture)
- **Secure programming** (defensive programming, memory corruption, user and kernel space vulnerabilities etc)

8.2. *Professional Development Courses*

- **ASIS International security certifications**; CPP (Certified Protection Professional - Board certification in security management), PCI (Professional Certified Investigator - board certification in investigations) and PSP (Physical Security Professional - board certification in physical security) credentials are recognised world-wide.
 - The CPP requires proof of knowledge and management skills in seven key domains of security.

Security principles and practices (includes:)

- a. Security industry standards
- b. Vulnerability, threat and impact assessments**
 - c. Potential security threats (all hazards, criminal activity)
 - d. Risk mitigation strategies
 - e. Risk mitigation techniques
 - f. Data collection and trend analysis techniques
 - g. Elements of a security awareness programme (including communication risk, privacy)

Business principles and practices (includes:)

- h. Confidential information protection techniques and methods

Investigations (not necessarily criminal, but includes:)

- i. Evidence collection techniques
- j. Protection / preservation of crime scene
- k. Requirements of chain of custody
- l. Methods for preservation of evidence
- m. Laws pertaining to the collection and preservation of evidence
- n. Surveillance techniques
- o. Technology / equipment and personnel to conduct surveillance
- p. Laws pertaining to managing surveillance processes
- q. Techniques, tools and resources related to:
 - i. Financial and fraud related crimes
 - ii. Intellectual property crimes
 - iii. Arson and property crimes
 - iv. Cybercrimes
- r. The nature of non-verbal communication and cultural considerations
- s. Statutes, regulations and case law governing or affecting the security industry and the protection of people, property and information
- t. Criminal law and procedures

Information Security

- u. Elements of an information security program, including physical security, procedural security, information systems security, employee awareness, and information destruction and recovery capabilities
- v. Risk mitigation strategies (e.g. technology, personnel, process, facility design)
- w. Protection technology, equipment and procedures
- x. Information security threats
- y. Information security theory and terminology
- z. Information security industry standards
- aa. Relevant laws and regulations regarding records management, retention, legal holds and destruction practices
- bb. Practices to protect proprietary information and intellectual property

- cc. Protection measures, equipment, and techniques; including information security processes, systems for physical access, data control, management and information destruction.
- dd. Elements of information asset protection including confidentiality, integrity and availability, authentication, accountability, and audit ability of sensitive information and associated information technology resources, assets and investigations
- ee. Information security theory and systems methodology
- ff. Multi-factor authentication techniques
- gg. Threats and vulnerabilities assessment and mitigation
- hh. Ethical hacking and penetration testing techniques and practices
- ii. Encryption and data masking techniques
- jj. Systems integration techniques
- kk. Cost-benefit analysis methodology
- ll. Project management techniques
- mm. Cost-benefit analysis methodology
- nn. Project management techniques
- oo. Budget development process
- pp. Vendor evaluation and selection process
- qq. Final acceptance and testing procedures, information systems, assessment and security programme documentation
- rr. Protection technology, investigations and procedures
- ss. Training and awareness methodologies and procedures

Crisis Management

- tt. Threats by type, likelihood of occurrence and consequences
- uu. Triage and damage assessment techniques
- vv. Communication techniques and notification protocols
- ww. Short and long term recovery strategies

Many, many other tasks and modules covering all types of security management - the above relate only directly to cyber.

The above qualification requires:

- Nine years of security work experience, with at least three of those years in responsible charge of a security function

OR

- A bachelor's degree or higher and seven years of security work experience, with at least three of those years in responsible charge of a security function.
- **CEPOL** is the European Union Agency for Law enforcement and provides many training courses for practicing professionals. Among these are:

- **25/2017 Cybercrime** – conducting forensic searches in various IT devices. Enhances skills in the cyber forensics area related to recovery of digital evidence or data from IT devices, in particular mobile devices and internet of things; to share experience on computed data analysis, technical aspects of internet investigations and examination of electronic devices.
- **23/2017 First responders and cyber forensics** – development of practical skills regarding the methodology used in digital forensics for identifying and responding effectively at the scene of cybercrime cases. Further develops the cooperation between law enforcement and European and international organisations regarding investigative methods and policies in the field of cyber forensics. Practical skills at computer forensics to reveal and investigate traces of cybercrime. Harmonise investigative methods between LEAs on how to intervene on the crime scene in case of cyber incidents and dealing with digital evidence.
- **95/2017 Cyber security and cyber defence** – enable understanding of the extensive nature of information society and recognise its complexity and different threats as well as basic notions and concepts related to cyber security. Trends in cyber threats. Overview of technological tools. Familiarity with international cyberspace issues and cyber diplomacy. Evaluate potential impacts of cyber security on public policies. Understand challenges in planning in respect of cyber threats.

8.3. *Continuing Professional Development Courses*

- **Institute of Information Security Professionals**

Offers an Accredited Training Scheme, which assesses training courses offered by commercial training providers against the Institute's Skills Framework V2. IISP accreditation means that course materials and content have been assessed to ensure that they meet the stated objectives of the course and that the course meets the competency levels claimed by the provider.

Sample courses

- Certified Application Security Tester (7Safe)
- Certified Security Testing Professional (7Safe)
- Certified Malware Investigator (7Safe)
- Certified Forensics Investigation Practitioner (7Safe)
- Certified Data Collection Technician (7Safe)
- Information Assurance (various)
- Risk management (various)
- Certificates in Information Assurance Architecture (InfoSecSkills)
- Introduction to Cyber Security (Open University)
- Cyber Security the Insider Threat (Templar Executives)
- Certificate in Information Security Management Principles (URM)

- Practitioner Certificate in Information Risk Management (URM)

8.4. Summary - Current Courses

MASTER'S COURSES	
TECHNICAL	<ul style="list-style-type: none"> • <i>Science, technology & national security</i> • <i>Video surveillance</i> • <i>Security architecture and network defence</i> • <i>Cryptosystems and data protection</i> • <i>Digital forensics</i> • <i>Investigation techniques</i>
HUMAN	<ul style="list-style-type: none"> • <i>Identity and collective violence</i> • <i>Gender and terrorism</i> • <i>Acquire knowledge to conduct effective investigations into suspected cyber attacks</i> • <i>Develop ability to deploy effective solutions to real world cyber security challenges</i> • <i>Understanding of criminal and victim characteristics</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>Protection of sensitive information</i> • <i>Information risk management and governance</i> • <i>Cyber intelligence and operations</i> • <i>Discover alternative strategies to prosecution, such as prevention, intervention and disruption.</i> • <i>Harmonisation of investigative methods</i> • <i>Cooperation at national, EU and international levels in respect of cyber forensics</i>
REGULATORY	<ul style="list-style-type: none"> • <i>Lawful investigations</i> • <i>Police and surveillance law</i> • <i>International agreements and conventions</i> • <i>European collaborative working arrangements</i> • <i>Laws relating to digital evidence and procedure</i>

PROFESSIONAL DEVELOPMENT COURSES	
TECHNICAL	<p><i>Technology is addressed in each of the domains within the ASIS certifications. Various modules cover practical methods of securing information and systems; understanding surveillance technology; methods and strategies relating to recovery of systems and data and encryption techniques. CEPOL have a number of practical courses that specialise in particular skills, such as recovering evidence, examining devices, malware, investigating IP addresses. The courses available with IISP accreditation focus largely on information security and</i></p>

	<i>technical capabilities / skills.</i>
HUMAN	<i>Human aspects of cybercrime are covered in all the domains; creating awareness of risks and strategies pertaining to cyber security, analysing trends and information management. Skills required to conduct effective investigations and understand evidential requirements play a significant part of the education. Also included are communication skills so that employees can be trained and made aware of risks and mitigation strategies. Knowledge of impact on society, as well as understanding the nature and characteristics of offenders and victims is also focused upon.</i>
ORGANISATIONAL	<i>Many of the modules relate to organisational factors. In particular, creating effective risk mitigation strategies, identifying vulnerabilities in systems, achieving industry standards for cyber security, creating general awareness and adopting best practice techniques by incorporating every area of business in the identification and analysis of risks. Collaborative and cooperative working is incorporated as a theme throughout and is highlighted as an important success factor.</i>
REGULATORY	<i>Regulatory factors play an important part of the professional development programmes. The domain addressing investigations requires participant to gain understanding of laws pertaining to evidence, surveillance processes and intellectual property. Additionally, statutes, regulations and case law affecting the security industry more widely are included. Laws relating to information security, records management and legal holds also form part of the courses. International agreements, policies and strategies also fall within this area.</i>

9. Stakeholder Perspectives

A summary of all end-user engagement activities identified the following research topics (areas of priority or particular challenge):

9.1. Enhancing capability of investigators

Improvement of mechanisms to identify perpetrators in response to changing criminal tactics and technological developments, such as connection encryption, use of darknets, crypto currencies and other complexities; archaic and slow information sharing mechanisms internally and across agencies and borders mean that investigators are unable to match the agility and dynamism of attackers; availability and organisation of specialist skills. Balance between centralising domain specific knowledge into specialist units vs. dispersing it throughout police; analysis and evaluation of skills and resources needed within the police; assessment of the impact of the proliferation of cybercrime into other forms of criminality in regards to identifying skill gaps and requirements; implementation of improved and more visible reporting mechanisms for citizens and private sector organisations; clarity regarding

accountability of cybercrime and cyberterrorism issues requires clear and harmonized classification of concepts; assessment and evolution of existing practices, such as search and seizure policies in order to ensure their applicability and suitability in cybercrime cases.

Cooperation and information exchange

Public / private and inter-agency: identification of mechanisms and approaches to incentivise cooperation from the private sector to improve resilience of all stakeholders; establishment of trust and cooperation that synthesises the protection of business interests with protection of the state and its citizens. Currently some sectors underwrite losses due to cybercrime with insurance and do not disclose them; multilateral, as opposed to bilateral approaches to cooperation; establishment of robust communication lines and contact points between public and private sector, such as ISPs and other service providers; fostering the environment of shared responsibility and trust; assessment of voluntary v. mandatory cooperation approaches - at what level does cooperation realistically need to be targeted?; identification of clear frameworks, training, financing and prioritisation at national and policy levels for cooperation; assessment of privacy, human rights and data protection implications of such approaches; results and incentivisation of ENISAs NIS Public-Private Information sharing platform; information requesting processes between LEAs both nationally and internationally are considered slow and archaic. Furthermore, 'protective marking' of documents is over-estimated, unnecessarily impeding access to information; assessment of the information-sharing ecosystem in order to analysed the complexities of the actors, requirements and governance structures.

International Cooperation: specifically a priority for cooperation between international intelligence agencies regarding issues of cyberterrorism; assessment of different international approaches including legislation and policy towards harmonisation of international approaches, especially between member states; LEAs are heavily impacted by geographical jurisdiction, which disempowers responders, approaches needed to minimise this impact in order to 'level the playing field'; if political intervention is required, where and how can this be pitched - who are the key stakeholders in this context?; requirement for inclusion: non-inclusive cooperation creates crime 'safe-havens'; networking and sharing of best practices between countries; the role of international bodies as facilitators of improved cooperation, what mechanisms are currently being undertaken, and could be realistically undertaken in the future by organisations such as EUROPOL and Interpol to foster improvement in this areas. Specifically the function and effectiveness of the EC3 within the EU.

Organisational and societal resilience

Priority identified as improving the all-round resilience of organisations (specifically critical infrastructure) and society as a whole. Components of this priority share significant overlap with other categories, however there are sufficient other points that justify the separation of this issue. Organisational and societal resilience in terms of cybercrime is not only an issue of cyber-security, but a question of overall organisation and industry resilience. The entire supply network and its linkages have to be assessed. Employees, their practises and the greater supply networks they fit within pose an equal if not greater threat to the integrity of critical infrastructures. This poses issues in terms of regulation, as it's not currently possible to regulate the entirety of cyberspace and so there is scope for research in order to effectively

regulate and protect the supply networks of critical infrastructure. Key areas: improved risk and impact assessment in terms of cybercrime resilience, and research; accreditation and standardisation of risk assessment processes and overall resilience against cybercrime and cyberterrorism threats; risk and impact assessment of cyberterrorism as a facet of critical infrastructure protection and all round societal resilience; improved and increased consideration of cybercrime as one facet of overall organisational resilience concepts and best practices; improved governance of IT systems and human practices, not only within specific organisations, but also in extended supply networks; appreciation of human and organisational factors, including responsibility segregation, culture, employees (wellbeing, turnover and practice) etc. ; the cost of prevention v. recovery, readdressing resource allocation to focus on prevention.

Legislative systems and data protection

The compatibility of law is important in establishing international inclusion and can result in tangible trans-border benefits. Law and policy is also important factor in addressing other key challenges, such as in improving trans-border access to data. In order to speed up access and simultaneously protect privacy and human rights legal appropriate legal assistance is required. The way in which law is applied is also a significant factor in how effective it is as although in many instances there is an awareness that law exists, such as in response to media piracy, it does not have a huge impact on behaviour due to low level of prosecution. In response, the key priority identified is for research into the requirements for policy and law in order to combat cybercrime effectively, but also how to integrate these frameworks and mechanisms into practice for maximum positive impact. A number of key issues have been identified in this respect: feasibility assessment for the harmonisation of the application of laws across member states e.g. in the digital forensics, and search and seizure policies of ruse in court, at what level can these be pitched? ; improving the availability of specialist legal expertise; identification of the role of research in these contexts; legal and policy for support for other research priorities, such as improved cooperation, internationally and between public and private sectors, and the prioritisation of cybercrime and cyberterrorism in national and international policing and security strategies; assessment on the impact of technology in the suitability and applicability of laws, especially consideration of privacy and data protection; the role of legal systems and policy in re-establishing public trust in response to recent claims over government surveillance and coercion of private sector into providing 'backdoors' into software systems.

Data protection and privacy: identifying and implementing the balance between the right to privacy and LEAs requirements for data access in order to investigate effectively; the role of data protection in information sharing mechanisms, the integration of international approaches and the balance between protecting the integrity of data and the privacy of individuals and meeting the information sharing requirements of LEAs; approaches to ensuring public confidence in privacy and data protection mechanisms and the impact of technological advancements on public data protection requirements. Use of social media, open source and big data analytics etc.; impact of how events are reported on public perceptions and the subsequent behaviours. Public distrust and perceptions of impunity drive uptake and development of tools and methods to increase privacy and anonymity;

establishment of international best practices based on the assessment of existing international approaches.

Awareness, education and training

increasing the awareness and education of stakeholders is considered to be an important first step in improving the all-round resilience of society. A key requirement in this context is to research the best mechanisms and approaches to improving and increasing education and awareness not only in a public setting, but also across private sector organisations and the public sector - including aspects such as judicial training. Awareness is also an issue on individual and organisational scale, with training presenting a vector to improving data handling practices and basic security safeguards such as password management, practices which would go some way to preventing a range of cybercrime incidents. The following issues have been identified in this respect: increased awareness of and incentivising reporting and cooperation at all levels, from citizens, to large private-sector organisation; integration within national policing strategies and identification of quantifiable objectives in order to acquire funding; potential for mechanisms in terms of standardisation and accreditation of training for LEA specialists, judicial members, the private sector and citizens; identification of appropriate approaches to increase overall societal awareness and resilience, including citizen education to promote uptake of basic skills and security best practices to improve online safety; organisational education, to improve best practice and increase awareness of factors such as employee wellbeing as a cyber-security risk; identification of clear education and awareness requirements and objectives that can be identified as part of government strategies; increased awareness and education as a proactive measure, and its potential to re-address the balance between reactive and proactive expenditure.

Technological evolution

the following issues and research topics were identified in relation to growing use of technology and the risks and benefits that involves: investigation into the use, development and impact of anonymisation techniques, especially in relation to their impact upon the effectiveness of criminal investigations, and the development of approaches that impact upon their investigative abilities; application of analytics, particularly from big-data, open sources and environment scanning in order to rationalise incoming data streams; more effective detection capabilities and sensory networks; prevalence and risk of legacy systems in industrial settings and their extended supply networks; priority and requirement assessment for improved detection mechanisms as industrial control systems have different requirements to IT networks; the proliferation of cybercrime into all forms of criminality; the human impact of technology, such as changes in user behaviour due to perceptions of anonymity; data and information visualisation - improving representation so that it can be interpreted, validated and ultimately used as part of investigations and prosecutions.

9.2. Erasmus+ Advisory Board

Further, to the work done already, the ISM-KA Advisory Board has also provided opinions on challenges / contributions to LEA's tackling various areas. Under the heading of 'Cybercrime' the range of answers can be placed into the following topics:

Technological

Contributors: recruiting IT specialists; up to date relevant technology; LEA's have to keep up with technological developments in order to fight cybercrime; technical knowledge and / or collaboration with external experts; aggressive upskilling of ICT professionals to create a workforce that is cybersecurity competent in order to create and reconstruct software, networks and systems which are robust and resilient to cyber-attack.

Challenges: future-proofing current technology and investing in new technologies; cybercriminals adapt more quickly and have greater resources; overly complex software and systems, rushed to market, without due consideration of early and integrated security led to vulnerable systems, easily exploited

Financial

Contributors: understanding economic drivers to create effective deterrence measures; economy of scale

Challenges: significant economic drivers to cybercrime. Present low-risk: high-reward equation is an ineffective deterrent; identify the potential harm and risk of offences and how much is at stake, in monetary terms; development of cybercrime into large-scale, lucrative opportunity for complex cybercriminal networks to commit crimes on unprecedented scale. Involves experts, highly organised and calculated activities leaving limited room for errors; challenge to enhance success and lower cost.

Political

Contributors: political agreements that frame and cover the work of agencies all over the world

Challenges: cybercrime is legitimised by various regimes as a political instrument. This creates moral and motivational ambiguity for authorities to address the problem.

Legal

Contributors: appreciation of the (international) legal framework to secure a proper balance between the right to privacy and crime prevention; sentences that reflect the impact of the crime - as a deterrent and to reflect investigation resources invested; cybercrime needs to be punished and regulations and legislation has to be put in place; strong understanding of legal issues associated with cybercrime and gathering / presenting digital evidence; international rule of law;

Challenges: cybercrime is international; the legal framework is insufficiently equipped to create an effective deterrent; finding a proper balance between the right to privacy and crime prevention; anonymity of cybercrime, compounded by cross-jurisdictional nature, causing confusion as to which is responsible for investigation and prosecution; legal differences and international cooperation

Training and awareness

Contributors: correctly training patrol officers and investigators and recruiting capable personnel; education of general public to provide understanding of how to avoid falling prey to common forms of cybercrime;

Challenges: shortage of IT manpower; developing HR tools to recruit, motivate and retain IT personnel; relevant resources and skills and training; limited number of experts available at LEA, including cyber expertise; technology is ubiquitous but perceived as an isolated specialism and general lack of understanding leads to reluctance to adopt even modest best practice security individually and collectively.

Collaboration and cooperation

Contributors: removal of jurisdictional barriers; improved cooperation; collaboration / centres of excellence; create, support and maintain partnerships across sectors, jurisdictions and boundaries, for more efficient information sharing and to overcome jurisdictional issues; sharing threat intelligence

Challenges: critical infrastructures are also particularly vulnerable. Therefore a close cooperation between the security authorities and the business and the scientific partners is very important.

International policies and agreements

development and implementation of policies related specifically to cybercrime; international rules of engagement

Specific practical issues

Challenges: ever-growing, complex pool of victims - individuals, businesses and governments (anyone or any organisation using the internet); little or no real evidence, making reporting, identification and investigating crimes very difficult; willingness to report.

9.3. Summary – Stakeholder Perspectives

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<p><i>Technical mechanisms to effect enhanced capabilities of investigators was cited as an important factor; the need to have technological means to adequately respond to evolving criminal tactics, in particular.</i></p> <p><i>Technological evolution involves both risks and benefits; techniques such as anonymisation, visualisation and analytics will enhance capabilities and improve detection rates.</i></p> <p><i>Technological know-how and digital skills should be taught to all stakeholders. Development and adoption of best practices for online behaviour need to be established as a norm.</i></p>
HUMAN	<p><i>Human elements play a large part in enhancing the capability of investigators, mainly in connection with improving communication skills and methods as well as in relation to the need to improve technical knowledge and digital skills.</i></p> <p><i>Cooperation and information exchange incorporates incentivisation of all stakeholders and requires trust to be established. Behaviour changes too, in terms of altering perceptions and viewing the problem and the solution as a shared responsibility. Issues relation got</i></p>

	<p><i>reluctance to report cybercrimes need to be addressed.</i></p> <p><i>Employees are key to organisational resilience; improved governance of practices is required. The roles and responsibilities of individuals needs to be ascertained.</i></p> <p><i>There is a significant human factor consideration within the technology domain; the nature and behaviour of users and responders must be accounted for.</i></p> <p><i>Awareness raising and education is considered to be one of the most important areas in cybercrime. All stakeholders should be aware of the risks and their role in mitigating them. Education about specific techniques to deter and counteract cybercrime will increase resilience on all levels.</i></p>
<p>ORGANISATIONAL</p>	<p><i>Organisational factors to facilitate the enhanced capability of investigators include more visible reporting mechanisms, clear and harmonised classification of concepts and assessment and evolution of policies.</i></p> <p><i>Cultures within organisations can form barriers to effective cooperation. Identification of frameworks, training and financing is needed. Governance structures also need to be assessed. On an international level, the roles of Europol and Interpol need to be assessed so that future expectations can be realistic.</i></p> <p><i>The resilience of organisations and industry is a significant factor and needs to be assessed. Risk and impact assessments are also crucial, along with the corresponding accreditation and standardisation requirements.</i></p> <p><i>Organisations need to review their networks and data streams and develop strategies for their analysis and protection.</i></p> <p><i>Organisations bear a responsibility to train and raise awareness among employees and to set and maintain standards so that a culture of awareness can be established.</i></p>
<p>REGULATORY</p>	<p><i>The legal implications arising from cooperation and information exchange need to be considered; data protection, human rights, and privacy are among those highlighted. Policies for classifying documents also need to be reviewed to prevent unnecessarily blocking access to information. On an international level, differences in legislation and policy prevent effective cooperation. Another significant area to be addressed is jurisdictional differences in law and procedures.</i></p> <p><i>The judiciary need to acquire greater knowledge about cybercrime in order to be able to adapt current legislation in an appropriate and effective way. Understanding digital evidence and the methods used to gather it is also crucial.</i></p>

<p>ERASMUS ADVISORY BOARD PERSPECTIVES</p>	
<p>TECHNICAL</p>	<p><i>Keeping up with technological developments was seen as a key factor for LEAs, this includes improving skills and recruiting specialists as well as creating and reconstructing more resilient software. On a</i></p>

	<i>wider scale, IT systems designed without inbuilt security measures were seen as a contributory problem.</i>
HUMAN	<p><i>LEAs need to be more skilled and competent in working with technology. Human factors relating to criminal activity involve the current low-risk / high reward equation that is a driving force for cybercrime; as this continues, the complexity of criminal networks and expertise of offenders increases. Varying perceptions of cybercrime in the global political arena presents significant challenges when trying to combat it.</i></p> <p><i>Awareness raising among all stakeholders Is a key factor and includes recruiting key personnel in organisations as well as education of the public. Cybersecurity needs to be viewed as part of the general life rather than an isolated specialism. This shift in thinking extends to collaboration issues, which need to overcome traditional boundaries of all kinds, and stretches from authorities to individual citizens on a local and global scale. Another problem created by perception relates to victims; unwillingness to report for various reasons contributes to the scale of cybercrime.</i></p>
ORGANISATIONAL	<i>Organisational factors incorporate high level policy makers facilitating cooperation and collaboration and businesses and authorities effectively recruiting, training and embedding cultural change. In each stakeholder domain, a shift in approach is required so that security and awareness become inherent and collaboration is at the forefront of considerations.</i>
REGULATORY	<i>The international legal framework is important in achieving a balance between privacy and security and creating new collaborative norms. Effective and appropriate laws to secure convictions need to be put in place and sentences should reflect the impact of the wrongdoing, thereby serving as a deterrent. Cross-jurisdictional legal issues are a particular challenge when dealing with crime that recognises no boundaries. Rules relating to digital evidence and information gathering need to be understood.</i>

10. Background

10.1. Current Research

- NATO Cooperative Cyber Defence Centre of Excellence identifies vulnerabilities in most widespread network security solutions (April 2017). The research presents an approach that combines scientific and practical considerations. *An analysis of the generated test cases confirms that IPv6 and IPv6-based evasion techniques pose a difficult task for network security monitoring. While detection of various transition mechanisms is relatively straightforward, other evasion methods prove more challenging. Additionally, some security solutions do not yet fully support IPv6.*
- Hedgehog in the Fog paper: *...we review relevant transition technologies, describe two newly-developed IPv6 transition mechanism-based proof-of-concept tools for the establishment of covert information exfiltration channels, and compare their*

performance against common tunnelling mechanisms. We evaluated commonly used exfiltration tools in an automated and virtualized environment, and assessed covert channel detection methods in the context of insider threat.

NATO's mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

- 2017 International Conference on Cyber Conflict U.S. (7-8 Nov 2017). Premier conference on cyber conflict. Provides venue for fresh ideas, relevant and actionable content, insight into future trends, and access to industry, government and military leaders, cyber innovators and pioneers in the discipline. Promotes multidisciplinary cyber initiatives and furthers research and cooperation on cyber threats and opportunities.
- 'A new strategy for improving cyber-attacks evaluation in the context of the Tallinn manual' *In this paper a systematic modelling methodology for evaluating the effects of cyber-attacks on States Critical Information Infrastructure (CII) is introduced. The analysis is focused on the United Nations Charter's normative scheme of the 'use of force'; in order to define whether these attacks constitute a wrongful 'use of force' under the principles of international law. By using the qualitative criteria for recognizing the impact of cyber-attacks as proposed by the International Group of Experts in the Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) and by applying Multiple Attribute Decision Making (MADM) methods, cyber operations evaluation results are presented.*
- PriceWaterhouseCoopers Global Economic Crime survey reveals a general picture and highlights the problems and issues from a business point of view. The data offers evidence of a general lack of preparedness. Also highlights trends in attack methods and reasons for not reporting etc.
- RSA white paper '2016: Current State of Cybercrime' contains up to date figures and reports on the latest approaches by financial institutions to combat fraud: biometrics, which they predict will be a growth area in risk-based authentication services.

10.2. Statistics

- The annual Crime Survey for England and Wales in 2017 included cybercrime for the first time. Although only estimates, the indication was 5.8 million crimes involving online fraud and computer misuse.
- Office for National Statistics provides an overview of fraud statistics for year ending March 2016, in England and Wales.
- Cyber Security Breaches Survey 2017 reflects that almost half of UK businesses have identified a breach or attack in 2016. Some of the main findings are:
 - (a) The organisations affected face considerable financial costs from breaches, not just in terms of the direct results of the breach and recovery or repair costs, but also in terms of the long-term damage to the business's reputation among customers or investors.
 - (b) The prevalence of ransomware in particular has heightened awareness and made cyber security a more urgent issue.
 - (c) Businesses are unprepared and do not consider the reality of the risks from ransomware. This also highlights the inherent value of the data that

- businesses hold, beyond financial or personal and businesses can be stopped from carrying out day to day work, putting relationships at risk.
- (d) Few businesses have sought out the information available to assist them. Many outsource this, but there are issues of trust.
 - (e) Few are aware of the Government's Cyber Essentials Scheme, which provides help and support.
 - (f) Many admit to requiring training, but are unaware of how to find materials or providers.
- National Cyber Security Centre weekly threat reports are derived from open source reporting and collate the recent figures relating to cybercrime, providing an overall view of the cyber threat landscape on an ongoing basis. Some of the recent headlines focus on:
 - (a) 300% increase in attacks on Microsoft cloud services over the last year (2016-2017). A large majority of the compromises are due to weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services. Over 2/3 of Azure attacks came from IP addresses in China and the U.S. (32.5% U.S., 35.1% China). The remainder came from 116 countries and regions.
 - (b) Individuals posting pictures on social media of boarding passes, concert tickets and baggage containing stickers provides attackers with personally identifiable information which can be used to commit crime.
 - (c) Email phishing scans and fraudulent social media accounts are commonly used to obtain money in the wake of disasters.
 - (d) Long term campaigns targeting travellers and business people allow hackers to obtain personal information through hotel Wi-Fi networks, on which malware is installed.
 - (e) Significant changes to the DDoS attack methodology over the last year (2016-2017), with reports of multiple attacks on the same victim companies. In the Q1, 2017, 58% of DDoS attacks targeted the IT services / cloud SaaS industry, 28% targeted financial services and 6% targeted media and entertainment. The average cost of a DDoS attack now exceeds \$2.5 million in lost revenue.

10.3. Reports

- Cisco 2017 Annual Cybersecurity Report highlights that 44% of security alerts aren't investigated; 49% experienced public scrutiny after a breach; 22% lost customers because of attacks; 29% lost revenue as a result of attacks. An overview focuses on the following categories:
 - **'perception** - confidence and trust in tools and infrastructure must be verified';
 - **'constraints** - organisational issues create environments that breed complexity';
 - **'impact** - complexity opens gaps in defences, giving bad actors unconstrained time to operate'.
- The Cisco approach includes:
 - **Address the full attack continuum** - threat-CENTRIC security solutions provide protection across the extended network before, during and after an attack
 - **Boost protection before an attack** - defending against context-aware threats requires context-aware security.

Respond faster during an attack - accurately detect, block, and defend against malicious activities by analysing behaviour patterns and vectors.

Contain and remediate after an attack - reduce time from months to minutes using continuous detection and retrospective security.

- UK National Cyber Security Centre 2017 report on criminal online activity: "*Very few people are aware of the extent of the online criminal ecosystem that supports and enables cyber attacks. A new report from the NCSC (Cyber crime: understanding the online business model) describes how Organised Criminal Groups (OCGs) share similar techniques and services and communicate with each other over the 'dark web' where they can collaborate and advertise new services, tools and techniques*". The National Cyber Security Centre has a great number of reports (including weekly threat assessments that will be relevant to all countries) and other various resources on the website.
- European Union Serious and Organised Crime Threat Assessment 2017 is a detailed analysis of the threat of serious and organised crime facing the EU providing information for practitioners, decision-makers, and the wider public. From the SOCTA 2017, Europol has undertaken the largest-ever data collection on serious and organised crime in the EU. Europol relied on thousands of contributions by Member States, Europol's operational and strategic partners outside the EU and our institutional partners as well as operational intelligence held in Europol's databases to produce the most detailed assessment of the nature and scale of criminal threats facing the EU and Member States. The report is divided into the following categories: Defining serious and organised crime; organised crime groups and other criminal actors; engines of organised crime; drivers of crime; currency counterfeiting; cybercrime; drug production, trafficking and distribution; environmental crime; fraud; intellectual property crime; organised property crime; people as a commodity; sports corruption; trafficking of firearms; links between serious and organised crime and terrorism.
- NCA (National Crime Agency) 'Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime'. Jointly produced by the NCA and the Strategic Cyber Industry Group. Outlines the real and immediate threat to UK businesses from cybercrime. It argues that the speed of criminal capability development is currently outpacing our response as a community and that only by working together across law enforcement and the private sector can we successfully reduce the threat to the UK from cybercrime. *This 'cyber arms race' is likely to be an enduring challenge, and an effective response requires collaborative action from government, law enforcement, industry regulators and critically, business leaders.....there is much more that needs to be done, working with the government and law enforcement to reduce vulnerabilities and prevent crime.* The reports outlines the threats and describes the typical characteristics of those perpetrating them, referring to capabilities and modus operandi. Also includes real-life cases as illustrations of the scale and nature of the problems that are rapidly increasing. Provides a good overview of the current landscape.
- ETL 2016 (Enisa current and emerging threat landscape report, published February 2017); ETL 2016 is streamlined towards the top cyber-threats, providing information on threat agents and attack vectors including all the remarkable developments, trends and issues. Moreover, it reports about threat agents, their motivations and how their practices tools and techniques have

advanced. Though the defenders have made significant progress in disrupting cyber-threats and in the attribution of incidents, adversaries continue to advance their tactics and techniques. Enisa's work in the area of threat analysis also includes: 1) threat assessments for two emerging technology areas - hardware and ad-hoc sensor networking for mobile to mobile communications and an update on the cyber-threat taxonomy.

The development and optimisation of malware to make a profit remains the main objective in attack methods, tools and tactics. Malware is at the top of the list of cyber threats with mobile malware, ransomware and information stealers being the key areas of criminal malware innovation. The report suggests that the increase in sophistication of attackers has given rise to the need for more sophisticated 'defenders' (i.e. ways for an organisation to mitigate the risk of an attack).

2016 saw an increase in operations coordinated by law enforcement authorities that were able to disrupt malicious activities, including exploitation of weaknesses in anonymisation infrastructures, tools and virtual currencies. There was recognition of the importance of cyber security in professional education and training to mitigate the risk of a future skills shortage.

- RUSI research paper - highlights the importance of financial institutions in the fight against cybercrime. Examines the reasons for under / non-reporting, vulnerabilities and suggestions for greater effectiveness.
- Control Risks '5 cyber watchpoints for 2017: what's in store for cyber security around the world?' Addresses issues in: Australia; Central South America; China; European Union; Russia; United Arab Emirates; United Kingdom; USA. Predicts that because *'Individual activists and mass-participation campaign continue to target companies and organisations for ideological reasons, 2017 will be a year when geopolitical shifts and technological advances by nation state and criminal actors will combine to create an unprecedentedly complex cyber threat landscape.'* In the U.S. - *the most sophisticated cyber espionage units will adopt increasingly innovative means of avoiding detection and attribution for their efforts. Rather than depending on bulky malware with hardcoded connections to command and control infrastructure, these actors will instead increasingly look to exploit legitimate processes and protocols to steal data and achieve their objectives, all while avoiding alerting the victim to the infection.* *the policy landscape will see increasing state-led efforts to legislate and regulate cyber-security issues and enforce national borders for data. Russia and China will lead the push towards data protectionism and are likely to prompt similar approaches in their respective spheres of influence. These efforts are also likely to include specific anti-encryption provisions, in response to the increasing normalisation of encryption as a tool for privacy and security. This in turn is like to contribute to a more complicated international operating environment for companies, but also to continued difficulties for law enforcement agencies attempting to pursue malicious actors across jurisdictions.*

10.4. Key legislation on cyber security and data flows in 2016:

- China - cyber security law outlines stricter government controls over 'critical information infrastructure'
- Russia - Yarovaya Law increases government access to online content

- UK - Investigatory powers Act places new obligations on telecommunications companies
- U.S. - amendments to Rule 41 expand hacking powers of law enforcement agencies
- U.S./EU - ongoing challenges to Privacy Shield Agreement threaten companies' ability to transfer data
- EU - Net neutrality legislation and guideline
 - GDPR give companies greater responsibility for data security
 - Proposed amendments to ePrivacy Directive to regulate communications services over the internet
 - Directive on Security of Network Information Systems aims to harmonise cyber security standards
 - Australia - Privacy Amendment Bill set to introduce mandatory disclosure of data breaches
 - United Arab Emirates - increased restrictions on use of virtual private networks in the country.
- Key points include: increased focus on mobile devices by cybercriminals, Demand on the cybercriminal underground, facilitated by the crimeware-as-a-service economy, will drive continued innovation from malware developers. There is likely to be a particular focus on the development of banking Trojans and mobile malware with multiple functionality. Development of criminal apps to monetise stolen credit card data. Etc.

10.5. Summary – Background

CURRENT RESEARCH	
TECHNICAL	<i>NATO research identifies vulnerabilities in most technology solutions and examines issues relating to IPv6. This early identification of potential technical issues can be further explored. Biometrics is predicted as a growth area in risk-based authentication services.</i>
HUMAN	<i>Multi-disciplinary approaches are identified as a major contributory factor in successfully combatting cybercrime, by many research bodies.</i>
ORGANISATIONAL	<i>The Tallinn Manual presents a systematic modelling methodology for evaluating cyber attacks on critical infrastructure. This key document is of central importance on an international scale and will influence approaches.</i> <i>The general lack of preparedness and inadequate protection of businesses and organisations is a theme running through the research.</i>
REGULATORY	

STATISTICS	
TECHNICAL	<i>Although many businesses have adopted limited practices to improve security of systems, the uptake of the Cyber Essentials Scheme is low. There is competing considerations between increased security and cost of investment in such measures.</i>

HUMAN	<p><i>Lack of awareness of citizens leads to a wealth of opportunities for cybercriminals who are quick to capitalise on poor password management, guessable passwords, posting personal information on social media and using insecure Wi-Fi networks for business transactions.</i></p> <p><i>Other common cybercrimes resulting from lack of awareness include phishing scams and fake social media accounts.</i></p> <p><i>Many of those in business are in need of training, but do not seek it out.</i></p> <p><i>The cost of cyber attacks goes beyond financial and affects trust and relationships between businesses and customers / investors.</i></p>
ORGANISATIONAL	<p><i>A large number of cybercrimes are unreported by organisations due to potential impact on reputation and relationships. Businesses generally do not appreciate the reality of the damage that can be caused by cybercrime, in financial and reputational terms. Many organisations require additional training and resources but have not acted on this need, leaving themselves vulnerable. Many would like assistance with this.</i></p>
REGULATORY	<p><i>In the UK, crime recording rules affect the number of crimes reflected in annual figures. There is also a degree of subjectivity in reporting.</i></p>

REPORTS

TECHNICAL	<p><i>Confidence and trust in technological solutions needs to be established. Reports include predictions in criminal use of technology; hardware and mobile technology are significant areas. Malware remains at the top of the threat list along with theft of personal information and ransomware.</i></p> <p><i>It is envisaged that a forthcoming trend will be the criminal exploitation of legitimate systems, which will increase the challenge to detect attacks, which is one of the aims of the perpetrators.</i></p>
HUMAN	<p><i>Reports explore the factors involved in under-reporting of cybercrime and identify needs for increased awareness and knowledge of attack method and the associated risks.</i></p> <p><i>Europol's extensive research combined with practical expertise and assessments of key areas includes human and economic drivers of cybercrime, the nature and actions of organised crime groups, specific areas vulnerable to attack, such as sports corruption and financial institutions and various methods and practices. Firearms, drugs and human trafficking are highlighted. The NCA report also addresses characteristics of perpetrators, including capabilities and modi operandi.</i></p>
ORGANISATIONAL	<p><i>General trends indicate a requirement for organisational change on all levels. Creating strategies for effective identification, defence and recovery needs to be focused upon. Shifting cultures to facilitate effective cooperation and collaboration is also key. The scale of cybercrime is shown as increasing rapidly in all areas, particularly fraud. Successful coordinated efforts are increasing, but not at the</i></p>

	<p><i>same rate as attacks. Organisational issues are capable of creating environments which serve to perpetuate the frequency and complexity of attacks.</i></p> <p><i>The UK's NCA identifies the need for stronger collaboration which needs to be instigated at organisational level. This is the key change required for more effective combatting of cybercrime. Case studies serve as a valuable resource for awareness-raising.</i></p> <p><i>The key role of financial organisations in the fight against cybercrime is addressed by RUSI. As well as having responsibilities to combat crime and share expertise, organisations are also identified as specific targets for ideological reasons.</i></p>
REGULATORY	<p><i>Countries across the globe will enact legislation in the near future, leading the data protection and information security approach being adopted worldwide. Encryption will become more normalised and efforts will increase in relation to preventing anti-encryption capabilities. This double-edged sword creates further difficulties for LEAs and others conducting investigations and seizing evidence.</i></p> <p><i>Recent changes in legislation across the world demonstrate increased state control, increased obligations on telecoms providers and stricter measures relating to data transfer. There are efforts to harmonise legislation and standards, to a limited degree.</i></p>

11. Current Policies

11.1. European Institutions

- Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's foreign and security policy. Peace and security, prosperity, democracy and a rules-based global order are the vital interests underpinning our external action. The vision is set out in sections: A Global Strategy to Promote our Citizens' Interests; The Principles Guiding our External Action; The Priorities of our External Action (The Security of Our Union; State and Societal Resilience to our East and South; An Integrated Approach to Conflicts and Crises; Cooperative Regional Orders; Global Governance for the 21st Century); From Vision to Action. June 2016.
- EU Policy Cycle - EMPACT. Europol has nine priority crime areas. For each one, a multi-annual strategic plan, a **European Multidisciplinary Platform Against Criminal Threats** project and an operational action plan are implemented. Cybercrime is one of the nine areas; the action is to Combat cybercrime, such as online and payment card fraud, that: 1) is committed by organised crime groups; 2) generates large criminal profits; 3) causes serious harm to its victims (such as child sexual exploitation); 4) affects critical infrastructure and information systems in the EU (such as cyberattacks). In 2010, the EU set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organised crime. The policy calls for effective cooperation among: law enforcement agencies; other EU agencies; EU institutions; relevant third parties. To that end, it also calls for robust action to target the most pressing criminal threats facing the EU. The first full policy cycle

will run until 2017. It consists of four steps:

- 1) The serious and organised crime threat assessment (SOCTA)
- 2) Strategic plans
- 3) European multidisciplinary platform against criminal threats (EMPACT)
- 4) Evaluation

Successes attributable in whole or in part to the EMPACT cycle have already been seen in each of the priority crime areas, and there is every reason to expect that this trend will continue.

- ENISA 2014 - 2017 Cyber Security Strategy.in order to prevent and deter future security threats, it is necessary to constantly develop cyber security related knowhow and to invest in technology. Implementing forward-looking procurement procedures is necessary to ensure production of reliable and competitive technical solutions and will support their export as well, whereas the knowledge and resources obtained in that process must be re-invested into innovative solutions. As a supporting activity, a modern legal framework must be ensured to provide complete solutions to the above-listed challenges. At the international level, the preservation of a free and secure cyberspace as well as Estonia's central role in guiding and developing international cyber security policy in international organisations as well as like-minded communities must be ensured.

Principles of ensuring cyber security:

- 1) cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.
- 2) Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information and identity.
- 3) Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
- 4) Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.
- 5) cyber security starts with individual responsibility for safe use of ICT tools
- 6) A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialise.
- 7) Cyber security is supported by intensive and internationally competitive research and development
- 8) Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence.

Subgoals:

- 1) Ensuring the protection of information systems underlying important services;
 - Ensuring alternative solutions for important services
 - Managing cross-dependency between important services
 - Ensuring the security of ICT infrastructure and services
 - Managing cyber threats to the public and private sector
 - Introduction of a national monitoring system for cybersecurity
 - Ensuring digital continuity of the state
 - promotion of international cooperation in the protection of the

- infrastructure of critical information
 - 2) Enhancing the fight against cybercrime
 - Enhancing the detection of cybercrime
 - Raising public awareness of cyber risks
 - Promoting international cooperation against cybercrime
 - 3) Development of national cyber defence capabilities
 - Synchronising military planning and preparation for civil emergencies
 - Developing collective cyber defence and international collaboration
 - Developing military cyber defence capabilities
 - Ensuring a high level of awareness concerning the role of cyber security in national defence.
 - 4) Estonia manages evolving cyber security threats
 - Ensuring the next generation cyber security professionals
 - Developing smart contracting for cyber security solutions
 - Supporting development of enterprises providing cyber security and national cyber security solutions.
 - Preventing security risks in new solutions
 - 5) Estonia develops cross-sectoral activities
 - Development of a legal framework to support cyber security
 - Promoting international cyber security policy
 - Closer cooperation with allies and partners
 - Enhancing the capability of the European Union
- Etc...
- European Commission Communication on Cybersecurity Strategy of the European Union - an Open, Safe and Secure Cyberspace. Jointly adopted by the Commission and the high Representative. It outlines the EU's vision in this domain, clarifies roles and responsibilities and proposes specific activities at EU level. Its goal is to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world. These actions include in particular:
 - achieving cyber resilience by increasing capabilities, preparedness, cooperation, information exchange and awareness in the field of Network and Information Security, for the public and private sectors and at national and EU level;
 - drastically reducing cybercrime by strengthening the expertise of those in charge of investigating and prosecuting it, by adopting a more coordinated approach between law Enforcement Agencies across the Union, and by enhancing cooperation with other actors;
 - developing an EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy;
 fostering the industrial and technological resources required to benefit from the Digital Single Market. This will help stimulate the emergence of a European industry and market for secure ICT; it will contribute to the growth and competitiveness of the EU economy; and it will increase the public and private spending on cybersecurity Research and Development;
 - enhancing the EU's international cyberspace policy to promote EU core values, to define norms for responsible behaviour, to advocate the application of existing international law in cyberspace and to assist countries outside the EU in building cybersecurity capacity.

- European Agenda on Security: on 28 April 2015 the European Commission set out a European agenda on Security for the period 2015-2020 to support Member States' cooperation in tackling security threats and step up our common efforts in the fight against terrorism, organised crime and cybercrime. The agenda sets out the concrete tools and measures which will be used in this joint work to ensure security and tackle these three most pressing threats more effectively. the responsibility for ensuring internal security is first and foremost with the Member States, but cross-border challenges defy the capacity of individual countries to act alone and require EU support to build trust and facilitate cooperation, exchange of information and joint action. The three most pressing challenges: 1) preventing terrorism and countering radicalisation; 2) fighting organised crime; 3) fighting cybercrime

Key Actions Include:

 - Countering radicalisation
 - Updating the Framework Decision on Terrorism
 - Cutting the financing of criminals
 - Enhancing dialogues with the IT industry
 - Strengthening the legal framework on firearms
 - Reinforcing our tools to fight cybercrime
 - Enhancing the capacities of Europol

(this page includes links to other relevant information)

11.2. Industry

- Privacy Enhancing Technologies: Evolution and State of the Art (enisa document guiding developers and others to build and maintain PETs) December 2016
- SHIELD project proposing universal solution for dynamically establishing and deploying a virtual security infrastructure into ISP and corporate networks (EU funded H2020, began 2017)

The SHIELD framework combines Network Functions Virtualisation (NFV), Security-as-a-Service (SecaaS), Big Data Analytics and Trusted Computing (TC), in order to provide an extensible, adaptable, fast, low-cost and trustworthy cybersecurity solution.
- European Commission's Energy Expert Cyber Security Platform Expert Group, proposing analysis of potential threats to cybersecurity within the EU and how to combat them, also encouraging EU energy regions to cooperate and share information about cyber risks.

A new report has been published on cyber security in the energy sector. The report identifies areas where action should be taken to improve cyber security and manage risks for energy infrastructure. The report identifies strategic challenges and specific needs for cyber security in the energy sector in four key areas:

 - 1) management of risks and threats;
 - 2) cyber defence;
 - 3) Cyber resilience;
 - 4) the capacity and competencies needed to take action.

It proposes that the EU Commission should analyse potential threats to cyber security within the EU and how to combat them, and also encourage EU energy regions to cooperate and share information about cyber security risks. The report

also suggests that the Commission should set up a cyber response framework for the energy sector, in order to be prepared for potential attacks, and take measures to improve the resilience of energy infrastructure to possible security breaches.

- GLACY (Global Action on Cybercrime) published document in October 2016 that was adopted at the closing conference of the GLACY project on Global Action on Cybercrime, Bucharest, 26-28 October 2016: 'Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries'.

Strategic Priorities:

- Mainstreaming cybercrime and electronic evidence in the criminal justice system
- Continuous law reform and development
- Strengthening Institutional Capacities on Cybercrime and Electronic Evidence
- Law Enforcement Training
- Judicial Training
- Cooperation between law enforcement and service providers
- More efficient regional and international cooperation

11.3. Law Enforcement

- Interpol 'Global Cybercrime Strategy'

Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of internet-related crime:

1) **Advanced cybercrime** (or high-tech crime_ - sophisticated attacks against computer hardware and software.

2) **Cyber-enabled crime** - many 'traditional' crimes have taken a new turn with the advent of the internet, such as crimes against children, financial crimes and even terrorism

INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled crimes. Most cybercrimes are transnational in nature, therefore INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale.

Main initiatives are:

- Operational and investigative support

Cyber intelligence and analysis

Digital forensics

Innovation and research

Capacity building

National Cyber Reviews

INTERPOL Global Complex for Innovation (IGCI) in Singapore is a cutting-edge research and development facility, which opened in 2014, it leverages global cyber-expertise from law enforcement and key private sector partners.

INTERPOL is uniquely positioned to advance the fight against cybercrime on a global scale through proactive research into emerging crimes, the latest training techniques, and development of innovative new policing tools.

This source includes cases / examples / latest news

- University of Birmingham 'Cybercrime Workshop: Better Policing Collaborative (BPC)' 27 March 2017. (Home Office, College of Policing, Higher Education Funding Council for England, Police Knowledge fund, Better Policing Collaborative, Centre for Crime, Justice and Policing, University of Birmingham, University of Derby)
- Europol - EMPACT policy cycle (2013 - 2017) Cybercrime is a key priority (as discussed above)

11.4. Summary – Current Policies

EUROPEAN INSTITUTIONS	
TECHNICAL	<p><i>The responsibility for the safe use of ICT tools is a shared one, from citizens to corporations, who should be more focused on whole system security and establishing best practices.</i></p> <p><i>Manufacturers and developers need to focus on preventing security risks in new solutions and incorporating security considerations into the design of new technology.</i></p> <p><i>Secure technologies that gain the trust of those who use them will further the European aim of a digital single market and the freedom of users to benefit from it.</i></p>
HUMAN	<p><i>Preventing and protecting victims is a priority area, particularly relation to child sexual exploitation and human trafficking. Also, the balance between creating a safe environment and maintaining rights, freedoms and opportunities for citizens is an important aim, and central to the solution.</i></p>
ORGANISATIONAL	<p><i>Collaboration, cooperation and a multi-disciplinary approach remains at the core of the policies. A key ingredient in this approach is the involvement of citizens in the fight against cybercrime.</i></p> <p><i>Organisations of all kinds form part of the strategic plans of various European bodies and have responsibilities ranging from protecting infrastructure to raising employee awareness and from implementing forward-looking, secure technologies to sharing information and expertise.</i></p> <p><i>Policy-making organisations have a responsibility to build resilience, set standards and create new norms that facilitate co-working and a united front, while respecting individual rights.</i></p>
REGULATORY	<p><i>A modern legal framework is called for, to underpin and support all other efforts in relation to combating cybercrime. This will assist in providing complete solutions. Cybersecurity is central to the effective functioning of the state in several respects. Legal instruments also protect the fundamental rights and freedoms of the citizens.</i></p> <p><i>Responsibility of organisations for taking positive action in respect of IT and system solutions may also be endorsed by appropriate legislation. Effective legislation would help facilitate many of the strategies, for example common understanding of crime types, collaboration and information sharing and cross-jurisdictional LEA measures.</i></p>

INDUSTRY	
TECHNICAL	<p><i>Privacy enhancing technologies are an important part of the European approach and guidance is provided for developers to build and maintain technology to these standards.</i></p> <p><i>The SHIELD framework combines Network Functions Visualisation (NFV), Security -as-a-Service (SecaaS), Big Data Analytics and Trusted Computing in order to provide an extensible, adaptable, fast, low-cost and trustworthy cybersecurity solution.</i></p> <p><i>The energy sector was singled out by the Commission, highlighting specific risks associated with this sector.</i></p>
HUMAN	<p><i>Collaboration of experts organised by the EU Commission analysed potential cybersecurity threats within the energy sector, and ways of combating these. This collaborative approach represents the importance of individual expertise and experience. Capacity and competencies form one of the key areas in a published report outlining challenges and needs in the energy sector.</i></p>
ORGANISATIONAL	<p><i>Managing risks for critical infrastructures falls within the remit of organisational responsibility. Effective arrangements for sharing information and expertise to enable collaboration is also a change that should occur at organisational level.</i></p>
REGULATORY	<p><i>A key element arising from the global Action on Cybercrime event in 2016 related to legal considerations. In particular, two areas were identified: evidence and training of those applying and interpreting the law. This represents the general issue of adapting existing legislation to the developing cybercriminality and ensuring that criminal justice processes and practices are relevant. Alongside this, is the requirement for continuous development and updating of the laws that support all actions in this area.</i></p>

LEA's	
TECHNICAL	<p><i>INTERPOL Global Complex for Innovation (IGCI) in Singapore is a cutting-edge research and development facility, which opened in 2014, it leverages global cyber-expertise from law enforcement and key private sector partners.</i></p> <p><i>INTERPOL is uniquely positioned to advance the fight against cybercrime on a global scale through proactive research into emerging crimes, the latest training techniques, and development of innovative new policing tools.</i></p>
HUMAN	<p><i>Interpol represents a desirable level of expertise and capability, backed by intelligence systems, IT professional from private industry and a high level research facility. From this position, they are able to increase the capacity of local law enforcement and set best practice examples.</i></p> <p><i>Digital forensics, cyber intelligence and analysis as well as operational and investigative support, illustrates what can be achieved with greater expertise and resources.</i></p>

ORGANISATIONAL	<i>Interpol is uniquely placed to be able to facilitate cooperation between LEAs and add their knowledge and expertise to enable more effective action against cross-jurisdictional cybercrime.</i>
REGULATORY	

12. Current Practice

12.1. Europe

- Cyber Europe 2016 'Stronger Together' (cyber-security exercise - large scale, distributed technical and operational exercise involving 300 stakeholder organisations.

enisa event (every two years): the pan-European exercise to protect EU Infrastructures against coordinated cyber-attack. In anticipation of a cyber attack on critical infrastructure....computer security attacks are increasingly used to perform industrial reconnaissance, lead disinformation campaigns, manipulate stock markets, leak sensitive information, tamper with customer data, sabotage critical infrastructures. In Cyber Europe 2016, Member State cybersecurity authorities and cybersecurity experts from the public and private sectors are called to react to a series of unprecedented, coordinated cyber-attacks. Thousands of experts from all Member States, Switzerland and Norway took part in the event. For the first time, a full scenario was developed with actors, media coverage, simulated companies and social media, bringing in the public affairs dimension associated with cyber crises, so as to increase realism to a level never seen before in cybersecurity exercises.
- European Audit Committee Leadership Network Discussion in May 2015: at the EACLN meeting in London discussion focused on several themes related to dealing with cyberrisks and cybersecurity:

Assessing cyberrisks

Identify the most important assets to protect

 - what is the company's most sensitive information?
 - How vulnerable is it and would the company know if it was under attack?
 - What is being done to protect it?
 - What would the impact be if high-priority assets were attacked?
 - What is the company's response plan to contain and mitigate the impact from such an attack?

Asses the threat landscape

 - Operational disruption
 - Physical destruction
 - Extortion
 - Data alteration
 - Intellectual property and digital asset theft
 - Reputational damage
 - Compliance risk

Mitigating cyberrisks

Enlist Outside Help

Create a Culture of Security

 - Lead from the top

- Limit employee exposure
- Build a human firewall
- Make cybersecurity a business issue, not just a technology issue
- Tailor cybersecurity to specific threats
- Share information with the government and other companies

Audit committee and board oversight of cyberrisks and cybersecurity

Audit committee or board oversight?

- A need for standards
- Oversight of internal controls
- Tap board knowledge without adding to committee assignments
- Europol: 'Unique Police2peer Initiative Combats Child Sexual Exploitation and Abuse Online' press release about one of Europol's latest successes and an indication of their approach.
- European Commission Public-Private Partnership on cybersecurity (part of the EU cybersecurity strategy, signed in July 2016)

12.2. International

- UN General Assembly paper: Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security - indication of current issues (in 2015).
The group examined existing and potential threats arising from the use of ICTs by States and considered actions to address them, including norms, rules, principles and confidence-building measures. In addition, the Group examined how international law applies to the use of ICTs by States.
The report expands the discussion of norms. The group called for the increased exchange of information and assistance to prosecute terrorist and criminal use of ICT's. In doing so, the Group emphasized that States should guarantee full respect for human rights, including privacy and freedom of expression.
One important recommendation was that a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions.
Confidence-building measures increase cooperation and transparency and reduce the risk of conflict. The Group called for regular dialogue with broad participation under the auspices of the United Nations and through bilateral, regional and multilateral forums. International cooperation would benefit from the appropriate participation of the private sector, academia and civil society. The Group reiterated the conclusions from the 2013 report in calling for the international community to assist in improving the security of critical ICT infrastructure, help to develop technical skills and advise on appropriate legislation, strategies and regulation. The present Group reiterated those conclusions and emphasised that all States can learn from each other about threats and effective responses to them.
the Group emphasised the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States. The Group also noted the established international

legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.

the Group proposed that the General Assembly consider convening a new Group of Governmental Experts in 2016.

Contents of the report:

- 1) Existing and emerging threats
- 2) Norms, rules and principles for the responsible behaviour of States
- 3) Confidence-building measures
- 4) International cooperation and assistance in ICT security and capacity-building
- 5) How international law applies to the use of ICTs

Possible measures for future work that were identified, but not limited to:

- a) Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels;
 - b) Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and security posed by the malicious use of ICTs and on the security of ICT-enabled critical infrastructure.
 - c) Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing work by other international organisations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and internet governance.
 - d) The Group in 2016 should continue with a view to promoting common understandings on existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as how international law applies to the use of ICTs by States, including norms, rules and principles of responsible behaviour of states, confidence-building measures and capacity-building.
- G7 Geared up for Cyber Threats in 2016, focusing on Financial Sector. The G7 stepped up its cybersecurity efforts during the Japanese chairmanship in 2016. The group held an ICT Ministers' Meeting on 29-30 April 2016. On 27 May 2016, it adopted the G7 Principles and Actions on Cyber as an annex of the G7 Leaders' Declaration and established the Ise-Shima Cyber Group. The G7 further endorsed the G7 Fundamental Elements of Cybersecurity for the Financial Sector on 7 October 2016.

The G7 ICT Ministers met in 2016, the first time in 20 years. They dealt with cyberspace in general, concentrating on economic and social aspects, but also devoted one session to cybersecurity. The Ministers adopted a Charter for the digitally connected World (the 'Charter'), issues a Joint Declaration (an Action Plan for implementing the Charter), and formulated the G7 Opportunities for Collaboration.

The Charter lists four fundamental principles underpinning the 'digitally connected world';

- 1) Promoting and protecting human rights;
- 2) Promoting and protecting the free flow of information (here the Charter talks about 'digital security')
- 3) Supporting a multi-stakeholder approach, and
- 4) Strengthening digital connectivity and inclusiveness for all

To develop these principles, the Charter formulates the G7 ICT Strategy. The

Strategy deals with promoting cybersecurity, along with cross-border information flows and privacy and data protection.

The Charter is implemented by the Action Plan contained in the Joint Declaration, in which Ministers state that they support policies which promote internet openness and the flow of information across borders; they oppose 'unjustifiable' data localisation requirements; and they support 'high standards of privacy and data protection', referring to the 'Privacy by Design' approach. International collaboration, capacity building and public-private partnerships are viewed as important elements of cybersecurity, as are training, education and increased awareness.

The annex to the Joint Declaration, titled 'G7 Opportunities for Collaboration, contains a list of projects which the G7 states consider important enough to call on for international cooperation. The section on 'promoting and protecting the free flow of information' lists several cybersecurity projects:

- the CyberGreen Project;
- Network Incident analysis Centre for Tactical Emergency Response (NICTER);
- Information Sharing and Analysis Centres (ISACs);
- Initiatives to enhance op-source security, such as the Linux Foundation's Core -
- Infrastructure Initiative (CII);
- Information sharing in the field of data economy, and
- International collaboration in the domain of spam and malware intelligence.

The G7 held its annual summit in Ise-Shima Japan on 26-27 May 2016. The summit declaration, while dealing with a variety of global and regional issues, contains several references to cyberspace and cybersecurity. The leaders also endorsed the G7 principles and Actions on Cyber, which form an annex of the declaration and elaborate some of the ideas from the declaration itself. In both documents, the G7 leaders express their common principles with respect to cyberspace, stating that its openness is essential to economic prosperity and the common democratic values of G7. By putting security on the same level as openness, the G7 countries want to emphasise that security is essential for cyberspace to remain open and accessible.

Interestingly, the declaration and annex fully avoid the use of the term 'encryption', which was one of the main topics on which the debate on national security and cyberspace has focused in recent years. It is possible that this is due to the fact that even the G7 states and their respective intelligence and law enforcement authorities have conflicting interests regarding enhancing or breaking encryption.

The G7 leaders reaffirm that international law is applicable in cyberspace and commit to promoting voluntary norms of responsible state behaviour and confidence-building measures. They refer to the 2015 UN GGE Report and call upon all states to be guided by it.

The G7 wants to promote cybersecurity by encouraging cooperation among national computer security incident-response teams, as well as building capacity and raising awareness. Information sharing on cybersecurity threats, especially to critical infrastructure, should be enhanced, and the G7 will collaborate on research in security, privacy, and resilience. This shows that at least on the international stage, the G7 states remain supportive of privacy.

The G7 encourages more states to join the Budapest Convention on Cybercrime of the Council of Europe and it promotes the activities of the G7 Roma-Lyon

Group's High-Tech Crime Subgroup and its 24/7 Network.

The Ise-Shima Cyber Group was established by the declaration. The group should enhance policy coordination and practical cooperation to promote security and stability in cyberspace'. It will re-convene during the Italian presidency of the G7 in 2017.

G7 Fundamental Elements of Cybersecurity for the Financial Sector

The Elements are non-binding principles of cybersecurity for private and public entities and authorities in the financial sector. They are described as the 'building blocks' upon which an entity can design, implement and re-evaluate its cybersecurity strategy and operating framework. The Elements were prepared by the G7 Cyber Expert Group and endorsed by the G7 finance ministers and central bank governors on the margins of the annual meeting of the International Monetary Fund (IMF) on 7 October 2016.

Eight topics listed in the Elements:

- 1) Cybersecurity strategy and framework;
 - 2) Governance;
 - 3) Risk and control assessment;
 - 4) Monitoring;
 - 5) Response;
 - 6) Recovery;
 - 7) Information sharing and
 - 8) Continuous learning.
- INTERPOL (including Global Complex for Innovation in Singapore; a cutting edge research and development facility, opened in 2014, leverage global cyber-expertise from law enforcement and key private sector partners.
 - Cyber Security Quarterly Round-Up, March 2017. Overview of latest developments in Europe, Hong Kong, UK and the U.S. The quarterly eBulletin provides a round-up of best practice, news and legislative developments concerning cyber security.

The UK will implement requirements for the Cyber Security Directive despite Brexit. The UK's National Cyber Security Centre (NCSC) has issued an open invitation for up to 100 secondments from the private sector. 'Industry 100' an initiative that will integrate up to 100 personnel from industry into the NCSC by the end of the financial year 2017 / 2018. The NCSC forms part of the UK's intelligence agency (GCHQ). It was set up to help protect the UK's critical services from cyber attacks, manage major incidents and improve the underlying security of the internet in the UK through technological improvement and advice to citizens and organisations. The aim of the initiative is two-fold:

- 1) It will allow the industry to draw on industry expertise - working collaboratively to share best practice whilst also having its thinking challenged;
- 2) The training received whilst at the NCSC aims to drive change within the industry and better equip the 'secondees' to tackle cyber threats on returning to their original day jobs. The roles sought by the NCSC included network defenders and analysts from critical infrastructure sectors, namely finance, energy, transport, telecoms and health, for two days a week over a six-month period. Industry will fund the roles.

On 10 January 2017 the Joint Committee on the National Security Strategy announced an inquiry into UK cyber security. The Joint Committee comprises 22 members appointed from both the House of Commons and the House of Lords

and was created to 'monitor the implementation and development' of the UK government's National Security Strategy. Some of the areas it is particularly interested in include:

- The types and sources of cyber threats faced by the UK;
- Whether the UK has committed sufficient human, financial and technical resources to address the scale of the cyber security challenge;
- The development of offensive cyber capabilities and the norms governing their use;
- The balance of responsibilities between the government and private sector in protecting critical national infrastructure
- The appropriate role for government in regulating and legislating in relation to cyber both nationally and internationally
- How the UK can cooperate with allies and partners on the development of capabilities, standard setting and intelligence sharing.

Insurers handling hundreds of data breach claims

Lloyd's of London's underwriting agency reports that it handled over 40 claims under cyber insurance policies in 2016, an increase of 78% on 2015. Hand-in-hand with this is a 50% growth in UK insurance policies taken out against cyber attacks during 2016.

Healthcare Sector is an Increasingly Attractive Cyber Target

In April - June 2016 the health sector accounted for the highest number of data security breaches, due in part to the size of the UK health sector. Out of date legacy hospital IT systems may be more susceptible to malware installed via a phishing attack.

The Growing Need for a Cyber Security Culture in the Financial Services Sector

Financial institutions are facing an increasing number of organised cyber attacks and multi-channel threats. According to a report published in February 2017, financial technology companies in particular are experiencing an increasing number of cyber attacks from those taking advantage of alternative lending and payment models as well as exploiting gaps and loopholes in what are predominantly digital systems designed for superfast processing and agile product innovation. This is according to the latest Cybercrime Report published by ThreatMetrix, a security company that monitors more than 20 billion online transactions worldwide per year.

Whilst a firm's cyber security compliance strategy will be bespoke to its own requirements, the FCA expects an organisation to adopt a 'security culture' driven from the board and senior management down to employees and has set out some key principles to which firms ought to adhere:

- **Good governance:** with engagement from the board and senior management;
- **Identification and protection of key assets:** for example through defence testing, staff training and security screening;
- **Adequate detection capabilities:** for example through the use of artificial intelligence to detect network vulnerabilities;
- **Recovery and response:** systems and controls to allow a firm to continue operating and protect essential data in the event of an interruption, for example, through upgrading business continuity plans;
- **Information sharing:** while a material breach must be reported under Principle II of the FCA Handbook, firms are also encouraged to share information with others on the Cyber Information Sharing Partnership in order to identify

and tackle patterns of attack.

The key emerging risk areas also identified were:

Ransomware: in particular the risk of self-replicating ransomware which can spread throughout a network;

Data storage / outsourcing: firms adopt the threat profile of cloud based service providers (plus other outsourced services providers), and remain responsible for any data breaches;

The skills gap: initiatives such as the government's FastTrack cyber apprenticeship scheme should be used to help narrow the skills gap.

12.3. National

- Replies from national governments to UN Developments in the field of information and telecommunications in the context of international security (Albania, Australia, Canada, Colombia, Cuba, El Salvador, Finland, India, Japan, Jordan, Lebanon, Poland, Portugal, Serbia, Spain, Switzerland, Togo, Turkmenistan, UK (GB & NI) outlining national priorities and developments.

On 23 December 2015, the General Assembly adopted resolution 70/237, entitled 'Developments in the field of information and telecommunications in the context of international security'. In paragraph 4 of the resolution, the Assembly invited all Member States, to continue to inform the Secretary-General of their views and assessments on the following questions:

- a) General appreciation of the issues of information security;
- b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;
- c) The content of the concepts mentioned in paragraph 3 of the resolution;
- d) Possible measures that could be taken by the international community to strengthen information security at the global level.

Albania

Main priority in the field of security and protection for classified information is the signing of the agreement between the Government of Albania and the EU (signed on 3 March 2016).

In the context of initiating and implementing the appropriate measures in Albania, to strengthen information security and to promote international cooperation in this matter, a revision of the legal statutes was undertaken.

- Council of Ministers decision no. 188, date 4 March 2015, "On the approval of rules ensuring staff security"

- Council of Ministers decision no. 189, dated 4 March 2015, "On ensuring physical security of classified information marked as 'state secret', NATO information"

- Decision of the Council of Ministers no. 190, dated 4 March 2015, "For several alterations and additions on Decision of the Council of Ministers no. 81, 'On defining the criteria and the procedures to destroy classified information'"

- Council of Ministers decision no. 701, dated 22 October 2014, "On approving the rules for securing classified information in the industrial area"

Albania has a more comprehensive legal regulation, which is concerned with the physical security of classified information. The 'areas of security' are defined and located, taking into account the different levels of classified information.

Following the adoption of the new decision for staff security, inter-institutional

cooperation, supervision and the inspection of state institutions have eventually increased. State agencies started the process of revising the lists of staff duties and issuing relevant security certificates according to the field of responsibility. With regard to industrial security, Albania has focused on reviewing politics of information security, by reviewing practices of the Council of Ministers by decision no. 701, dated 22 October 2014.

Another important step on which we have put emphasis, is the drafting of a new law for dealing with classified information – an initiative which constitutes an efficient up to date piece of law with high European standards. The review of national legislation in this field is done taking into account the acquis of the European Union and in particular, Council Decision 2013/488/EU on the security rules for protecting EU classified information.

Australia

Cybersecurity is as intrinsically linked to innovation as it is to national security. It is the bedrock of innovation, growth and prosperity.

Governments, businesses and individuals need to work together to build a trusted online environment. Not only to protect critical information, but to provide the environment for innovation to flourish; to enable the technology industry to thrive; and to capitalise on the growing global need for better cybersecurity solutions, equipment and skilled individuals.

Australia launched its new Cyber Security Strategy on 21 April 2016.

Australia believes that a priority task for the international community is the elaboration of how international law applies to States' behaviour in cyberspace, especially in non-conflict situations.

There is scope for the further development of voluntary norms set out in the 2015 report of the Group of Governmental Experts in relation to the protection of critical infrastructure, computer emergency response teams, the responsibility of States to assist, cooperation on cybercrime and preventing the proliferation of malicious cyber tools and techniques. It is important that work on confidence-building measures moves to the next phase, from the promotion of transparency to the implementation of cooperative measures.

Canada

On cyber issues, Canada believes that:

- A free, open and secure cyberspace is critical to global security, economic prosperity and the promotion of human rights, democracy and inclusion.
- Any approach to tackling cyberthreats must go hand in hand with respect for human rights and fundamental freedoms.
- Existing international law is applicable to the use of information and communications technologies by States.
- Promoting peacetime norms helps sustain an environment in which responsible behaviour guides state actions, sustains partnerships and supports a stable cyberspace.
- Practical confidence-building measures are a proven method to reduce tensions and the risk of armed conflict.

The Canadian Government released its Cyber Security Strategy in 2010 and has continued efforts to help secure Canada's cybersystems and protect Canadians online. Since then Canada has also launched the 'Get Cyber Safe' public awareness

campaign. Recently, the Government has committed to undertaking a review of existing measures to protect Canadians and our critical infrastructure from cyber threats.

At the international level, Canada is active in a number of ways on cyber issues:

- Canada will continue to promote the development of peacetime norms for state behaviour in cyberspace, including the outcomes of the 2012-2013 and 2014-2015 UN Group of Governmental Experts. Canada has been selected to participate in the 2015-2016 Group.

- Canada ratified the Budapest Convention in July 2015. Canada encourages countries to become parties to the Convention, or to use it as a model to implement their own cybercrime laws.

- Since 2007, Canada has committed \$8.25 million to support cybersecurity capacity-building projects in the Americas and South-East Asia

Canada is a founding partner of the Global Forum on Cyber Expertise

- Canada is working with the U.S. to align our cybersecurity public awareness campaign initiatives via the 'Stop. Think. Connect' coalition.

- Canada is also working with the U.S. to implement the Canada-U.S. Cybersecurity Action Plan, which aims to enhance the resiliency of our cyberinfrastructure.

Canada has been working to develop confidence-building measures in various forums, including the Organisation for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations

- Canada supports the North Atlantic Treaty Organisation efforts to strengthen the Alliances' cyberdefence and that of individual allies. Canada has contributed \$1 million to the NATO Cooperative Cyber Defence Centre of Excellence.

- Canada has supported the use of information and communications technologies (ICTs) as tools for development, including to help community organisations deliver essential services such as emergency assistance in conflicts.

Canada's International Development Research Centre has helped to advance development around the work with ICT for development research and capacity-building.

Colombia

Through its 'Vive Digital' Plan (2010 – 2014) and the new Plan 'Vive Digital – para la gente' (2014-2018), Colombia has achieved a digital revolution, increasing its total internet connections from 2.2 million to over 12.2. million in just five years.

It is not possible to maximise the benefits and use of information and communications technologies if citizens or companies cannot trust them, in other words, if there is a perceived lack of security in the digital environment.

National efforts to strengthen information security and to promote international cooperation in this field:

- A new national digital security policy, contained in document CONPES 3854 of 2016, which seeks to ensure that the Government, public and private organisations, law enforcement personnel, academics and individuals in general in Colombia are able to depend on a reliable and secure digital environment that maximises economic and social benefits, boosting competitiveness and productivity in all sectors of the economy. The policy is the result of a process that engaged multiple stakeholders and it is one of the first national policies in the world to incorporate the digital security risk management recommendations issued in September 2015 by the OECD.

Coordination and advisory bodies for digital security will be established at the highest level of government and cross-sectoral liaison units will be set up in all agencies of the national executive branch. Multiple stakeholders will be supported to manage digital security risk in their socioeconomic activities, and to generate confidence in the use of the digital environment by establishing mechanisms for active ongoing participation, ensuring an appropriate legal and regulatory framework and providing training in responsible behaviour in the digital environment. Standing mechanisms will be established, with a strategic focus, to promote cooperation, collaboration and assistance in the area of digital security at the national and international levels.

Cuba

Joint cooperation between all States is the only way to prevent and confront these threats and to avoid cyberspace from turning into a theatre of military operations. The use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of internationally recognised norms in this area and can give rise to tensions and situations that might be detrimental to international peace and security.

The Heads of State and Government of Latin America and the Caribbean, at the second Summit of the Community of Latin American and Caribbean States, held in Havana in January 2014, proclaimed the Latin American and Caribbean region to be a zone of peace, in order to, among other objectives, foster cooperation and friendly relations among themselves and with other nations, irrespective of differences in their political, economic, and social systems or development levels, to practice tolerance and to live together in peace with one another as good neighbours.

In 2016, the importance of information and communications technologies, including the internet as tools to foster peace, human well-being, development, knowledge, social inclusion and economic growth was again highlighted. The peaceful use of information and communication technologies in a manner compatible with the purposes and principles of the Charter of the UN and international law was also reaffirmed.

No reference to positive action, just reference to illegal radio and television broadcasts being made by the U.S. against Cuba.

El Salvador

The El Salvador Armed Forces have upgraded the perimeter security computer equipment and implemented security policies governing access to the computer network's resources (regular changes to user passwords, restriction of access to USB ports and DVD and CD readers, and blocking of access to equipment unit C).

Finland

The following efforts have been taken at the national level:

- 1) the National Cyber Security Strategy of Finland (2013) and its Implementation Programme (2014) define key guidelines and actions in strengthening cybersecurity and resilience. The Implementation Programme is being updated through a consultative multi-stakeholder process with the aim of finalising it in 2016.
- 2) Since the adoption of the national Cyber Security Strategy, Finland has established the National Cyber Security Centre and Cybercrime Prevention Centre, and an Ambassador for cyber Affairs has been appointed. The national Information Security

Strategy was adopted in February 2016.

3) As part of Finnish development cooperation, Finland supports various information and communications technologies (ICTs) for development and cyber capacity-building projects. Finland is a founding partner of the Global Forum on Cyber Expertise. Finland has joined the US led Global Connect Initiative, which seeks to bring 1.5 billion people online by 2020. Finland aims to join the new World Bank Digital Development Partnership Trust Fund. Finland supports internet governance based on a multi-stakeholder model. ~

4) Finland actively engages in international dialogue on cyber issues in multilateral and regional forums, and in bilateral contracts. Within the Organisation for Security and Cooperation in Europe (OSCE), Finland works towards strengthening trust, security and stability in cyberspace and implements the agreed cyber confidence and security building measures.

5) Finland has endorsed the 2015 report of the UN Group of Governmental Experts in the Field of Information and Communications Technology in the Context of international Security. Finland has participated actively in the discussions on international law in cyberspace, e.g. in consultations on Tallinn Manual 2.0 and in UN Institute for Disarmament Research workshops. Finland joined the Freedom online Coalition in 2012 and contributes to the Digital Defenders Partnership.

6) Finland has been a party to the Budapest convention since 2007. The new Strategic Police Plan, targeting resources at computerised crime prevention and developing cybersecurity knowhow was launched in 2015. There is also a Comprehensive Cybercrime Prevention Plan.

Priority areas for further work by the international community:

a) Finland attaches a lot of importance to the work of the new Group of Governmental Experts and is prepared to contribute to its success, including to further the identification of norms of responsible state behaviour in cyberspace with a special emphasis on peacetime activities.

b) Further developing and implementing regional confidence-building measures in the framework of the OSCE

c) Continuing support to cyber capacity-building with a view to strengthening resilience and security in cyberspace

d) Finland will continue to support and encourage multi-stakeholder dialogue. Strengthening public-private partnerships nationally and internationally is a priority.

Japan

Our efforts comply with the following five principles:

- 1) Free flow of information;
- 2) Rule of law;
- 3) Openness;
- 4) Self-governance
- 5) Multi-stakeholder approach

Japanese efforts consist of the following three pillars:

- 1) The rule of law in cyberspace;
- 2) Confidence-building measures;
- 3) Capacity-building.

Japan is engaged in the promotion of confidence-building through bilateral dialogue and multilateral frameworks such as the Regional Forum of the Association of

Southeast Asian Nations. With regard to capacity-building, Japan is actively engaged in human resource development assistance and technical cooperation focussing on the ASEAN region.

Japan urges the need for further elaboration of the deliberation about peacetime rules of international law as well as the development of voluntary norms in the next Group of Governmental Experts. As for confidence-building measures and capacity-building, it is critical to promote the implementation of the recommendations contained in the Group's reports by each State and region. Study on ways to lead tangible cooperation is necessary.

Jordan

The Jordanian Army has played an active and influential role in promoting security and peace at the national, regional and global levels through the development of technology that it employs to secure information and both wired and wireless communication, including the following:

- a) It has updated its communications and information systems by installing protected networks that use encrypted IP technology all over the Kingdom, including at the borders, which it uses to strengthen national and regional security;
- b) It engages in security cooperation with the international community using communications systems that are compatible with those used by the North Atlantic Treaty Organisation and the U.S. Army, and that meet type 1 international encryption standards;
- c) It has improved its technical capacities by acquiring an infrastructure-independent communications system for use in maintaining national security in conflict zones, refugee camps and remote areas. The Jordanian Army also uses that technology in support of peacekeeping operations in conflict zones around the world;
- d) It trains and certifies all communications systems users and maintenance and support personnel without relying on the supplier company, in order to ensure optimum reliability and dependability at all times;
- e) The highest command-and-control standards are applied to all systems used by the military in order to raise the level of national and regional security coordination and cooperation;
- f) It takes active part in international conferences and keeps abreast of their outcomes in order to increase complementarity between friendly armies, avoid interference between communications systems used by neighbouring States in the region and ensure coordinated control and surveillance at international borders. Focus should always be placed on citizen awareness of pervasive cyber threats and how cybersecurity measures when using electronic systems can minimise and counteract those threats. Heightened security awareness while handling any kind of information should not interfere with the benefits of technology

The following measures have been taken to protect vital national information networks:

- a) Encryption is used for all voice, data and video communications systems;
- b) Closed networks (intranets) are used;
- c) Links with other security agencies are established through stand-alone peripheral devices;
- d) Information and Communications security measures and the 'need to know' principles are applied. Access permissions and user identities are checked

continually;

e) Virtual networks are used whereby the user interacts with a screen linked to the network on the basis of access permissions for access to information. Access or connection may not be done via other devices, such as flash drives.

f) It takes active part in international conferences and keeps abreast of their outcomes in order to increase complementarity between friendly armies, avoid interference between communications systems used by neighbouring States in the region and ensure coordinated control and surveillance at international borders. Focus should always be placed on citizen awareness of pervasive cyber threats and how cybersecurity measures when using electronic systems can minimise and counteract those threats. Heightened security awareness while handling any kind of information should not interfere with the benefits of technology.

The following measures have been taken to protect vital national information networks:

a) Encryption is used for all voice, data and video communications systems;

b) Closed networks (intranets) are used;

c) Links with other security agencies are established through stand-alone peripheral devices;

Information and communications security measures and the 'need to know' principle are applied. Access permissions and user identities are checked continually;

d) Information and communications security measures and the 'need to know' principle are applied. Access permissions and user identities are checked continually;

e) Virtual networks are used whereby the user interacts with a screen linked to the network on the basis of access permissions for access to information. Access or connection may not be done via other devices, such as flash drives;

f) Jordan has enacted the following cybersecurity legislation:

1) A law on cybercrimes has been enacted;

2) A law on electronic transactions has been enacted;

3) A national cybersecurity and protection strategy has been drafted;

4) National cybersecurity and protection policies have been drafted;

5) A national cybersecurity and protection strategy was approved by the Cabinet

in 2012;

We propose the following global measures:

a) Communications networks and information should be classified by importance;

b) Cybersecurity and protection measures should be implemented;

c) The need-to-know principle should be applied;

d) Technical measures such as encryption and frequency-hopping should be employed;

e) Users and network access permissions should be verified and categorised;

f) Networks should be linked by stand-alone peripheral devices;

g) Within certain networks, closed intranets should be used, and the World Wide Web should be avoided where possible;

h) The UN intranet should be enhanced and kept separate from public networks. It should be protected through technical and security measures such as encryption, safeguards and verification of access permissions;

i) Cooperation should be promoted among computer emergency response teams to follow up breaches, install safeguards and address gaps;

j) Security measures and procedures for addressing breaches should be circulated

Recommendations:

- a) International response and recovery teams should be formed to address cybersecurity incidents, crises and disasters;
- b) A Jordanian representative should be included in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security scheduled to be formed in 2016
- c) Scientific and research cooperation and training exchanges among the members of the Security Council should be increased.

12.4. Summary – Current Practice

EUROPEAN	
TECHNOLOGY	<p><i>Practical exercises based on realistic attacks, with Member State teams responding to different methods.</i></p> <p><i>Key approach is understanding the extent and type of damage caused by cybercrime. There has to be a continual assessment of the threat landscape in order to tailor an effective response.</i></p>
HUMAN	<p><i>There is a focus on practical application of skills, awareness and training through large scale exercises. Thousands of participants across all sectors and Member States joined together to share expertise.</i></p> <p><i>Other approaches include limiting employee exposure and building a human 'firewall'; make employees part of the solution.</i></p>
ORGANISATIONAL	<p><i>Businesses are a main part of the European approach; they are part of the solution and help to identify main risks. By involving businesses and organisations and adopting their perspectives, a more realistic understanding of the problem can be acquired.</i></p> <p><i>Effective leadership and oversight is a big consideration, as is sharing information with governments and other companies.</i></p>
REGULATORY	<p><i>The Council of Europe has the only internationally binding legal instrument on cybercrime – the Budapest Convention. The EU is also overhauling legislation concerning cybercrime in various ways. Difficulties relate to lack of common understanding of cybercrime.</i></p>

INTERNATIONAL	
TECHNOLOGY	<p><i>States should not allow the development or use of malicious ICT tools and software. Technical skills and protection of ICT infrastructure are raised as pertinent points. International capacity building and the fostering of common understandings of key issues surrounding malicious use of ICT. Privacy by Design concept is promoted.</i></p>
HUMAN	<p><i>Confidence building is seen as an important factor; increasing cooperation and reducing conflict. The social aspects of cybercrime are highlighted. Humans are key to cybercrime, in every way. The sharing and building of skills and the provision of expertise and support on an international level is seen as fundamental. Again, training and awareness raising are referred to.</i></p>

ORGANISATIONAL	<p><i>The openness and security of cyberspace is essential to economic prosperity and G7 values. Again, cooperation and collaboration, as well as information sharing are key features.</i></p> <p><i>In particular, the roles and responsibilities of governments and organisations need to be determined, understood and normalised. This would create a structure on which to build effective resilience with consistent and practical standards and approaches.</i></p>
REGULATORY	<p><i>The ways in which international laws are applied in various states is important and human rights, privacy and freedom of expression must be integrated and accounted for.</i></p> <p><i>Support and information exchange to facilitate successful prosecutions must become an established norm. Advice should be sought on effective legislation, strategies and regulation. The importance of international law is emphasised. The UN Charter and the principle of sovereignty, in particular. The principles of humanity, necessity, proportionality and distinction are highlighted. More nations should sign up to the Council of Europe and the Budapest Convention.</i></p> <p><i>UN resolution 70/237, entitled 'Developments in the field of information and telecommunications in the context of international security' has produced a somewhat unified effort from across the globe in this area.</i></p>

NATIONAL	
TECHNOLOGY	<p><i>Commonly used practices to reduce vulnerabilities, such as isolating parts of networks, restricting access, closed intranets, encryption and frequency-hopping are among very many referred to, and reflect common principles. Encryption standards, as well as structural and organisational built-in measures and practices to improve resilience are focused upon. Also, the use of specific expertise and skills as well as acquiring support and advice from central specialist bodies.</i></p>
HUMAN	<p><i>Training, awareness and increased ICT skills run throughout the information. Key professionals should take part in collaboration efforts to ensure a unified approach and foster common understanding. Although structural defences can be put in place, it is recognised that a single individual can be the weakest link. This is a major challenge.</i></p> <p><i>Confidence building is of central importance and will have a positive effect on other measures and approaches. Collaboration and cooperation on every level underlies most strategies.</i></p>
ORGANISATIONAL	<p><i>Most nations have a cybersecurity strategy in place and policies and practices to give effect to it. The role and responsibility assignment and understanding is key, as well as effective oversight and management of cybercrime.</i></p>
REGULATORY	<p><i>All nations have laws on cybersecurity in place, including regulations pertaining to information, electronic communications and telecommunications.</i></p> <p><i>Many countries adapt current, traditional legislation to fit new</i></p>

offending types.

Rule of law is a consistent, fundamental principle underlying all action. Another consistent theme is the need for human rights and fundamental freedoms to be at the forefront of considerations and approaches.

13. LEGAL FACTORS

13.1. European

Tackling and dealing with cybercrime is of central importance to the EU, as it directly affects the core principles of a single (digital) market and the fundamental rights and freedoms of individuals. In its review in summer 2017, the various agencies and institutions of the EU consistently cited collaboration, integration and cooperation between Member States and international organisations such as NATO and the United Nations. Central to its approach is the Rome Declaration, which underpins the cybercrime strategies that followed. The Rome Declaration that emphasises the need for the growth of the Single Market, while ensuring Europe is a safe and secure Union in which businesses and citizens can be successful.

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Focus on technological protection of the devices and the internet that control so many of today's assets and are a main part of most citizens' lives. Greater resilience and strategic autonomy as well as boosting capabilities relating to technology and skills are seen as key factors. Deterrence, prevention and international cooperation are recurring themes. The approach proposed includes adopting a wide-ranging perspective and developing effective structures that span all sectors in order to achieve common understanding.

- ENISA will coordinate the response and provide support to Member States, Institutions and businesses in key areas. The body will also serve as a knowledge and information point.
- The development of secure technologies and applications is seen as a key area, with incentives such as certification schemes and a 'security by design' approach by developers and manufacturers, as well as those with responsibilities for health care and infrastructure systems.
- Efficient crisis management and response strategies are seen as of major importance, with the emphasis on information sharing and a united response, where required. The Blueprint explains how cybersecurity is mainstreamed into existing Crisis Management mechanisms at EU level.
- The need to drive standards higher is recognised and will be driven forward by the Directive on the Security of Network and Information Systems (the NIS Directive), which will be implemented by Member States in 2018. This will foster improved cooperation between Member States, improve national cybersecurity capabilities and achieve more effective risk management practices across the EU.
- A rapid response depends on effective information flows at national, EU and international levels.
- The importance of research is emphasised and plans for a European Cybersecurity Research and Competence Centre referred to, as well as a network of competence centres to support industry through testing and simulation.

- Strong cyber skills base and education is a strong factor. The requirement for training and education at all levels is recognised, from primary education to top level professionals.
- Different approaches in respect of cyber deterrence are also promoted, this includes more effective law enforcement response focusing on detection, traceability and prosecution. Being caught and sanctioned is seen as the main thing to turn the tide in relation to deterrence. The implementation of the 2013 Directive on attacks against information systems would bring about a uniform approach and understanding of cybercriminal activities, facilitating a more unified response across borders.
- Public-private cooperation is again referred to as an essential element of a more effective response in all areas.

Impact Assessment relating to the EU Cybersecurity Agency (ENISA)

- Interrelated problems, that impact on the overall cyber resilience of the EU, have been identified as:
 - (a) Fragmentation of policies and approaches to cybersecurity across Member States
 - (b) Dispersed resources and approaches to cybersecurity of the EU institutions, agencies and bodies
 - (c) An insufficient awareness of citizens and companies of cyber threats and insufficient information concerning the security properties of the ICT products and services they purchase, coupled with the growing emergence of multiple national and sectoral certification schemes.
- Specific policy objectives of the initiative are the following:
 - (a) Increase capabilities and preparedness of Member States and businesses, in particular regarding critical infrastructures
 - (b) Improve cooperation and coordination across Member States and EU institutions, agencies and bodies
 - (c) Increase EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises
 - (d) Increase awareness of citizens and businesses on cybersecurity issues
 - (e) Increase the overall transparency of cybersecurity assurance of ICT products and services to strengthen trust in the digital single market and in digital innovation
 - (f) Avoid fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors.
- Implementing the NIS Directive is seen as involving the following aspects:
 - (a) Member State's obligation to adopt a national strategy on security of network and information systems
 - (b) The setting up of national competent authorities, single point of contacts and Computer Security Incident Response Teams
 - (c) The security and incident notifications requirements applicable to operators of essential services and to digital service providers
 - (d) The relationship between the NIS Directive and other legislation

Report on compliance by Member States with the NIS Directive

- The NIS Directive has led to substantive progress in criminalising cyberattacks and creating a common understanding of these among Member States, in order to facilitate cross-border cooperation of law enforcement. However, there are improvements to be made so that the Directive can achieve its full potential and aims:
 - (a) Improvement of the use of definitions as laid down in the NIS.
 - (b) In relation to including all the possibilities defining actions in relation to offences and including common standards of penalties for cyberattacks.
 - (c) Implementation of administrative provisions on appropriate reporting channels
 - (d) Monitoring and statistics for the offences included in the NIS Directive.

13.2. International

Developments in the field of information and telecommunications in the context of international security

- The process facilitates the broadest positive opportunities for the development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community. The dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation.

Tallinn Manual Process

The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Authored by nineteen international law experts, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, the updated and considerably expanded second edition of the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare, is an influential resource for legal advisers dealing with cyber issues. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence

- Based on the understanding that cyber operations are conducted by and also directed against, states. Cyber events do not occur in a legal vacuum; states have both obligations and rights under international law.
- The Tallinn 2.0 Manual focuses on events that states encounter on a daily basis, which fall below the thresholds relating to armed conflict or use of force. It covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict. It incorporates the various bases for the exercise of jurisdiction, which is a critical element of cybercrime.
- Areas of law covered include:
 - (a) State responsibility
 - (b) Legal standards for attribution
 - (c) Human rights law
 - (d) Air and space law
 - (e) Maritime law

(f) Diplomatic and consular law

All of these are examined and analysed within the context of cyber operations.

- The Manual is structured around two pillars; the first is research and the results of the research inform the second pillar which is the training pillar, where students keep abreast of the most recent and influential research on the legal issues pertaining to both defensive and offensive cyber operations.
- The Residential Course is offered twice a year, now in Tallinn, Estonia in cooperation with the U.S. Naval War College and the University of Exeter. An indication of the content is:
 - (a) Technical aspects of cyber operations
 - (b) How technical attribution is achieved and challenged
 - (c) Various actors in cyberspace
 - (d) Overview of current status of international cyber affairs
 - (e) Peacetime international law governing cyber operations
 - (f) International humanitarian law that applies during armed conflict involving cyber operations
 - (g) Complex exercise allowing participants to apply the law learned.

14. Overall Summary

The section summaries are arranged around four key areas: Technology, Human, Organisational and Regulatory. This simplification is useful for illustrating themes which can be identified in the approach to tackling cybercrime, from a range of perspectives and objectives, and provides an overview of the current priorities.

The information gathered from various sources range from stakeholder perspectives in 2014 to predictions for the future and while complexities exist in each area, common and consistent topics of relevance can be seen to emerge:

14.1. 'THOR' Summary

TECHNICAL	<p><i>Technology considerations can be understood in terms of:</i></p> <p><i>Those producing hardware and software - Privacy Enhancing Technologies and well-designed systems that factor in security considerations, methods for recovery and which facilitate collection of evidence.</i></p> <p><i>Those managing IT systems - policies, practices and practical arrangements should incorporate information and system security and reflect best practice being promoted and tested.</i></p> <p><i>A thorough understanding of system capabilities and vulnerabilities, along with risk assessments and associated mitigation strategies are key requirements.</i></p> <p><i>LEAs - increased digital skills, along with understanding of the technology involved not only in crimes committed, but in relation to investigation techniques and acquisition of evidence are key areas for LEAs.</i></p>
HUMAN	<p><i>Human factors play an important part in cybercrime topics, from individual responsibility to acquiring relevant expertise and from</i></p>

	<p><i>understanding cyber criminals' motives and behaviours, to predicting next moves.</i></p> <p><i>Another overriding consideration is the balance to be achieved between security and freedom; establishing trust to enable economies to flourish and individuals to lead fulfilling lives is as important as providing protection and ensuring security. These too, are key considerations.</i></p>
ORGANISATIONAL	<p><i>Perhaps the overriding theme that arises from the horizon scanning is the need for collaboration and cooperation on all levels, between all stakeholders and in respect of each of the areas addressed. This culture change needs primarily to occur at organisational level. Connected to this is the need for a shift in culture and norms based on a new, digital reality, which includes shared responsibility and joint effort.</i></p>
REGULATORY	<p><i>Regulations, laws and agreements are the cornerstone for all actions; enabling police to investigate, creating rights, founding collaboration and ensuring standards are maintained. This is an area of constant development as countries across the globe respond to and create acceptable practices and norms.</i></p> <p><i>Within and underlying all activities must be the principle relating to the rule of law. The protection of human rights and fundamental freedoms must run throughout all areas relating to cybercrime and its response.</i></p> <p><i>A key difficulty is the difference between legislation in different jurisdictions; this is perpetuated by the lack of common understanding and definition of cybercrime and differing perceptions of its impact.</i></p>

Annex 7

COUNTER TERRORISM

**International Security Management Knowledge Alliance (ISM-KA)
Addressing Security Challenges in an Interconnected World**



WP2 Counter Terrorism Module

Document Summary Information

Authors and Contributors

Initials	Name	Organisation	Role
Raymond Brown	RB		

Version control				
DATE	AMENDED BY	SECTIONS AMENDED	REASON FOR AMENDMENT	NEW VERSION
21/11/17	RB	1. Module Des - a,b,c,f, Thor. 2. Desk Based Res Com- d, Reports a, b. 3. Current Courses - a,c,d. 6. Current Policies - a, b.	ISPC Review (BVJ)	1.1
06/03/17	RB	3. Current Courses -a.	New Material	1.2

Quality Control

Role	Date	Who	Approved/Comment

1. Module Descriptor

Module Name	Counter Terrorism
Module Aim	This module will provide insight into the fundamental issues in international terrorism, including Terrorist Modus Operandi, Terrorist Ideologies, Aims, Beliefs, Motivations, Counter Terrorism Strategy, Human Rights, Terrorist Financing, Border Security and Radicalisation.
Learning Outcomes	
LO1	Understand the role and impact of terrorism on the international community.
LO2	The threat to the international community and key features of an effective international response to terrorism.
LO3	Emerging trends in terrorism in the 21st century.
LO4	The background and characteristics of the international terrorist threat from terrorist organisations such as Al Qaeda, ISIS, Taliban, Boko Haram, Hamas and Hezbollah.
Indicative Content	<ul style="list-style-type: none"> Ideologies that motivate individuals and organisations to resort to terrorism. The use of various propaganda methods such as the internet, by terrorist organisations and examining the global trends in terrorism. To provide students with an awareness of the functions that comprises of government and law enforcement responses, to international terrorism and considers the challenges to protect the international community from the threat of terrorism. Students will consider and critically engage with and challenge common understandings of radicalisation and deradicalisation, in order to contribute to the improvement of the counter-radicalisation, deradicalisation and disengagement initiatives that play a crucial role in reducing the terrorist threat. Participants will be introduced to the role that terrorist legislation and human rights standards, contributes in combating international terrorism, both in terms of the obligations, that they impose on governments and law enforcement, to protect citizens from harm and in terms of the constraints they place on the counter terrorism tactics that nations may adopt. The question of how global information and intelligence sharing, supports numerous efforts to counter the international terrorist threat and the challenges of adapting to these challenges in today's world.

HORIZON SCANNING

2. Current Courses

2.2 Current Courses

Masters courses

- MSc (University of Portsmouth) Security Management
<http://www.port.ac.uk/courses/law-and-criminology/msc-security-management/>
- [International Security - University of Groningen, Groningen](#)
- [University Autònoma de Barcelona - \(UAB\) Barcelona](#)
- [MA in International Terrorism - University of Copenhagen, Copenhagen, Denmark.](#)
- [International Relations - University of Bologna, Bologna Italy.](#)
- [MLitt Terrorism and Political Violence - University of St Andrews](#)
- [MA Violence, Terrorism and Security - Queens University Belfast UK](#)
- [Security, Terrorism and Insurgency - University of Leeds](#)
- [MA International Security and Development - Swansea University](#)
- <http://www.coventry.ac.uk/course>
- [http://www.mastersportal.eu/studies/76413/international-security.](http://www.mastersportal.eu/studies/76413/international-security) - MSc (Walden University) International Security and Global Governance (USA)
- <https://www.fsv.cuni.cz/en/miss> - Master in International Security Studies (MISS) Charles University, Prague (Czechoslovakia)
- [http://www.mastersportal.eu/studies/61896/international-conflict.](http://www.mastersportal.eu/studies/61896/international-conflict)
- [International Conflict and Security - MA - Brussels ... - University of Kent](#)
- [http://www.mastersportal.eu/studies/152070/international-security.](http://www.mastersportal.eu/studies/152070/international-security)Paris

2.2 CPD Courses

- [Counter terrorism | College of Policing](#)
- [Certificate Course in Combating the Financing of Terrorism](#)
- [Counter Terrorism Conference 2017: Stopping the evolving threat ...](#)
- [Certificate Course in Combating the Financing of Terrorism.](#)
- Certificate in Security Management (BTEC level 3)
[https://www.security-institute.org/qualifications/certificate.](https://www.security-institute.org/qualifications/certificate)
- Security Institute Diploma in Security Management (BTEC level 5)
[https://www.security-institute.org/qualifications/diploma.](https://www.security-institute.org/qualifications/diploma)
- <http://www.perpetuitytraining.com/syisecurityinstitute.html> - The Security Institute qualifications for practitioners in security
- The Prevent Duty - CPD Courses - Reach 4 Skills
- Prepare for Prevent - SSS CPD Training & Assessment

3. Stakeholder Perspectives

3.1. *Institutional Bodies*

- Royal United Services Institute - (RUSI - World's oldest independent think tank on international affairs and security.
- Chatham House: Counter Terrorism
- Hear from our Students - University of St Andrews
- MA Violence, Terrorism and Security | Postgraduate Taught Course
- International Institute for Strategic Studies (IISS)

3.2. *Law Enforcement*

- Policing Insight - Governance, management and politics. UK
- Police Oracle - News Overview UK
- The Counter Terrorist Magazine USA
- The IACSP's Counter-Terrorism Journal V19N2 by IACSP - USA
- Organization for Security and Co-operation in Europe -OSCE
- Events | Europol
- United Nations Security Council
- NATO - Topic: Countering terrorism

3.3. *Businesses and NGO's*

- New US counterterrorism NGO working to expose terrorist financing
- Fighting Fire with Water: NGOs and Counterterrorism Policy Tools.
- The Increasing Threat of Cyber Terrorism in the UK - 2 Sec
- What tech companies share with police to combat terrorism
- Terrorism is now a key business risk and too many companies are insufficiently prepared.

4. Current Research

- <http://www.europarl.europa.eu/news/en/headlines/priorities/20151125TST04632> - How is Europe fighting terrorism
- <http://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12249/full>, - Terrorist use of the Internet
- <http://www.europarl.europa.eu/news/en/headlines/security/20160708STO36564/terrorism-82-of-europeans-want-eu-to-do-more-to-tackle-threat> - Terrorism continues to pose a threat to Europe

4.1. *Statistics*

- Global Terrorism Database - The GTD is an open-source database
- Global Terrorism Index 2016 - Institute for Economics and Peace
- Terrorism in Great Britain: the statistics - Commons Library briefing.

- [Counter terrorism statistics - GOV.UK](#)
- [YouGov | Terrorist attack in Britain expected by 84% of people](#)
- [UK Terrorism Stats: 97% Are Muslim, Majority of 'Domestic Extremists.](#)
- [Jane's Terrorism & Insurgency Centre](#)

4.2. Reports

- [CONTEST, UK strategy for countering terrorism: annual report for 2015.](#)
- [Reports | Counter-Terrorism Implementation Task Force - K UN.ORG](#)
- [Independent Reviewer of Terrorism Legislation - GOV.UK](#)
- [https://www.europol.europa.eu/about-europol/eu-internet-referral-unit.](https://www.europol.europa.eu/about-europol/eu-internet-referral-unit)
- <http://journals.sagepub.com>
- [Refworld | Country Reports on Terrorism 2015 - Denmark](#)
- [NATO - Topic: Countering terrorism](#)
- [Countering terrorism | OSCE](#)
- [Global Terrorism and Insurgency - News and Defence ... - Jane's 360](#)

5. Current Policies

5.1. Government & Institutions

- <http://www.europarl.europa.eu/news/en/headlines/security/20170324STO68406/security-we-need-to-work-quickly-and-effectively-in-order-to-combat-terrorism> - civil Liberties Committee collaborate with EU Minister
- [Home Office - GOV.UK](#)
- [CONTEST, UK strategy for countering terrorism: annual report for 2015.](#)
- [http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator.](http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator)
- [http://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list.](http://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list)
- [Stockwell 1 – the recommendations | Independent Police Complaints.](#)
- [Implementing 9/11 Commission Recommendations | Homeland Security](#)
- [UN Global Counter-Terrorism Strategy - the United Nations](#)

5.2. Industry

- [G4S United Kingdom](#) - G4S is the leading global integrated security company, specialising in the provision of security products, services and solutions.
- [Serco Group Plc](#) - Serco specialise in the delivery of essential public services, working in defence, transport, justice, immigration, healthcare and other citizen services.
- [Securitas AB - Securitas](#) - Securitas AB offer a broad range of services of specialised guarding, technology solutions and consulting and investigations.
- [Hijack Exercise](#) - One of Green Light's flagship programmes is its Hijack Exercise - London - UK.

5.3. *Law Enforcement*

- [Stay Safe - The National Police Chiefs Council - NPCC](#)
- Terrorism MI5 - Security Service - International Terrorism.
- [Internet / Home - INTERPOL](#)
- [Europol: Home](#)
- <https://www.europol.europa.eu/about-europol/eu-internet-referral-unit-eu-iru#fndtn-tabs-0-bottom->
- [National Crime Agency - Home](#)

6. Current Practice

6.1. *European*

- [http://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing.](http://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing)
- [http://www.consilium.europa.eu/en/policies/fight-against-terrorism/foreign-fighters.](http://www.consilium.europa.eu/en/policies/fight-against-terrorism/foreign-fighters)
- [Netherlands' Unit Interventie Mariniers counter terror exercise](#)
- [National Guard at international counter terrorism exercise in Sweden.](#)
- [OSCE Counter-Terrorism Conference 2017 in Vienna | OSCE](#)
- Action against Terrorism Unit - Organization for Security and Co www.osce.org.
- [A new EU counter-terrorism unit will tackle extremists online Security.](#)

6.2. *International*

- [Nobody panic! Washington DC holds 'full scale terror attack' drill.](#)
- [The U.S.–Yemeni Joint Counterterrorism Exercises: The Other Side](#)
- [Singapore stages biggest islandwide counter-terrorism.](#)
- [SONA: Phl Air Force, Navy at Marines, sumabak sa anti-hijacking.](#)
- [Panic at Lagos Airport as Nigerian Air Force Carries Out Counter](#)
- [India, Oman to hold counter-terror exercises -](#)
- [Governor Cuomo Announces Over 600 Joint Counter Terrorism - 28 Dec 2016 - New York - USA.](#)
- [Counter terrorism - British Transport Police](#)

6.3. *National*

- [Terror training exercise staged at Trafford Centre | UK news.](#)
- [Met officers hold mock terrorism exercise on River Thames - BBC News](#)
- [PM announces major counter- Terrorism training exercise in Scotland.](#)
- [TERROR EXERCISE IN LONDON - YouTube 1/07/2015 - Operation -Strong Tower. The largest counter terrorism exercise the UK.](#)

7. Legal Factors

7.1. *National*

- [Investigatory Powers Act 2016 - Legislation.gov.uk](#)
- [RIPA codes - GOV.UK](#)
- [Regulation of Investigatory Powers Act 2000 - Legislation.gov.uk](#)
- [Law and Governance | MI5 - The Security Service](#)
- [Justice and Security Act 2013 - Legislation.gov.uk](#)
- [Criminal Procedure and Investigations Act 1996 - Legislation.gov.uk](#)
- [Serious Crime Act 2007 - Legislation.gov.uk](#)
- [The Terrorism Acts in 2015 - GOV.UK](#)
- [Schedule 7 Code of Practice - GOV.UK](#)
- [Extradition of Abu Hamza and four others for terrorism offences can go.](#)
- [Police and Criminal Evidence Act 1984 - Legislation.gov.uk](#)

7.2. *European*

- [EU counter-terrorism law opens door to discrimination.](#)
- [EUROPA - EU law - EU counter-terrorism laws "stripping rights", says Amnesty - EU observer](#)
- [Changing Turkey's anti-terror laws would threaten EU security.](#)
- [France extends draconian anti-terrorism laws.](#)
- [Netherlands - Counter-Terrorism - Legislation line - Counter-Terrorism › Netherlands \(Crimes of Terrorism Act\) \(2004\).](#)

7.3. *International*

- [UNITED NATIONS ACTION TO COUNTER TERRORISM - K UN.ORG](#)
- [Defining Terrorism in International Law - Oxford Scholarship - Despite numerous efforts since the 1920s, the international community has failed to define or criminalise 'terrorism' in international law.](#)
- [Status of the Universal Anti-Terrorism Conventions and Protocols.](#)
- [Fact Sheet: Impact of Warrantless Section 702 Surveillance on People -](#)
- [From a War on Terrorism to Global Security Law | Institute for Advanced Study \(IAS\).](#)
- [Legislation line. - Legislation and international standards relating to human rights topics. Constitution, criminal and criminal procedure codes.](#)
- [Notices / INTERPOL expertise / Internet / Home - INTERPOL -](#)
- <https://www.interpol.int/INTERPOL-expertise/Notices>
Cyberspace, Terrorism and International Law

8. Current Courses

8.1. *Master Programmes*

The following summary of information was gained from current modules on Masters Programmes;

- Fundamental Issues in International Terrorism
- Terrorist Ideologies, Aims, Beliefs and Motivations
- Terrorist Modus Operandi
- Radicalisation, Counter-radicalisation and Deradicalisation
- Improvised Explosive Devices (IED's) : Threats and Counter measures
- Psychology of Terrorism
- Aviation Terrorism & Security
- Maritime Terrorism & Security
- CBRN Weapons in Terrorism
- Cyberterrorism, Terrorist Use of ICT and Cybersecurity
- International Policing Policy
- Intelligence
- Terrorism and Human Rights
- Homeland Security
- Critical Infrastructure Protection
- Personnel and Personal Security
- Terrorist Financing
- Suicide Terrorism
- 'Lone Wolf' Terrorist attacks
- Territory and Border Security
- Economic Security
- Environmental Security
- Legislation
- Advanced Policing

8.2. *Professional Development Courses*

The following is a summary of information that was gained from content on professional development courses, such as Certificate in Terrorism studies and Continuous Professional Development (CPD) courses. For example;

- Terrorist finance
- Security Management
- Anti-Terrorism Courses
- Counter Terrorism Strategies course i.e. UK's Contest Strategy.
- Terrorist Ideologies, Aims, Beliefs and Motivations
- Aviation Terrorism and Security
- Maritime Terrorism and Security
- Cyberterrorism, Terrorist Use of ICT and Cybersecurity

- Intelligence
- Covert Investigators course

8.3. THOR Summary - Current Courses

MASTER'S PROGRAMMES	
TECHNICAL	<ul style="list-style-type: none"> • Cyberterrorism, • Terrorist Use of ICT • Cybersecurity • Improvised Explosive Devices (IED's): Threats and Counter measures • Technical Surveillance
HUMAN	<ul style="list-style-type: none"> • Terrorism and Human Rights • Radicalisation, Counter-radicalisation and Deradicalisation • Terrorist Ideologies, Aims, Beliefs and Motivations • Territory and Border Security
ORGANISATIONAL	<ul style="list-style-type: none"> • Homeland security • National Security • Aviation Security • Maritime Security • Intelligence
REGULATORY	<ul style="list-style-type: none"> • Terrorist legislation • Human Rights legislation • Surveillance legislation • Terrorist Finance

PROFESSIONAL DEVELOPMENT COURSES	
TECHNICAL	<ul style="list-style-type: none"> • Cyberterrorism, • Terrorist Use of ICT • Cybersecurity • Improvised Explosive Devices (IED's): Threats and Counter measures • Technical Surveillance
HUMAN	<ul style="list-style-type: none"> • Terrorism and Human Rights • Radicalisation, Counter-radicalisation and Deradicalisation • Terrorist Ideologies, Aims, Beliefs and Motivations • Security Management • Anti-Terrorism Courses
ORGANISATIONAL	<ul style="list-style-type: none"> • Homeland security • National Security • Aviation Security • Maritime Security • Intelligence
REGULATORY	<ul style="list-style-type: none"> • Terrorist legislation • Human Rights legislation

- *Surveillance legislation*
- *Terrorist Finance*

9. Stakeholder Perspectives

A summary of information identified from a variety of sources which identified areas of priority or particular challenge:

9.1. *Counter Terrorism Strategy*

- The continual review and improvement of a Counter Terrorism (CT) Strategy is crucial for Governments and Law Enforcement. The majority of democratic governments have a CT Strategy in place, with large respected organisations, such as the Organisation for Security and Co-operation in Europe (OSCE) having a CT strategy.
- Terrorism is recognised as one of the most significant threats to peace, security and stability in the world today. Terrorism seeks to undermine the very values that unite society. At the same time, citizens unequivocally reject the association of terrorism with any particular race, nationality or religion. On 17th October 2017, the UK's, MI5 (Security Service, Director General, Andrew Parker stated that, "*Today there is more terrorist activity, it's coming at us more quickly and it can be harder to detect.*" From data collected, having a CT strategy is crucial when implementing effective measures to prevent and combat terrorism. For example the UK has CONTEST as its CT strategy. It was first developed by the Home Office in early 2003. The aim of the strategy is, to reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence. CONTEST is split into four work streams that are known within the counter-terrorism community as the 'four P's': *Prevent, Pursue, Protect, and Prepare*. These pillars are also the same for Spain, as part of their Spanish National Security Strategy.
- Other countries in Europe have similar CT Strategies, such as Spain and organisations such as the United Nations (UN) have also adopted a CT Strategy. Another example is the International Association for Counterterrorism and Security Professionals (IACSP). It believes that all elements of the world's societies must become better educated about the threats of terrorism as a first step toward developing innovative and effective counter-measures to combat ongoing terrorist threats. (A1)

9.2. *Radicalisation*

- Organisations and Governments should continue to shape responses to violent extremism and terrorism not only with research but also with projects designed to prevent people being drawn into terrorism. For example, the Royal United Services Institute (RUSI), the world's oldest independent think tank on international affairs and security has implemented the EU's first external Countering Violent Extremism (CVE) intervention in Kenya and Somalia and is now one of the most influential organisations working on CVE in East Africa.
- Similar organisations and government can improve their contribution, using their expertise, assisting in CVE, incorporating research, policy analysis, programme

implementation, training and education. The RUSI's CVE work reaches across the world, with particular emphasis on the UK, Europe, Middle East, East Africa, and Central Asia. Training in CVE is also assessed as being a critical factor.

- The number of potential extremists flagged up by the public to the UK government's anti-radicalisation, 'Prevent', scheme has doubled since the UK was hit by a flurry of recent terrorist attacks. Police received about 200 referrals to the programme from within communities between April and the end of July 2017. This is compared with about 100 recorded in the previous four months.
- Radicalisation prevention plans. For example, in Catalonia, Spain, the public education system has been working on a jihadist radicalism prevention plan, within schools together with a prevention plan against hate and discrimination situations. This plan has been developed in collaboration with the 'Catalan' Police Force (Mossos d'Esquadra). (A1)

9.3. *Online Terrorist Propaganda*

- EU countries, including LEA's such as Europol and Interpol are concerned about violent extremist, online content. To illustrate, collaboration with Finland, Luxembourg, the Netherlands, Interpol and Europol, coordinated a two-day joint operation, during which 1628 pieces of terrorist and violent extremist online content were assessed for the purpose of referral to online platforms. The activities focused mainly on the online production of terrorist material by IS and al-Qaeda affiliated media outlets. The processed content had been hosted by 38 online platforms.
- A particular finding of this operation was the identification of terrorist content on the Darknet i.e. links to open web shared on designated Darknet libraries. The Internet has become a strategic device for terrorists, used to identify, recruit and train new members, collect and transfer funds, organize terrorist acts, incite violence and increasingly as a weapon for cyber-attacks - complementing international efforts already existing in this field.
- Government and organizations can also continue to provide a platform for experts, civil society and the business community to identify and share best practices and promote human rights in the fight against terrorism use of the Internet.
- It is worthy to note the EUROPOL, Internet Organised Crime Threat Assessment (IOCTA) 2017 states, "While terrorists continue to use the internet mostly for communication, propaganda and knowledge sharing purposes, their capabilities to launch cyber-attacks remain limited." (A2)

9.4. *Finance*

- The financing of terrorist organisations is an important issue, where finance is made available to provide support to terrorist organizations to facilitate their ongoing terrorist activity. Governments and organisations such as the USA counter terrorism NGO, are working to expose terrorist financing worldwide. This new counter terrorism NGO, led by international leaders and former diplomats is called the Counter Extremism Project (CEP). The project seeks to target the growing threat from Islamist groups on multiple fronts, one of which is exposing their financing networks.

- NGOs are particularly well suited to combating network-type terrorist groups like al-Qaeda and its franchises because such groups depend on complicit society. Here NGOs have distinct advantages because of their potential to credibly challenge terrorist narratives on the ground. However, continued financial investigations/monitoring by government/financial institutions/NGO's and LEA are required. (A2)

9.5. *Terrorism is a key business risk*

- The business community takes the impact of terrorism seriously. Terrorism is now a key business risk with too many companies insufficiently prepared. To illustrate, Terrorism as a threat has clearly registered with the UK's top executives.
- Along with fraud, regulation and reputation, it's up there as a major risk that could damage their business and worse, harm the public and their employees. Continued improved collaboration and communication between government, LEA's and the business community are required. (A2)

9.6. *Human Rights*

- Human Rights are a critical requirement to improve Law Enforcement Agencies (LEA) practice and to assist law enforcement practitioners. In strengthening their compliance with human rights legislation, policies, procedures and international human rights standards, in the investigation of terrorism-related crimes, the human cost of terrorism has been felt in virtually every corner of the globe.
- Terrorism clearly has a very real and direct impact on human rights, with devastating consequences for the enjoyment of the, right to life, liberty and physical integrity of victims. In addition to these individual costs, terrorism can destabilise Governments, can undermine civil society, jeopardise peace and security and threaten social and economic development. All of these have a real impact on the enjoyment of human rights.

Security of the individual is a basic human right and the protection of an individual is, accordingly, a fundamental obligation of Government. Countries have an obligation to ensure the human rights of their nationals and others, by taking positive measures to protect them against the threat of terrorist acts and bringing the perpetrators of such acts to justice. In recent years, however, the measures adopted by countries to counter terrorism have themselves often posed serious challenges to human rights and the rule of law.

- Some countries have engaged in torture and other ill-treatment to counter terrorism, while the legal and practical safeguards available to prevent torture, such as regular and independent monitoring of detention centres have often been disregarded.

Other countries have returned persons suspected of engaging in terrorist activities to countries

where they face a real risk of torture or other serious human rights abuse, thereby violating international legal obligations. 'Anti-terror measures violate civil liberties'. This was raised in a Human Rights Watch article: <https://www.hrw.org/news/2017/09/25/frances-counterterrorism-bill-normalizes-emergency-practices> (A1)

9.7. *State terrorism*

It is a challenging concept. However, we should consider that terrorism is not just a “non-state actor concept” but a more comprehensive one that should include the state as well. (A1)

9.8. THOR Summary - Stakeholder Perspectives

STAKEHOLDER PERSPECTIVES	
TECHNICAL	<p>From a technical perspective the <u>Internet</u>, as a strategic device for terrorists was cited as a serious concern, in particular;</p> <ul style="list-style-type: none"> • use of the Darknet • as a device to identify, recruit and train new members • collect and transfer funds • incite violence • as a weapon for cyber-attacks (although the capabilities to launch cyber-attacks appear to remain limited at present) • Government and Law Enforcement Agencies (LEA's) should continue to provide a platform for experts, public and the business community, to identify and share best practices and promote human rights in the fight against terrorism use of the Internet. • A stronger awareness of how terrorists exploit the internet should be considered and taught to stakeholders.
HUMAN	<ul style="list-style-type: none"> • Complying with <u>Human Rights</u> was cited as a continued critical requirement to improve LEA's practice and to assist law enforcement practitioners. • There were serious concerns around countering violent extremism. • Issues in relation to the potential reluctance to report suspected terrorist activity needs to be continued to be addressed. • Human elements play a significant part in enhancing the capability of LEA's in the fight against terrorism, mainly in connection with improving the quality of investigations, communication and information sharing with the public, as well as the need, to continue to enhance their knowledge of human rights legislation and countering violent extremism. • Further awareness, education and training required in the area of Human Rights, Radicalisation and Countering Violent Extremism.
ORGANISATIONAL	<ul style="list-style-type: none"> • Organisations need to ensure that they are aware of their countries, Counter Terrorism (CT) Strategy. • It was cited that from an organisational perspective, that Terrorism is a key business risk, with too many companies are insufficiently prepared. • Along with fraud, regulation and reputation, it's a major risk that can damage an organisations business and worse, harm the public and their employees. • <u>Financing</u> of terrorist organisations was viewed as an important issue. All organisations need to be aware of this issue. • Organisations also have serious concerns on radicalisation and <u>countering</u>

	<p><u>violent extremism.</u></p> <ul style="list-style-type: none"> • Ongoing education, training collaboration and communication between government, LEA's and the business community is required regarding, terrorism, terrorism finance, countering violent extremism and being aware of CT strategy. • State Terrorism: we should consider that terrorism is not just a "non-state actor concept" but a more comprehensive one that should include the state as well.
REGULATORY	<ul style="list-style-type: none"> • Regulatory and legal implications around areas such as human rights, surveillance, data protection and privacy need to be considered. • With Governments having in place CT strategies, legislation should be 'fit for purpose' and 'human rights' compliant. Terrorism Regulations, Legislation, Policy and Procedures should be reviewed regularly. • Ongoing education and training should be considered regarding Legislation on Terrorism, Terrorism Finance, Human Rights and being aware of CT Policies and Procedures.

10. Background

10.1. Current Research

Database

- Current terrorism statistics and data bases are important to LEA, Government, Academia and the Private Sector. The Global Terrorism Database (GTD) is an open-source database including information on terrorist events/trends around the world from 1970 through 2016 (with annual updates planned). Unlike many other event databases, the GTD includes systematic data on domestic as well as international terrorist incidents that have occurred during this time period.
- Statistical information contained in the GTD is based on reports from a variety of open media sources. Information is not added to the GTD unless and until the sources are assessed as credible. In the year ending March 2017, arrests for international terrorism accounted for the majority of all arrests (75%) and arrests for domestic terrorism accounted for 16% of all arrests.
- In 2000 there were nearly 2,000 deaths of private citizens from terrorist attacks. This increased to over 12,500 in 2015, representing an increase of 550 %. It is also worthy to note the continued terrorism tactic of 'Suicide and 'Lone Wolf' attacks and that large scale and mass casualty terrorist attacks are anticipated to continue. (A2)

Border Security

- Border security is vital to any country to thwart the terrorist threat. The EU Parliament as reiterated concerns regarding EU citizens becoming radicalized and travelling to fight in Iraq or Syria and continue represent a growing threat to the EU.

- Most of the recent terrorist attacks in Europe were perpetrated by home-grown terrorists. MEPs have adopted new rules to ensure stronger checks at the EU's external borders and prevent the preparation of terrorist acts. The new directive on combating terrorism is intended to be a valuable tool in tackling the phenomenon of aspiring or returning foreign fighters and so-called "lone wolves". An estimated 5,000 Europeans have joined conflicts in Iraq and Syria, with the majority of them originating in four EU countries, namely France, UK, Germany and Belgium.
- An EU survey has also showed that the majority of people think the fight against terrorism should be the EU's main priority for more action. Respondents considered the following measures to be the most urgent: fight against the financing of terrorist groups, fight against the roots of terrorism and radicalisation and strengthening border controls. (A1)

Online Terrorism

- The public interest and policy debates surrounding the role of the Internet in terrorist activities continue to increase.
- Results suggest that extreme right wing individuals, those who planned an attack (as opposed to merely providing material support), conducted a lethal attack, committed an improvised explosive device (IED) attack, committed an armed assault, acted within a cell, attempted to recruit others and engaged in non-virtual network activities and non-virtual place interactions were significantly more likely to learn online compared with those who did not engage in these behaviours. (A1)

Law enforcement training research

The H2020 TARGET project is developing "the use of Augmented and Virtual Reality and serious gaming techniques for the training and competence assessment of Security Critical Agents (SCA), including first responders (police, fire, emergency medical services), counter terrorism units, border guards and critical infrastructure operators." They are developing six scenarios to improve the training on the LEAs in case of a major event. More information on the project can be found on <http://www.target-h2020.eu>. (A1)

10.2. Reports

Government and Organisational Responses

- Countries and organisations around the world have their own responses to Terrorism. Having a CT Strategy appears to be a common thread. To illustrate the UK has its own CONTEST strategy which aims to reduce the risk to the UK and its interests overseas from terrorism so that people can go about their lives freely and with confidence. CONTEST deals with all forms of terrorism and continues to be based around four strands: *Pursue*: the investigation and disruption of terrorist attacks; *Prevent*: work to stop people becoming terrorists or supporting terrorism; *Protect*: improving our protective security to stop a terrorist attack and *Prepare*: working to minimise the impact of an attack and to recover as quickly as possible.
- The UK National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR), set out the Government's vision for a secure and prosperous UK with a global reach and

influence. Terrorism remains one of the highest priority risks to the UK's national security. Tackling terrorism at home and abroad through CONTEST is one of the UK's priorities.

- Canadas CT Strategy is centred around building resilience against Terrorism and has four mutually reinforcing elements: prevent individuals from engaging in terrorism; detect the activities of individuals and organizations who may pose a terrorist threat, deny terrorists the means and opportunity to carry out their activities and respond proportionately, rapidly and in an organized manner to terrorist activities and mitigate their effects.
- Australia's CT Strategy is centred on five core elements: challenging violent extremism ideologies, stopping people becoming terrorists, shaping the global environment, disrupting terrorist activity within Australia and effective response and recovery.
- The EU CT Strategy has as its pillars Prevent, Protect, Pursue and Respond. These are also the same four pillars used in Spain, for its Spanish Security Strategy, aligned with the EU strategic commitment to combat terrorism globally.
<https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204>
- The United Nations (UN) comments that member states repeatedly cite terrorism as a major threat to international peace and security. Addressing this threat is a priority of the UN through its Global Counter-Terrorism Strategy. Terrorists' use of the internet and social media has increased significantly in the recent years. Jihadist groups in particular, have demonstrated a sophisticated understanding of how social networks operate. They have launched well organized concerted social media campaigns to recruit followers and to promote or glorify acts of terrorism or violent extremism. (A1)

Legislation

- Internationally, within Europe and the UK, Terrorism legislation is an essential ingredient in the challenge of defeating terrorism. For example, Denmark continue to use its 2006 terrorism legislation that allows enhanced information sharing between Denmark's two intelligence services (PET) and the Danish Defense Intelligence Service (DDIS). The legislation also permits official surveillance and wiretapping of terrorist suspects with a valid warrant. Danish security and law enforcement organizations engage, in information sharing through the Center for Terror Analysis (CTA), the Danish government's intelligence fusion center, which merges reporting from PET, DDIS, the Ministry of Foreign Affairs and the Danish Emergency Management Agency.
- The UK has the Regulation of Investigatory Powers Act 2000 (RIPA) regulating the powers of public bodies, to carry out surveillance and investigation and covering the interception of communications. It was ostensibly introduced to take account of technological change such as the growth of the Internet and strong encryption.
- In 2015, Spain fully modified the terrorism articles in its criminal law. It expanded the scope of conduct which might be considered under the terrorism category. One of the main reforms was the consideration of cybercrime as terrorism, when used for terrorist purposes. It was a great step forward in the field of cyber prevention of terrorism. Later in the same year, with the last reform, the "reviewable permanent prison" sentence was included as an option for terrorism related crimes.
- Other factors that require continued appropriate legislation, policy and procedures include;
 - Countering violent extremism and radicalisation that lead to terrorism, following a multidimensional approach,
 - Preventing and suppressing the financing of terrorism,
 - Countering the use of the Internet for terrorist purposes,
 - Promoting dialogue and co-operation on counter-terrorism issues, in particular, through public-private partnerships between State authorities

and the private sector (business community, industry), as well as civil society and the media,

- Strengthening travel document security and
- Promoting and protecting human rights and fundamental freedoms in the context of counter-terrorism measures. (A1)

10.3. THOR Summary - Background

Current Research	
TECHNICAL	<ul style="list-style-type: none"> • Research as indicated that terrorism, national and global statistics and <u>data bases</u> are important, to identify trends and methodologies. • <u>Online</u> - extreme right wing individuals, those who planned a terrorist attack conducted a lethal attack, committed an improvised explosive device (IED) attack, committed an armed assault, acted within a cell, attempted to recruit others and engaged in non-virtual network activities and non-virtual place interactions, were significantly more likely to learn online.
HUMAN	<ul style="list-style-type: none"> • Multidisciplinary approaches, including information sharing and communication are 'Golden Threads', identified as a positive contributory factor, in successfully combating terrorism, terrorism finance, radicalisation and countering violent extremism.
ORGANISATIONAL	<ul style="list-style-type: none"> • A Counter Terrorism (CT) Strategy, is a theme that's appears as a common approach to countries and international organisations. • European Union (EU) Citizens indicated that the majority of people think the fight against terrorism should be the EU's main priority.
REGULATORY	<ul style="list-style-type: none"> • Border security is vital asset to any nation, to thwart the terrorist threat. The EU Parliament as reiterated concerns regarding EU citizens, becoming radicalized and travelling to fight in Iraq or Syria and continue to represent a growing threat to the EU. • New EU regulations are now in place to ensure stronger checks on EU borders.

Reports	
TECHNICAL	<ul style="list-style-type: none"> • The United Nations (UN) Global CT Strategy - Terrorists' use of the <u>internet</u> and <u>social media</u> has increased significantly in the recent years. Jihadist groups in particular, have demonstrated a sophisticated understanding of how social networks operate. • It is assessed that the terrorist use of the <u>internet</u> and <u>social media</u> will continue to increase. Stakeholders should be aware of this important issue.
HUMAN	<ul style="list-style-type: none"> • The UK, National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR), set out the Government's vision for a secure and prosperous UK, with a global reach and influence. Tackling terrorism at home and abroad through CONTEST (CT Strategy) is one of the UK's priorities.

	<ul style="list-style-type: none"> • <i>The threat of terrorism is also a priority for the UN, which has in place its own 'Global Counter Terrorism Strategy',</i>
<p>ORGANISATIONAL</p>	<ul style="list-style-type: none"> • <i>The UK's CT Strategy, CONTEST requires and needs stronger, information sharing and collaboration between LEA's and the public in the fight against terrorism. Having a CT strategy in place creates a structured and co-ordinated response to combatting terrorism.</i> • <i>Having the CONTEST strategy, aims to reduce the risk to the UK and its interests overseas from terrorism so that people can go about their lives freely and with confidence. CONTEST deals with all forms of terrorism and continues to be based around four strands: <u>Pursue</u>: the investigation and disruption of terrorist attacks; <u>Prevent</u>: work to stop people becoming terrorists or supporting terrorism; <u>Protect</u>: improving our protective security to stop a terrorist attack and <u>Prepare</u>: working to minimise the impact of an attack and to recover as quickly as possible.</i> • <i>The awareness and the education to stakeholders of the immense value of having a CT Strategy should be emphasized.</i>
<p>REGULATORY</p>	<ul style="list-style-type: none"> • <i>Research indicates that the following is required; continued appropriate regulations, legislation, policy and procedures including; cooperation on counter terrorism, preventing and suppressing the financing of terrorism, countering the use of the internet for terrorist purposes and countering violent extremism.</i>

11. Current Policies

11.1. Government and Institutions

- On the 5th December 2016 EU Ministers, agreed that all EU citizens and third country nationals entering or leaving the EU will now be systematically checked against databases, e.g. of lost and stolen documents. It is assessed this is critical in securing the EU's external borders, which means building up a stronger shield against terrorism in Europe and preserving the right to life. Systematic checks against databases are a further mandatory step towards the minimum protection of the citizens.
- Stopping people committing appalling acts of terrorism in the UK is something we should all want. Safeguarding our young people from becoming radicalised, either by the extreme right wing or Islamist extremists should not be a controversial aim. However there are some who actively seek to undermine the Prevent programme (Contest Strategy), without offering any meaningful alternatives. Concerns about spying on communities, such as asking teachers and others to be alert to signs of radicalisation and refer those who may need help may work in a similar way to safeguarding processes designed to protect people.
- The UK Government seeks to make the UK, a hostile environment for terrorist financing by disrupting terrorist fundraising and the movement of terrorist funds into and out of the UK. Collaboration with the private sector on terrorist finance will also improve through, Joint Money Laundering Intelligence Taskforce initiatives. An Action Plan will deliver significant changes to the UK anti-money laundering and counter-terrorist finance regimes and puts the public-private partnership at the heart of the response.
- The fight against online extremism was a key theme for the EU in 2017. The IT industry (Private Sector), has decided to create a shared database to help identify potential terrorist content on social media and prevent its reappearance on other platforms.
- Another example is the USA's Homeland Security - its main aims are the following;
 - Strengthening the Homeland Security Enterprise
 - Enforcing and Administering our Immigration Laws
 - Securing a Safeguarding and Securing Cyberspace
 - International Engagement
 - Management of Borders
 - Strengthening Resilience to Disasters
- The different aims of the USA Homeland Security are similar to the added value proclaimed by the EU in its Counter-Terrorism Strategy. It states that the EU adds value by:
 - Strengthening national capabilities

- Facilitating European cooperation
- Developing collective capability
- Promoting international partnership

All these actions are contributing to the four main pillars of the strategy: preventing, protecting, pursuing and responding. (A1)

Industry

- The security industry offers a broad range of services from specialised guarding, technology solutions, mobile services, monitoring, consulting and investigations. Typically these Security companies work around the world. For example, the security company, 'Securitas', operates in North America, Europe, Latin America, Middle East, Asia and Africa. From data collected, companies in the security industry tend to offer programmes and services that are customised to their clients' needs and reflect the current threat environment. Also reputable companies in the security industry consider future terrorist attack scenarios. Training and Consultancy services being provided was a common theme, striving to ensure that common sense prevails and that realistic solutions aim to reflect national and international standards, whilst developing individual and corporate mindsets. The training and consultancy services provided are to educate, advise and inform individuals, organisations and governments of the threat of international terrorism, criminal activity and the actions of desperate individuals who aim to disrupt the lives of citizens.
- Aviation security is another important issue to thwart terrorist attacks. To illustrate, the company, 'Green Light Ltd', a UK security training and consultancy company has, as one of its flagship programmes a, 'Hijack Exercise'. The company was founded by a veteran of the aviation security industry and outspoken advocate of the need to deploy a common sense approach to resolve modern-day security dilemmas. Companies like these advise governments and industry, especially in respect of passenger risk analysis and in-flight security solutions. Typical examples of organisations that can use these services are the following;
 - Airlines
 - Airports
 - Immigration & Customs Authorities
 - Sea Ports
 - Police Forces
 - Contract Security Companies
 - Security Technology Manufacturers
 - Business Executives
 - Shipping Companies
 - Cargo Agencies & Freight Forwarders
 - Civil Aviation Authorities
 - Rail Networks
 - Hotel Chains
 - Tourist Sites

- Sports & Entertainment Venues
- Media Outlets
- Companies in the security industry, have versatile and highly qualified advisors and consultants that can be utilised in a positive way. They have expertise in their given specialism in areas such as transportation, safety and security. Their years of operational experience enables them to advise and support their clients, allowing them to evaluate and manage contemporary security challenges and to identify the solutions necessary to establish a secure environment.
- Security companies such as G4S offer a range of services that can support law enforcement and government in the UK and overseas. These include the supply of security personnel, monitoring equipment, response units and secure prisoner transportation. Private security also provides mass employment, with G4S, the world's largest security company measured by revenues and its operations in around 125 countries, with 585,000 employees and being the world's third-largest private employer. (A2)

11.2. Law Enforcement

- The UK's, National Counter Terrorism Policing, has released to the public an information film, providing advice on the steps to take to keep safe in the event of a firearms or weapons attack.
- MI5 (Security Service) the UK's, 'Intelligence Service', state that Terrorist groups use violence and threats of violence to publicise their causes and as a means to achieve their goals. They often aim to influence or exert pressure on governments and government policies but reject democratic processes, or even democracy itself.
- INTERPOL enables police in 190 countries to work together to fight international crime. They provide a range of policing expertise and capabilities, supporting three main crime programmes: Counter-terrorism, Cybercrime, and Organised and emerging crime.
- Europol assists 28 EU Member States in their fight against serious international crime and terrorism. They also work with many non-EU partner states and international organisations. Large-scale terrorist networks pose a significant threat to the internal security of the EU. Terrorism, cybercrime and people smuggling, to name just a few, pose a severe threat to the safety and livelihood of its people. The biggest security threats come from:
 - terrorism
 - international drug trafficking and money laundering
 - organised fraud
 - the counterfeiting of euros
 - people smuggling
- NCA has been designed to maximise the impact of the UK's collective resources against serious and organised crime. The NCA responds to a broad range of threats,

many of which also remain a responsibility for police forces and other agencies. Where crime is particularly complex or impractical for a single force or agency to tackle, the NCA will channel its influence and specialist capabilities to ensure that it is within our reach. The NCA's partnerships go beyond law enforcement. We work with private industry, local and national government and other public sector organisations, the charity and voluntary sectors, think tanks and academia amongst others. Sharing skills, information, expertise and technology enables us to deliver the best response to opportunities and threats. (A1)

11.3. THOR Summary - Current Policies

Current Polices	
TECHNICAL	<ul style="list-style-type: none"> • <i>The fight against online extremism is a key theme for the EU in 2017. The IT industry has decided to create a shared database to help identify potential terrorist content on social media and prevent its reappearance on other platforms.</i> • <i>Safeguarding and Securing Cyberspace is an ongoing objective.</i>
HUMAN	<ul style="list-style-type: none"> • <i>Governments are striving to make their countries a hostile environment for terrorist financing by disrupting terrorist fundraising and the movement of terrorist funds, in and out of their countries. Collaboration and information sharing between nations is crucial.</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>Collaboration, cooperation and a multi-disciplinary approach remains at the core to the success of counter terrorism strategies, legislation and policies. A key ingredient in this is the involvement and consultation with the public.</i> • <i>Safeguarding young people from becoming radicalised, either by the extreme right wing or Islamist extremists is a concern.</i> • <i>The Aviation security industry should continue to be consulted to thwart terrorist attacks on Aircraft.</i> • <i>The security industry offers a broad range of services from specialised guarding, technology solutions, mobile services, monitoring, consulting and investigations. This industry can support LEA's in their fight against terrorism.</i>
REGULATORY	<ul style="list-style-type: none"> • <i>Regulations and Legislation in place to combat terrorism. However these regulations and legislation require to be reviewed regularly.</i> • <i>Stakeholders should be aware of relevant terrorist regulations and legislation.</i>

12. Current Practice

12.1. National

- Counter-terror officers have stepped up their planning for a marauding-style terror attack in the UK, following the atrocities in Europe.

- The UK's Metropolitan Police Service (MPS), held a mock terrorism training exercise on the River Thames, London.
- PM Theresa May announced a counter-terrorism training exercise in Scotland to strengthen the UK's response to a terrorist attack.
- UK Police Test Terrorism Attack Response in London (CT Exercise).

12.2. *European Union*

- The European Union (EU), Council is currently working on a European Commission proposal to amend the fourth anti-money laundering directive. The proposed amendments, among other issues:
 - address the possible threats linked to the use of new technologies in financial transactions,
 - strengthen and harmonise checks on financial flows from high-risk third countries,
 - increase transparency,
 - confer more powers on national financial intelligence units.
- The threat posed by Europeans being radicalised, many of who have also travelled abroad to fight, is likely to persist in the coming years. An effective response to these issues requires a comprehensive approach and long term commitment.
- Dutch counter terrorism exercise in Rotterdam.
- Members of the National Guard are taking part in an international counter terrorism-exercise, in Sweden, that aims to combat attacks using improvised explosive devices (IED).
- The OSCE region gathered for their annual OSCE-wide Counter-Terrorism Conference (26/05/17). Participants discussed national experiences and international co-operation in countering terrorism, good practices from the OSCE region on rehabilitation and reintegration strategies, as well as prevention of radicalisation to terrorism.
- Terrorism constitutes one of the most serious threats to OSCE participating States and it is likely to remain a shared security challenge in the foreseeable future. Concerted international cooperation is crucial for effective policy implementation and cooperation among participating States is seen as a vital element of countering terrorism within the framework of the OSCE.
- The EU plans for a new European Counter-Terrorism Unit that will tackle extremists online in a joint effort of law enforcement from various states. Terrorists are exploiting the web for propaganda purpose and to menace the Western infidels for this reason intelligence agencies and law enforcement need to increase their efforts to tackle any kind of extremist content online.
- The fight against terrorism must, as with other types of crime, include the collaboration of civilians. Therefore, many police forces have been promoting official channels to provide information to them anonymously. For example, in Spain, both the national police (Policia Nacional) and the Catalan Police (Mossos d'Esquadra), are active in the social media promoting a phone number and an email, which is created for terrorism attacks/radicalization prevention.

12.3. *International*

- USA - Secret Service held a counter terrorism exercise in Washington DC (26/04/17).
- Yemen - The USA and Yemeni held joint counter terrorism exercise.
- Singapore has staged its biggest island wide counter-terrorism exercise - Heavily armed military from the Police and Singapore Armed Forces (SAF) turned out in force, to seek out and neutralise a mock terror threat in the country's largest counter-terrorism exercise (17/10/16).
- Philippines Air Force, Navy and Marines take part in a joint counter Anti - Hijacking Aircraft exercise. (26/10/16)
- Nigeria - Lagos Airport - Nigerian Air Force carries out Counter-Terrorism Exercise (8/11/16).
- Plan to enhance interoperability and exchange skills. The armies of India and Oman are scheduled to conduct their second bilateral exercise in March 2017 with a focus on counter-terrorism.
- USA - New York. Governor announces over 600 Joint Counter Terrorism Exercises across New York.
- UK - British Transport Police - Counter Terrorism. 'The threat from terrorism to the UK is serious. Our job is to keep everyone who travels and works on the rail network safe'. (A1)

12.4. *THOR Summary - Current Practice*

Current Practice	
TECHNICAL	<ul style="list-style-type: none"> • <i>The EU is addressing the possible threats linked to the use of new technologies in financial transactions.</i>
HUMAN	<ul style="list-style-type: none"> • <i>The threat posed by Europeans being <u>radicalised</u>, many of who, have also travelled abroad to fight, is likely to persist in the coming years.</i> • <i>LEA's carrying out 'CT' exercises.</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>OSCE - Terrorism constitutes one of the most serious threats to OSCE participating States and it is likely to remain a shared security challenge in the foreseeable future. Concerted international cooperation is crucial for effective policy implementation and cooperation among participating States is seen as a vital element of countering terrorism.</i> • <i>Information sharing, communication and co-operation crucial.</i>
REGULATORY	<ul style="list-style-type: none"> • <i>EU - Finance. Confer more powers on 'National Financial Intelligence Units'.</i> • <i>EU - Anti Money Laundering Legislation being reviewed.</i>

13. Legal Factors

13.1. National

- *Investigatory Powers Act (IPA) 2016*. This Act makes provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security.
- *Regulation of Investigatory Powers Act (RIPA) 2000*. This Act makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters.
- *Codes of practice* and guidance for making an application under the Regulation of Investigatory Powers Act (RIPA) 2000.
- *Justice and Security Act 2013*. An Act which provides oversight of the Security Service, the Secret Intelligence Service, the Government Communications Headquarters and other activities relating to intelligence or security matters.
- *Criminal Procedure and Investigation Act 1996*. This Act makes provision about criminal procedure and criminal investigations.
- *Serious Crime Act 2017*. An Act to make provision about serious crime prevention orders and to create offences in respect of encouragement or assistance of crime etc.
- The Terrorism Act 2015. The annual report (01/12/16) by the Independent Reviewer of Terrorism Legislation on the operation of the Terrorism Acts in 2015.
- Police and Criminal Evidence Act 1984 (PACE) Codes of Practice.
- Extradition', of Abu Hamza and four others extradited for terrorism offences. European Court of Human Rights judges ruled the UK Government could lawfully extradite radical preacher Abu Hamza to the USA to face terrorist charges.
- Agreement to strengthen the unity on the defense of the liberties and on the fight against terrorism (2015) was signed by the two main political parties in Spain. This is also known as the "The pact against jihadism". They commit themselves to reform the Spanish Criminal Law to redefine the concept of terrorism and the respective sentences.

13.2. European

France - French legislators have voted to extend the country's state of emergency, despite growing concerns that the anti-terror measures violate civil liberties. The extension comes as lawmakers continue to debate proposals that would expand government surveillance and make it easier for the president to activate a state of emergency in the future.

OSCE (March 2017). Practical implementation of the international legal framework against terrorism means that states have to make every effort to prevent terrorist attacks, legislation, regulations and investigation techniques have to reflect a proactive approach anticipating terrorist methods and tactics, criminalising and investigating preparatory acts, such as producing or acquiring fake documents as well as terrorist financing.

13.3. International

- EU Minister argues that changing Turkey's anti-terrorism laws is out of the question as it would endanger both Turkey and Europe's security.
- UN Office of Counter Terrorism. International Legal Instruments;
- Since 1963, the international community has elaborated 19 international legal instruments to prevent terrorist acts.
- Cyberspace, Terrorism and International Law ; Governments have long worried about terrorists using the Internet to launch cyberattacks, spread propaganda, recruit and radicalise individuals and raise funds. However, the Islamic State's exploitation of social media has caused a crisis and generated questions about international law's role in addressing terrorism in cyberspace.
- Defining Terrorism in International Law; Despite numerous efforts since the 1920s, the international community has failed to define or criminalise 'terrorism' in international law. Terrorism should be defined and criminalised because it seriously undermines fundamental human rights, jeopardises the state, peaceful politics and may threaten international peace and security.
- USA - Human Rights Watch, object to warrantless surveillance designed to monitor Americans and others. While Section 702 FISA Amendments Act of 2008 states that the NSA's surveillance under the law must "target" foreigners abroad, in reality the law allows the agency to capture potentially vast numbers of Americans' communications with people overseas (as well as Americans' domestic Internet communications that just happen to be routed through another country en route to the recipient). This surveillance is warrantless and no judge ever reviews or approves the government's individual targeting decisions. The law does not require the government to show it has any suspicion that anyone who may be caught up in this dragnet has engaged in wrongdoing.
- INTERPOL - Terrorism poses a grave threat to national security and the lives of individuals around the world. INTERPOL has a number of initiatives to support our member countries in their efforts to protect their citizens from terrorism in its many forms. Experts at the General Secretariat collect, store and analyse information about suspected individuals and groups and their activities and exchange data with our member countries and other international organisations. A chief initiative in this area is the Counter-Terrorism Fusion Centre, which works to disrupt the recruitment and activities of foreign terrorists. (A1)

13.4. THOR Summary - Legal Factors

Legal Factors	
TECHNICAL	<ul style="list-style-type: none"> • <i>Exploitation of social media for terrorist purposes. Concerns regarding terrorist cyber-attacks.</i> • <i>Questions about International Law's role in addressing terrorism in cyberspace.</i>
HUMAN	<ul style="list-style-type: none"> • <i>Human Rights, Legislation, Policy, Civil Liberties and Privacy Issues to be considered.</i>
ORGANISATIONAL	<ul style="list-style-type: none"> • <i>France - Concerns that the anti-terror measures violate civil liberties.</i> • <i>USA - Warrantless surveillance issues around communications.</i> • <i>INTERPOL - Terrorism poses a grave threat to national security and the lives of individuals around the world. It has a number of initiatives to support its member countries in their efforts to protect their citizens from terrorism.</i>
REGULATORY	<ul style="list-style-type: none"> • <i>Despite numerous efforts since the 1920s, the international community has failed to define or criminalise 'terrorism' in international law.</i>

Overall Summary

As per [Appendix 1](#) (Thor Factors), this section provides an overall summary from desk based research to date, considering four key areas: Technology, Human, Organisational and Regulatory. This simplification was beneficial for illustrating themes, which can be identified in the approach to this Counter Terrorism module, from a range of perspectives, objectives and provides an overview.

To re-emphasise the information was gathered from a variety of sources, ranging from stakeholder perspectives, to assessments for the future and while complexities do exist in each area, common and consistent themes of relevance can be seen to emerge. See 'THOR' - Overall Summary.

14. THOR - Overall Summary

TECHNICAL	<ul style="list-style-type: none"> • <i>From a technical perspective the <u>Internet</u>, as a <u>strategic device</u> for terrorists was cited as a serious concern, in particular;</i> • <i>Use of the Darknet and Cyberterrorism,</i> • <i>As a device to identify, recruit and train new members.</i> • <i>Collect and transfer funds.</i> • <i>Global Data Bases were noted to be important to track trends and methodologies of terrorism.</i>
HUMAN	<ul style="list-style-type: none"> • <i>Terrorist Ideologies, Aims, Beliefs and Motivations</i> • <i>Radicalization and countering violent extremism,</i> • <i>Human Rights,</i> • <i>Civil Liberties and Privacy issues,</i>

ORGANISATIONAL	<ul style="list-style-type: none"> • <i>National Security, Intelligence gathering and co-operation.</i> • <i>INTERPOL, Terrorism poses a grave threat to national security.</i> • <i>OSCE - Terrorism constitutes one of the most serious threats.</i> • <i>UN - The UN Global CT Strategy, Terrorists' use of the internet and social media has increased significantly in the recent years.</i> • <i>The Private Security Industry can provide valuable support to Governments to thwart the threat of terrorism.</i> • <i>Organisations also have serious concerns on radicalisation and <u>countering violent extremism</u>.</i> • <i>Ongoing education, training collaboration and communication between government, LEA's and the business community is required regarding, terrorism, terrorism finance, countering violent extremism and being aware of CT strategy.</i> • <i>Information sharing, communication and co-operation are crucial.</i> • <i>The awareness and the education to stakeholders of the immense value of having a CT Strategy should be emphasised.</i> • <i>State Terrorism: we should consider that terrorism is not just a "non-state actor concept" but a more comprehensive one that should include the state as well.</i>
REGULATORY	<ul style="list-style-type: none"> • <i>Regulatory and legal implications around areas such as, Terrorism, Human Rights, Surveillance, Data protection, Finance and Privacy need to be considered.</i> • <i>Despite numerous efforts since the 1920s, the international community has failed to define or criminalise 'terrorism' in international law.</i> • <i>Border security is vital asset to nations in thwarting the terrorist threat.</i>

To conclude, information will continue to be gathered from various credible sources, from current courses, stakeholder perspectives, current practice, current policies and legal factors. From our initial, 'THOR' overall summary, the general themes identified for the Counter Terrorism module include;

- **T** - Territory / Border Security.
- **E** - Engagement / Information Sharing.
- **R** - Radicalisation.
- **R** - Regulations / Legislation / Human Rights.
- **O** - Online / Internet.
- **R** - Recording of information / Databases.
- **I** - Interoperability / Communication.
- **S** - Strategies - Counter Terrorism.
- **M** - Monetary/Finance.