TIMELEX

CYBERSEC4EUROPE

Overview of existing Cybersecurity Public authorities and entities, Public-Private Partnerships and Private initiatives in the European Member States

TABLE OF CONTENTS

INTRODUCTION

On 12 September 2018, the European Commission presented a proposal for a Regulation which will establish a European Cybersecurity Industrial, Technology and Research Competence Centre, a Network of National Coordination Centres and a Cybersecurity Competence Community (the "Regulation"). The proposal already went through the European Parliament for amendments and is now at the stage of the trilogue negotiations.

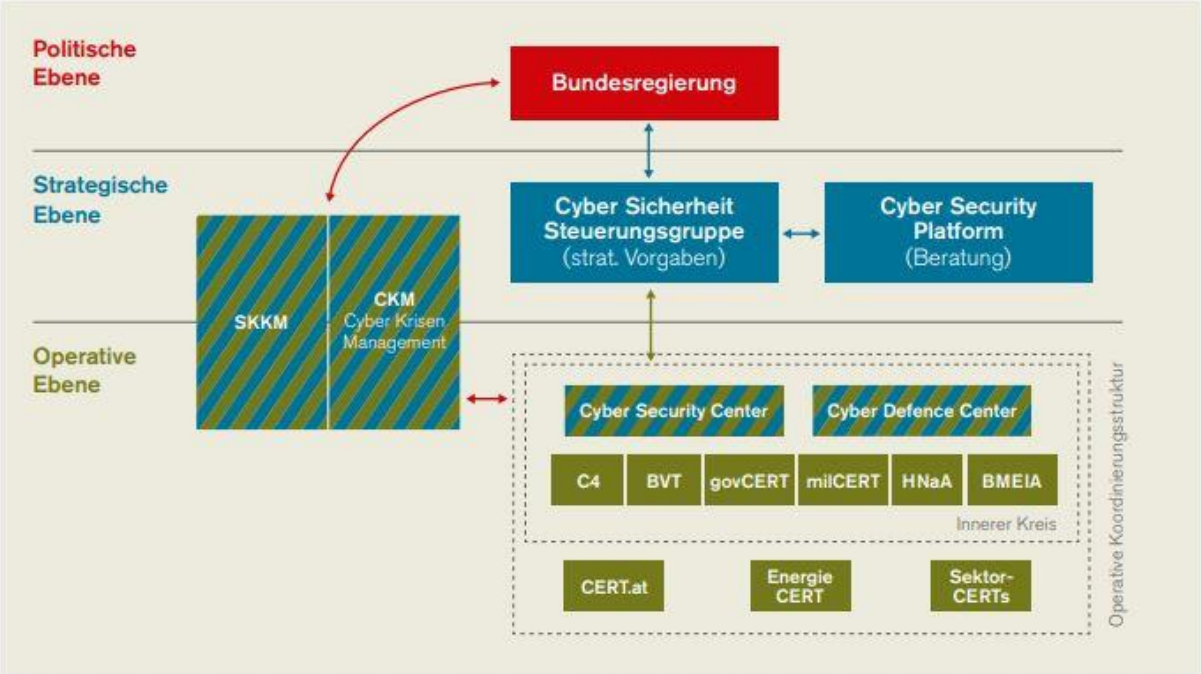
The proposal creates a European entity, the Cybersecurity Competence Centre (1), and two groups composed of national entities, the Network of National Coordination Centres (2) and the Cybersecurity Competence Community (3). The Regulation is mainly focussed on the establishment and governance structure of the **Competence Centre (1)** and the connections to and role of the National Coordination Centres and the Competence Community in the Competence Centre.

In order to develop a sustainable European Cybersecurity Competence Network, four Horizon 2020 pilot projects – ECHO, CONCORDIA, SPARTA and CyberSecurity4Europe – are tasked with establishing and operating a pilot for the European Cybersecurity Competence Network. Timelex is involved as a partner in the CyberSec4EU consortium, where one of the important tasks is defining and establishing a governance model for the European Cybersecurity Competence Network of cybersecurity centres of excellence, in line with the Regulation. It is in the framework of CyberSec4EU's objective and the Regulation that this contribution provides an overview of cybersecurity entities, structures and initiatives in the Member States, as a key factor in the governance and structure of the Network will be the designation of the entities under the Regulation.

According to the Regulation, the **National Coordination Centres (2)** are nominated by the Member States, based on administrative capacity and access to technological expertise regarding cybersecurity. The Commission will accredit or reject the nomination by the Member States. It is to be expected that the Member States will nominate public entities as the National Coordination Centres, since these will play an important role in the allocation of European funding. This contribution provides an overview of the national public bodies which exist and might be nominated by the Member States as National Coordination Centres. As the overview shows the answer is not always clear cut, since not every Member State has a Cybersecurity entity and as some Member States have a multiple of public entities which are involved in and have responsibilities in Cybersecurity.

The members of the **Cybersecurity Competence Community (3)** will be comprised of the main stakeholders, being civil society, industry from the demand and supply-side, the academic and research community, associations of users and other associations as well as public entities and other entities dealing with operational and technical matters in the area of cybersecurity. Applicants for membership will be assessed based on conditions relating to their cybersecurity expertise. Once successfully passed the assessment, these applicants will be accredited by the Competence Centre. In order to give a primary view on entities which might be appointed as Community members, this overview looks at Public-Private Partnerships and industry led initiatives in the Member States.

1. AUSTRIA



Source: *Republik Östenrich, Bericht "Cyber Sicherheit in Östenrich", 2018.*

Public Entities	
Name	**Cyber Security Steering group**
Legal form and members	This group is made up of the National Security Council and Cyber security Experts of the ministries represented in the national security council.
Governance	Under the auspices of the Federal Chancellery.
Funding	
Tasks	Strategical level. The group advises the government on cybersecurity, oversees the implementation of the Austrian cyber security strategy and drafts the annual cyber security report of Austria.
Name	**CSC – Cyber Security Centre**
Legal form and members	Involves the ministries and the operational structures of the business and research sectors. Supported at operational level by the Federal Ministry of Defence and Sports.
Governance	Under the Federal Ministry of Interior affairs, Part of the operational coordination structures (OpKoord). Undertaking ensured by the GovCERT and the CERT.at (these CERT's are the same entity and are operated by a private company. However, the head of the GovCERT is the Director of one of the departments in the Federal Chancellery.)
Funding	Funded by the Federal Chancellery
Tasks	Operational level. Tasks: • NIS-entity • Prevention of incidents on and protection of critical infrastructures

	• Coordination and management of cyber crisis • Technical competence and contact point • Collecting information and passing it on
Name	**ATC – Austrian Trust Circle**
Legal form and members	
Governance	Initiative of CERT.at and the Austrian Federal Chancellery.
Funding	
Tasks	Exchanges information on security in the individual areas of the strategic information infrastructure and creates a framework for joint projects in the security sector.
Name	**CERT.AT**
Legal form and members	
Governance	Operated by a private company, performing a task of general interest.
Funding	Funded by nic.at, the Austrian Domain registry
Tasks	• primary contact point for IT-security in a national context • coordinate other CERTs operating in the area of critical infrastructure or communication infrastructure • provides basic IT-security information (warnings, alerts, advise) for SMEs • coordinate the response in case of a cyber attack
Public-Private partnerships	
Name	**CSP – Austrian Cyber Security Platform**
Legal form and members	Stakeholders from business, academic and administrative background.

Governance	Was created by the KSÖ, the Kuratorium Sicheres Österreich, a self-contained organization with close relationships to the Ministry of Interior.
	
	Bodies:
	• Plenary meeting: representatives of all stakeholders
	• Working groups: operational arm, can be topic-related, industry-related and organization-related
	  ○ Working group on standardization
	  ○ Working group on the Austrian Cyber Security Strategy
	Secretariat: carried out by the Federal Chancellery
	
	Decision making power lies with the public sector.
	
	The CSP communicates with the government through CSS, the cyber security steering group.

Funding	Membership fees

Tasks	Focusses on information exchange and cooperation, but also provides advice and input in the Austrian legislation.
Name	**KSÖ, the Kuratorium Sicheres Österreich**
Legal form and members	Non-profit, independent association

Governance	Bodies:
	• General assembly
	  ○ Voting: votes by simple majority.
	• Management Board: elected by the general assembly for a 3-year term from amongst the members. The members of the Federal Ministry of Interior who act as contractors or sponsors to the KSÖ cannot be elected. The members of the management board do their work voluntarily.
	  ○ Voting: votes by simple majority, but at least 6 members have to be present
	• Presidium: day to day management
	• State clubs: state sections of the KSÖ
	• Auditors
	• Arbitration body

Funding	Membership fees and funding by the Federal Ministry of interior.
Tasks	Interface between business, research, public authorities and society and, as a competence network, helps to bring together the relevant actors in order to work together towards this goal. Detailed list of tasks of the bodies can be found in the statutes.
Name	**A-SIT**
Legal form and members	Made up of public institutions: • Federal ministry for Digital and Economic Affairs • Central bank of the Republic of Austria • Graz university of Technology • Federal Computing Centre • Danube University Krems

Governance	Bodies:
	• General assembly
	  ○ Voting: 1/3th of the ordinary members (with voting rights) have to be present, votes with simple majority
	• Board of Directors: general leader and secretary general (+ extra members appointed by the General Assembly). Governing board.
	  ○ Voting: when made up of two members both have to be present and take decisions unanimously, when more than 2 members decisions are taken with 2/3 presence and simple majority that represents half of the board

	• Presidium: decides on membership and appoints provisional members of the board • Auditors • Arbitration body
Funding	Membership fees, grants, subsidies and income from the provision of services to public and private organizations.
Tasks	Competence centre for IT-security. • Evaluation: conformity and accreditation • Research- and technology observation • Financial supervision • Institutional support • Awareness
Private Initiatives	
Name	**SBA Research**
Legal form and members	Made up of companies, Austrian and international universities and research institutions
Governance	The center is part of the Austrian COMET excellence program (COMET – Competence Centers for Excellent Technologies). Bodies: • Management • Scientific board: advisory and internal review board.
Funding	
Tasks	Research Center for Information Security
Name	**Cyber Security Austria**
Legal form and members	non-profit, independent and non-partisan association

Governance	Bodies:
	• General assembly:
	  ○ Voting: ½ of the members with voting rights have to be present, simple majority
	• Executive committee:
	  ○ CSA Board : Extended board
	  ○ votes by simple majority when all its members have been invited and at least half of them are present
	• "wisenrat": Experts assisting the Executive Board or the CSA Board in finding and implementing the strategy, establishing and directing working groups on each of the thematic areas defined by the CSA Board, and preparing the results of the working groups for further use by the CSA Board.
	• Auditors
	• Arbitration body

Funding	Membership fees and donations

Tasks	Awareness and knowledge sharing.

2. BELGIUM

Public Entities	
Name	**CCB – Centre For Cybersecurity Belgium**
Legal form and members	Operational service under the Prime Minister.
Governance	The CCB was established by a Royal Decree and resorts under the authority of the Prime Minister. The Prime Ministers' office offers logistic and administrative support. Bodies: • Director • Adjunct Director The director and the adjunct director are appointed by the king in a royal Decree, after consultation in the council of ministers and after consultation of the National Security Council. They are appointed for 5 years and operate under the direct authority of the Minister.
Funding	
Tasks	• The core task of the CCB is monitoring, coordinating and supervising the implementation of the Belgian Cybersecurity Policy. • manage cybersecurity projects • coordinate all different actors involved • draft proposals for legislation in the area of cyber security • the CCB participates in crisis management • plays a role in standardization and guidance and the implementation thereof, as well as the evaluation and certification of the security of information- and communication systems. • create awareness and disseminate information to the public about cyber security. • operates the Computer Emergency Response Team (CERT)
Name	**CERT.be**
Legal form and members	
Governance	Operates under CCB, headed by a separate Director.
Funding	
Tasks	Operational part of the CCB. • assisting private and public sector organizations in the event of a cyber incident • coordinating the handling of large-scale incidents

	• information sharing through events and publications free of charge • contact point for incident reporting
Public-Private partnerships	
Name	**CSC – Cyber Security Coalition**
Legal form and members	Non-profit organization, a partnership between academic actors, public authorities (such as the CCB) and the private sector.
Governance	• Annual general meeting: representation of all members • Board of Directors: appointed by the members, at least one director from the public, private and academic sectors, appoints a chairman for a term of 4 years. Task: Coalition's governance. • Focus groups: domain experts from the members. Meet on a regular basis to share their experience, best practices and participate jointly in several projects.
Funding	Membership fees
Tasks	• Expertise and skills sharing • Information exchange • Implementation of joint actions • Operational collaboration • Policies recommendations • Raising awareness
Private initiatives	
Name	**Brussels Initiative on Cybersecurity innovation**
Legal form and members	Gathers university and research centers
Governance	Set up by Sirris, a non-profit organization that gathers the technological industry and supported by public (CCB) and private organizations.
Funding	
Tasks	Focusses on collaboration between cybersecurity researchers.

3. BULGARIA

Public Entities	
Name	**Cyber Security Council**
Legal form and members	Includes representatives of the Ministry of Transport, Information Technology and Communications, Ministry of Justice, Ministry of Finance, Ministry of Economy, Ministry of Energy, as well as representatives of business, academia and non-governmental organisations. Includes the National Cyber Security Coordinator.
Governance	Chaired by the Minister of Interior and Minister of Defense.
Funding	
Tasks	• development of the National Cyber Security Strategy and National Network and Information Security Strategy

	• manage and organize the national cyber security system
Name	**National Security State Agency**
Legal form and members	
Governance	
Funding	
Tasks	• protect strategic communication and information systems from potential cyber security incidents • create a Monitoring and Incident Reaction Centre
Name	**Electronic Governance State Agency**
Legal form and members	
Governance	
Funding	
Tasks	• monitor, coordinate and facilitate the compliance of all administrative bodies to network and information security requirements • maintain a NIS register • National Single Point of Contact • Establish a national CSIRT (now only CERT Bulgaria is existing, the governmental CERT)

4. CROATIA

Public Entities	
Name	**National Cyber Security Council**
Legal form and members	Interdepartmental panel composed of the authorized representatives of the competent public bodies with national and sectoral policy and coordination responsibilities.
Governance	Drafts its own Rules of Procedure. Reports back annually to the government on its own work and the work of the Coordination Group
Funding	
Tasks	Tasks: • Monitor and implement the Cyber Security strategy • Propose measures to improve the implementation of the strategy • Propose the organization of national exercises • Issue recommendations, opinions, reports and guidelines • propose amendments to the Strategy and Action plan or propose the adoption of a new Strategy and action plans, in accordance with the new requirements. • Addressing issues essential for cyber crisis management and proposing measures for higher efficiency

	• Analyzing the reports on the state of cyber security submitted by the Operational and Technical Coordination Group • Making periodic assessments of the state of cyber security • Defining cyber crisis action plans • Making programmes and action plans for the Operational and Technical Coordination Group and directing its work • Cyber crisis management
Name	**Operational and technical cyber security coordination group**
Legal form and members	Interdepartmental panel composed of the authorized representatives of the competent bodies with operational and technical responsibilities.
Governance	Performs its tasks according to the programs, activity plans and guidelines provided by the National Council. Reports back annually to the National Cyber Security Council.
Funding	
Tasks	• Monitor the state of security to detect threats • Reports on the state of cyber security • Propose cyber crisis action plans
Name	**HAKOM - Regulatory Authority for network Industries**
Legal form and members	An independent autonomous and non-profit legal entity with public authority.
Governance	Bodies: • Council: five members, including a Chairman and a Deputy Chairman, appointed for a period of 5 years by the Parliament upon proposal of the Government of the Republic of Croatia. ○ Voting: simple majority • Administrative service: expert, administrative and technical tasks Executive Director: manages the Administrative service, appointed by and accountable to the Council. Has representatives in the National Cyber Security Council and the Coordination group. Council
Funding	Revenues collected through address and number allocation management, radio frequency (RF) spectrum management and revenues collected by electronic communications operators, postal service providers and railway infrastructure managers in accordance with publicly available annual financial plan.
Tasks	Regulates electronic communications. Consult with the private sector in order to support the communication industry.
Public-Private partnerships	
Name	**CARNet - Croatian Academic and Research Network**

Legal form and members	Brings together the public entities and the academic, scientific and research community.
Governance	Operates within the Ministry of Science and Education Bodies: • Managing Council: represents the Croatian Government, members are appointed by the Minister of Science and Education • Executive Committee: short- and long-term planning, and makes decisions on business organization and is responsible for the relations with the government bodies, users, partners and the public • the CEO: coordinates activities at the level of the entire institution and outside it and represents CARNET in public • Council of Users: all CARNET coordinators of CARNET member institutions, which represent users from the academic community, heads of county expert councils of Computer Science teachers, as well as representatives of educational institutions and the CEO of CARNET. Departments: • General and Financial Activities Department • Network Infrastructure Department • Computing Infrastructure and Services Department • **National CERT Department** • User Support Department • Education Support Department • Office of the CEO
Funding	
Tasks	• Network of the academic, scientific and research community of the Republic of Croatia • Operates the national CERT
Name	**HKKOI - The Croatian Defense Industry Competitiveness Cluster:**
Legal form and members	Formal association of all stakeholders (particularly industry stakeholders) that in their activities and scope of operation support the defense and security system of the Republic of Croatia and the EU.
Governance	Bodies: • Assembly of Croatian Defense Industry Competitiveness Cluster: representatives of regular members. • Management Board of Croatian Defense Industry Competitiveness Cluster: 9 members elected by the Assembly for a 3year term, includes the president and the vice-president. Adopts and executes executive decisions that contribute to achieving the planned goals of the Association in line with the adopted Annual Activities' Action Plan and the Work Plan presented by President o Voting: simple majority

	• President of the Croatian Defense industry Competitiveness Cluster: elected by the Assembly for a two-year term and may be reappointed, leads the Cluster, the Assembly and the Management Board Regular members are approved by the Management Board. The statutes outline who the membership is open to.
Funding	
Tasks	Brings together the country's relevant companies and SMEs and research sector in cooperation with Croatia's Ministry of Defence to spin out commercial applications from military technologies.

5. CYPRUS

Public Entities	
Name	**OCECPR – Office Of The Commisioner Of Electronic Communications And Postal Regulation**
Legal form and members	Independent regulatory authority
Governance	The Commissioner reports to the President of Cyprus. Bodies: • Commissioner: head of the authority, appointed by the Council of Ministers for a period not exceeding 6 years. • Deputy Commissioner: assists the Commissioner, appointed by the Council of Ministers for a maximum period of 6 years. • Advisory Committee
Funding	
Tasks	• Responsible for electronic communications and postal services, with additional responsibilities in the areas of terminal equipment, network and information security and protection of critical information infrastructures • Coordinating and implementing the cybersecurity strategy • NIS • Coordinates CERTS and CSIRTS • Assists in the exchange of information between the competent authorities, stakeholders and consumers • Minimum standards for security • Working groups
Name	**CSIRT CY**
Legal form and members	
Governance	Operated by the OCECPR
Funding	

Tasks	National CSIRT.
Public-Private partnerships	
Name	**Cybercrime Centre of Excellence**
Legal form and members	Partnership between public and private entities.
Governance	Coordinated by the Cyprus Neuroscience & Technology Institute with the Office of the Commissioner of Electronic Communications and Postal Regulation, the European University Cyprus, Aditess and the Office for Combating Cybercrime as partners.
Funding	Co-funded by the Prevention and Fight against crime programme of the EU
Tasks	Provides short-term highly focused and specialized training seminars on cybercrime-related issues for public and private sector participants. Courses will be made available under creative commons licensing terms for LEAs worldwide.

6. CZECHIA

Public Entities	
Name	**NUKIB - National Cyber and Information Security Agency**
Legal form and members	
Governance	Operates under the National Security Agency, who has the overall responsibility for national cyber security.
Funding	Government funding
Tasks	Has the overall responsibility for cyber security. Resorts under the NSA. Comprised of the government CERT and the Cyber security policies department. • operate the Government CERT (GovCERT.CZ) • cooperation with other Czech CERT teams and CSIRTs • cooperation with international CERT teams and CSIRTs • drafting of security standards for different categories of entities in the Czech Republic • support of education in the field of cyber security • research and development in the area of cyber security
Name	**Cyber Security Council**
Legal form and members	Includes representatives from the Czech NSA, the Ministry of Interior, the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Finance, the Ministry of Industry and Trade, the Ministry of Transport, the Police, the Office for Foreign Relations and Information (the external civilian intelligence service), the Security Information Service (the internal civilian intelligence service), Military Intelligence, the Office for Personal Data Protection, and the Czech Telecommunications Office.

Governance	
Funding	
Tasks	Provides a forum for inter-agency coordination: cooperation in the fields of cyber security, cyber defence and cyber crime • coordination of activities of state bodies in the field of cybernetic security and contribution to fulfilling international obligations in this field • coordination between state bodies while fulfilling obligations in the field of cyber security stemming from membership of the Czech Republic in international organizations and coordination of participation of the Czech Republic in international organizations and other international activities associated with cyber security • providing for good cooperation between its members • discussion of current issues of cyber security and drafting expert proposals and recommendations to the Government • collection and analysis of information about cyber security provided by its members • drafting of report on the cyber security in the Czech Republic which shall be presented by the Prime Minister to the Government on a regular basis as a policy document outlining priorities and corresponding tasks in the field of cyber security • cooperation with external entities and using their information in order to provide for cyber security of the Czech Republic
Public-Private partnerships	
Name	**CSIRT.CZ**
Legal form and members	
Governance	Operated by CZ.NIC, a non-profit organization that does the domain name registry, on the basis of a public contract with the NSA. Governed by elected members and representatives of the government
Funding	Funding by member ship fees.

Tasks	• To maintain foreign relations with the global community of CERT/CSIRT teams as well as with organisations supporting the community.
	• To cooperate with various entities across the country: ISPs, content providers, banks, security organs, institutions in the academic sphere, public authorities and other institutions.
	• To provide security services such as:
	  ○ Addressing security incidents and coordination thereof
	  ○ Education and tutoring
	  ○ Proactive services in the area of security

7. DENMARK

Public Entities	
Name	**Centre For Cyber Security**
Legal form and members	
Governance	Operates under the Danish Defence Intelligence Services, however, the center is an independent authority. Three departments: • advisory and telecommunications • network security • legal and policy Branches: advice and standards, defense and accreditation, cyber policy, situation center, cyber analysis, defensive cyber operations
Funding	
Tasks	• Advise Danish public authorities and private companies that provide critical infrastructures on how to prevent, counter and protect against cyber attacks • Detect attacks • Issues guidelines and recommendations • Approving and supervising electronic information systems and installations that process classified information • Administrates GovCERT, the CERT for the governmental institutions and the providers of critical infrastructures
Private initiatives	
Name	**Council for Digital Security**
Legal form and members	Private sector and academic organizations

Governance	Bodies:
	• General Assembly
	  ○ Voting: simple majority
	• Board of Directors: day to day management. Equal representation of Public Sector, Consumers, Research, Professional users, IT-suppliers and Private business community.
	  ○ Voting: simple majority
	• Chairman and vice chairman
	• General Assembly Board of Directors votes with simple majority

Funding	Membership fees
Tasks	Security and privacy advocacy group
Name	**Dansk IT**
Structure	IT Professionals.

Governance	• General meeting: The general meeting elects the board of directors and the auditor, approves the accounts, determines the quota with the exceptions stipulated in the articles of association, adopts amendments to the articles of association, etc. • The Board of Directors: members elected at the General Meeting. Elections are held every 3 years. Leads the association's activities, hires the executive board, appoints and dismisses councils and committees and is overall responsible for the association's operations. Voting with minimum half of the members present and with a simple majority. • Executive committee: chairman and two vice chairman, elected by the Board of Directors. Day to day management. • Executive board: executive committee and a CEO • Councils: implement the association's membership-oriented activities within the subject council's subject area. Can set up working groups and event committees.
Funding	Membership fees
Tasks	Representative body for information technology professionals in Denmark, cyber security being one of the areas covered

8. ESTONIA

Public Entities	
Name	**Ministry of Economic Affairs and Communications**
Legal form and members	
Governance	
Funding	
Tasks	Overall cyber security policy coordination
Name	**Cyber Security Council**
Legal form and members	Inter-agency body that involves all ministries and government agencies Cooperates with NGO's, business organizations, governments and educational institutions
Governance	Operates at the Security Committee Of The Government. Chaired by the Secretary General of the Ministry of Economic Affairs and Communications.
Funding	
Tasks	• Support inter-agency cooperation • Cyber security policy • Overseeing the implementation of Cyber Security strategy objectives • Submitting annual progress reports ○ Based on overviews of the implementation made upon the request of the Council to the government agencies

Name	RIA – Estonian Information Systems Authority
Legal form and members	
Governance	Accountable to the Minister of Economic Affairs and Communications. Bodies: • Special Projects Department • Structural Funds Department • Information Security Department • Communication Department • Administration Branch • State Information System Branch • Cyber Security Branch • Led by the Director General, who is appointed and dismissed by the Minister on the proposal of the Secretary General. Manages RIA. • Bodies are led by the Deputy Director General, head of department or an official or employee designated by the Director General. More on governance in the statutes
Funding	State budget, appropriations arising from participation in international cooperation projects, and funds allocated by the European Union.
Tasks	• Development and administration of state information systems • Drafting policies and strategies on the state information systems • coordinating the implementation of security standards • organizing activities related to cyber security • handling security incidents either reported or occurring on Estonian networks • supervision over the application of security measures by providers of critical infrastructures • risk analysis and drafting security measures for critical infrastructures • can conduct extra-judicial proceedings • Operating CERT-EE • Raises the security awareness of users

9. FINLAND

Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters.

Public Entities	
Name	**Finnish Transport and Communications Agency (TRAFICOM)**
Legal form and members	

Governance	State agency
Funding	State funding (including taxes on businesses and citizens)
Tasks	Incident reporting. Operates the National Cyber Security Centre.
Name	**NCSC-FI – The national Cyber Security Centre Finland**
Legal form and members	
Governance	Operates under FICORA.
Funding	State funding
Tasks	• monitors the operational reliability and security of communications networks and services • raises awareness on cyber security • Cyber security situation picture: report on vulnerabilities, disturbances and their effects, threat prediction, collect information on incidents and disseminates it to all actors which will estimate the effect on their activity and send this back to the centre • Operates the national CERT
Public-Private partnerships	
Name	**National Emergency Supply Organisation**
Legal form and members	Consists of the National Emergency Supply Agency, the National Emergency Supply Council, and the individual NESO sectors and pools.
Governance	• The National Emergency Supply Agency is tasked with planning and measures related to developing and maintaining security of supply. The statutory duties of the agency include providing support for the pools' and sectors' operations. The National Emergency Supply Agency is led by a chief executive officer in accordance with guidelines issued by the NESA Board of Directors. • The National Emergency Supply Council is a body that assesses and reviews the general state of security of supply. • The general mandate for the NESO sectors is to steer, co-ordinate, and monitor preparedness in their respective fields and to determine the goals for the pools. • The business-driven NESO pools are responsible for operational preparedness in their fields. The pools are tasked with monitoring, analysing, planning, and preparing measures for the development of security of supply within their individual industries, as well as with determining which enterprises are critical to security of supply.
Funding	State funding
Tasks	Network of multiple public-private partnership initiatives whose objectives are related to the security of supply. Ensures the conditions necessary for the operations of organisations that are critical to security of supply.
Private initiatives	
Name	**The Finnish Information Security Cluster**

Legal form and members	Association of Finnish information and cyber security companies.
Governance	• board of directors: governs the organization, composed of vice members of the members • CEO: operational head • Executive secretaries • Working groups
Funding	Membership fees
Tasks	Increase cross-border activities, promote public-private-partnerships, conduct market surveys, enable national depth and width of high-level education and dialogue with national and international regulatory bodies.

10. FRANCE

Public Entities	
Name	**ANSSI – The National Cybersecurity Agency Of France**
Legal form and members	Created by Decree 2009-834 of 7 July 2009 as a governmental authority.

Governance	Resides under the General Secretary for Defence and National Security.
	• Executive office: General Director, Deputy General Director
	• Strategic committee: Committee made up of senior government officials (advance proposals for state strategy in cybersecurity)
	• 5 departments
	  ○ Administration/ general affairs
	  ○ Expertise
	  ○ Secure Information Systems
	  ○ Operations: implementation of the defence authority-based information systems
	  ○ External relations and coordination
	• Cyber Anticipation Unit: coordinates the anticipation work supporting the decision-making process

Funding	the ANSSI is funded by the General Secretariat for National Defence.

Tasks	Directed at government departments and public services, operators of vital importance, businesses and individuals.
	• Cybersecurity and network and information security
	• Reacting to the cyber threat: detection centre
	• Gather skills
	• Providing information and advice
	  ○ Assist government departments and operators of vital importance
	  ○ Citizens
	• Supporting product and services development
	• Promotion of French technologies, systems and know-how
	• Training

	• Accreditation and certification • Building trust • Steering research
Name	**CERT.FR**
Legal form and members	
Governance	Within the Operational Center for Information Systems Security (COSSI) of The National Agency for Security Information Systems (ANSSI).
Funding	
Tasks	National CERT • detect the vulnerabilities of the systems, especially through a technology watch • pilot the resolution of incidents, if necessary with the global network of CERTs • help to put in place means to guard against future incidents • organize the establishment of a network of trust
Name	**OCLCTIC – Central Office for Combating Crime Related to Information and Communication Technologies**
Legal form and members	Government agency
Governance	OCLCTIC is an office which is part of the judicial police.
Funding	State funding.
Tasks	Focusses on the prevention and mitigation of cybercrime, but also has a research department.
Public-Private partnerships	
Name	**France Cybersecurity Label**
Legal form and members	

Governance	Initiative of ANSSI.
	• A governance structure:
	  ○ defines the general governance of the Label and especially the evolution of award criteria. This structure also oversees the Label's communication, external relations and administration.
	  ○ Committee made up of representatives of all involved parties:
	  ▪ Officials: amongst others, representatives of ANSSI
	  ▪ Industrial: representatives from the "Alliance pour la Confiance Numérique" (ACN) and HEXATRUST
	  ▪ Users
	• An award structure:
	  ○ also known as the "Award Committee", which is informed by third-party advisers. This structure decides whether or not to award the Label to applicants.

	○ two representatives of the College of officials, two representatives of the College of users and two representatives of the College of industrial corporations. Every college has one vote. Decisions are made with 2 votes out of three.
Funding	
Tasks	Promotes French Cybersecurity solutions, raise awareness, provide certification and increase the use and security level of users. They do this through certification.
Private initiatives	
Name	**Hexatrust**: Alliance of stakeholders
Name	**ACN** – Digital Trust Alliance: industry and research groups
Name	**CICS** – Council of trust and security industry
Name	**FIEEC** – Federation of electric, electronic and communication industries

11. GERMANY

Public Entities	
Name	**BSI – Federal Office for Information Security**
Legal form and members	Public authority established by the "Act on the Federal Office for Information Security" of 14 August 2009.
Governance	The BSI is a federal authority, overseen by the Ministry of Interior.
Funding	State funding.
Tasks	The main task of the BSI is to promote the security of information technology. Focusses exclusively on the security in governmental authorities and providers of critical infrastructures.
Name	**Nationales Cyber-Abwehrzentrum - National Cyber Defence Centre**
Legal form and members	Members of this centre are different authorities such as The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr and authorities supervising critical infrastructure operators.
Governance	Reports to the BSI, reports to the Federal Ministry of the Interior.
Funding	
Tasks	Cooperation platform to analyze cybersecurity incidents and provide recommendations for action
Name	**CERT Bund**
Legal form and members	
Governance	Part of the BSI
Funding	State funding
Tasks	National CERT • creates and publishes recommendations for preventive measures

	• points out vulnerabilities in hardware and software products • proposes measures to address known vulnerabilities • supports public agencies efforts to respond to IT security incidents • recommends various mitigation measures • operates Germany's national IT Situation Centre
Public-Private partnerships	
Name	**Cyber-Sicherheitsrat - National Cyber Security Council**
Legal form and members	Representatives are the Federal Chancellery and one State Secretary from each of the ministries Foreign Office, Federal Ministry of the Interior, Federal Ministry of Defense, Federal Ministry for Economic Affairs and Energy, Federal Ministry of Justice and Consumer Protection, Federal Ministry of Finance and Federal Ministry of Education and Research. The economy is represented by the Federal Association of German Industry, the Digital Association BITKOM Federal Association for Information Technology, Telecommunications and New Media, the German Chambers of Industry and Commerce, the transmission system operator Amprion and the public-private cooperation between operators of critical infrastructures
Governance	Chairmanship of the Federal Government Commissioner for Information Technology.
Funding	
Tasks	• Raise awareness • Organizes political cooperation on cyber security within the federal government and between the state and industry. • Coordinate the preventive instruments and the policy for cybersecurity between the state and the economy • Gather knowledge from different actors proposals for the further development of national regulations for more cybersecurity
Name	**UP KRITIS (PPP)**
Legal form and members	Public-private cooperation between operators of critical infrastructures and governmental agencies involved in critical infrastructure protection.
Governance	Initiative of BSI and Federal Office of Civil Protection and Disaster Assistance. • Political Council: Council is composed of high-level decision-makers from the operators of critical infrastructures and the administration on equal terms. Strengthens partnership cooperation in the UP KRITIS and provides impulses for strategic goals and projects in UP KRITIS. Deals with personnel, organizational and financial concerns. • Plenary: cross-industry and cross-thematic cooperation • Thematic and sectoral working groups
Funding	
Tasks	Brings together the private and public sector experience and promotes cross-company and cross-sectoral communication and cooperation. Enhances critical

	infrastructure protection through for example recommendations. Platform for communication in crisis management.
Private initiatives	
Name	**Cyber-Sicherheitsrat Deutschland - Cyber Security Council Germany**
Legal form and members	The Council is a private organization that gathers companies, operators of critical infrastructures, experts and policymakers.
Governance	Executive committee of 4 members, general assembly of all members (associated members – authorities and policymakers – have no voting rights)
Funding	Membership subscriptions.
Tasks	Aims to advise businesses, government agencies and policymakers, as well as strengthening cyber security in Germany. The Council has the following objectives: • To increase collaboration between politics, public administration, business and academia for the purpose of improving IT protection. • To set up initiatives and projects to promote awareness of cyber security. • To develop a nationwide cyber-security network in a European and international context. • To provide a knowledge platform, forum and network for members of the association. Actions: • Briefing meetings and discussions on cyber-security. • Industry-based and topic-based working groups for drawing up solutions. • A neutral platform and network to identify collaboration partners. • Advice for policymakers. • Trips abroad for international dialogue with policymakers and business managers on the subject of cyber security. • Organising training on IT security. • Awareness campaigns. • Preparation of studies, analyses and articles. • Commenting on legislation and draft legislation.

12. GREECE

Public Entities	
Name	**National Cyber Security Authority**
Legal form and members	
Governance	Part of the ministry of Digital Policy, Telecommunications and Information. The Authority can ask for the assistance of a National Advisory Board made up of relevant public and private sector relevant stakeholders.

Funding	
Tasks	• Monitors, implements and bears overall responsibility for the National Cyber Security Strategy • National Advisory Body/forum: participation of stakeholders • monitor, coordinate and evaluate the work by the stakeholders involved, for the achievement of the strategic actions and objectives • determines the minimum security requirements and the corresponding technical and organizational measures, which the stakeholders must implement • supervises national exercises • citizen awareness programme
Name	**CERT-GR (NAAEA)**
Legal form and members	
Governance	A division in Cyberspace Directorate of the National Intelligence Agency.
Funding	
Tasks	National CERT. Prevention as well as the passive and active encounter of electronic attacks against communication networks, data storage facilities and IT systems. In addition, the Authority is responsible for processing the data and notifying the competent authorities.
Name	**ADAE – The Hellenic Authority for Communication Security and Privacy**
Legal form and members	
Governance	Bodies: • Plenary • President and vice-president • Several Divisions and Departments
Funding	
Tasks	• Privacy • Security of networks and communications • NIS

13. HUNGARY

Public Entities	
Name	**The National Cyber Security Coordination Council**
Legal form and members	Government body comprised of a representative from the Prime Minister's Office and Ministers with responsibilities relevant to information and cybersecurity.
Governance	Operates under the Ministry of Interior • Daily operative work by a National Cyber Coordinator.

	• Cyber Security Working groups, which involve the private sector • National Cyber Security Forum: forum for governmental decision makers, businesses, NGO's and academics
Funding	
Tasks	• Coordinates the governmental activities • Monitors implementation
Name	**National Cyber Defence institute (cyber security centre)**
Legal form and members	Umbrella organisation, incorporating the CERT-Hungary, the National Electronic Information Security Authority and the Cyber Defence Management Authority.
Governance	Operates under the National Security Service.
Funding	
Tasks	• Regulatory Control and Enforcement • An event management center • Responsible under the NIS • Enhance awareness among users
Name	**CERT Hungary**
Legal form and members	
Governance	Operates within the National Cyber Defense Institute.
Funding	
Tasks	• Operational cyber security capabilities • Has contacts with the private sector for the purpose of promoting information exchanges and developing long-term cyber strategies • Provides educational materials and provides trainings
Private initiatives	
Name	**Hungarian Association of IT Companies**: Industry platform, that touches upon cybersecurity as part of their operations

14. IRELAND

Public Entities	
Name	**NCSC – National Cyber Security Centre**
Legal form and members	
Governance	Operates under the Department of communications, Climate Action and Environment.
Funding	
Tasks	• Advising and informing government IT and Critical National Infrastructure providers of current threats and vulnerabilities associated with NIS • Manage cyber security incidents

	• Guidance and advice to citizens and businesses on major cyber security incidents • International relationships for information sharing • Operates the CSIRT-IE
Public-Private partnerships	
Name	**Cyber Ireland**
Legal form and members	Alliance between industry, academia and government.
Governance	
Funding	Government funding
Tasks	• Pool talent • Innovation through enhanced research • Promotion • Internationalization • Collaboration

15. ITALY

Public Entities	
Name	**Prime Minister and Committee for The Security of the Republic (Comitato Interministeriale per la sicurezza della Repubblica, CISR)**
Legal form and members	
Governance	The committee is supported by a technical committee.
Funding	State funding
Tasks	The **prime minister** has the overall responsibility regarding cyber security, supported by the advice of the Committee. He adopts the National Cybersecurity Strategic Framework and the National Plan and ensures its practical implementation through the adoption of specific directives. The **Committee**: • propose the adoption of legislative measures • approves guidelines to foster public-private partnerships • decision-making role in the approval of measures to improve cyber security • promotes initiatives for participating in international cooperation Technical committee (working level): supervises the timely and correct implementation of the National Cybersecurity Plan
Name	**The Security Intelligence Department (Dipartimento Informazioni per la Sicurezza, Dis)**
Legal form and members	

Governance	
Funding	
Tasks	• Conducting analysis and assessments of cyber threats • Promote cybersecurity awareness and education • providing warnings and information on cyber threats to the Cyber Security Unit • Defines the Cybersecurity requirements that need to be adopted for the protection of ICT systems and critical infrastructures. • works with the Agency for Internal Information and Security (Agenzia Informazioni e Sicurezza Interna, AISI) and the Agency for External Information and Security (Agenzia Informazioni e Sicurezza Esterna, AISE) for ICT security and interacts with public authorities, academia, and public electronic communications networks and service providers.
Name	**The Cybersecurity Unit (Nucleo per la Sicurezza Cibernetica)**
Legal form and members	The Unit is comprised of representatives of the Ministries of Economy and Finance, Health, Foreign Affairs, Interior, Defense, Justice, the AISE, AISI, DIS, and the Department of Civil Protection.
Governance	Established by a Decree of the Council of Ministers. Operates within the Prime Minister's Military Advisor's Office.
Funding	
Tasks	• Coordinates the activities of the institutions responsible for cyber security, • handles cyber incidents and restores network functionality, • point of contact during a crisis • 24/7 Alert and Response Cell • NIS • evaluates and promotes procedures for information-sharing and early warning for crisis management • promotes and coordinates the execution of cyber security exercises on the national level and coordinates the nation's participation in international exercises • disseminates cyber alerts • Information sharing with public and private stakeholders. In case of a cybersecurity incident they can activate the Inter-ministerial Unit for Situation and Planning (Nucleo Interministeriale Situazione e Pianificazione, NISP), in its Inter-ministerial Cyber Crisis Unit composition (Tavolo interministeriale di crisi cibernetica), which oversees response coordination, while the national Computer Emergency Response Team (CERT) is responsible for technical response measures. CERT-N: national CERT, prevent cyber incidents and coordinate the national response to such incidents, manage cyber crises and interact with private sector in that regard.

	CERT-PA: CERT of the public administration, management of incident reporting for cybersecurity incidents occurring within its government-based constituency. Facilitates public-private information sharing
Name	**Inter-ministerial Unit for Situation and Planning (Nucleo Interministeriale Situazione e Pianificazione, NISP)**
Legal form and members	Involves representatives from the Ministries of Defence, Foreign Affairs and the Interior as well as from other agencies and administrative bodies including AISI and the Department of Fire, Rescue and Public Civil Defence
Governance	The NISP is chaired by the Secretary of State.
Funding	
Tasks	• supports inter-ministerial coordination in crisis prevention and emergency preparedness by harmonising common procedures and capabilities (information sharing, intelligence-gathering, inter-ministerial and operational planning, international collaboration) • develops crisis exercises • In the event of a crisis, NISP maintains a coordinating role, but also acts to examine the situation, to identify and propose measures to be taken by CoPS and the President of the Council of Ministers, and to formulate the national position and collaborative efforts vis-à-vis international actors. In the execution of its crisis preparation and response mandate, NISP relies on approval and support from the Ministry of the Interior and its Interministerial Technical Commission for Civil Defence (Commissione Interministeriale Tecnica per la Difesa Civile, CITDC)
Name	**Political Strategic Committee (Comitato Politico Strategico, COPS)**
Legal form and members	Ministers of Foreign Affairs, the Interior, Defence, and Economy and Finance
Governance	
Funding	
Tasks	Advisory body for the President of the Council of Ministers in case of a crisis
Public-Private partnerships	
Name	**CERT-Nazionale**
Legal form and members	Public authority that works together with all other relevant stakeholders.
Governance	Operates under the ministry of Economy. Headed by the Director General of the High Institute for Communication and Information Technologies (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)). CERT Nazionale is not an authoritative body. It performs its functions through cooperation agreements and protocols.
Funding	Government funding
Tasks	• provide timely information on potential cyber threats that could harm businesses and citizens

	• increase awareness and a culture of security; • to cooperate with similar institutions, national and international, and with other public and private actors involved in information security by promoting their interaction • facilitate the response to large-scale cyber incidents • provide support in the cyber-crisis resolution process.
Private initiatives	
Name	**Global Cyber Security Centre**: Non-profit, develop and disseminate knowledge and awareness on Cyber Security, creating the conditions for improving capabilities, skills, cooperation and communication between the different stakeholders involved in the use and protection of internet.
Name	**The Italian Association of Critical Infrastructures' experts**: Non-profit organization made up of academic representatives, network providers and entities engaged with critical infrastructure.
Name	**ANITEC:** a representative body for information technology companies in Italy, engages with cybersecurity in the course of its operations

16. LATVIA

Ministries that touch upon cyber security each have a role in handling the strategy, methodology and coordination of cyber security for their respective competences.

Public Entities	
Name	**National Information technology Security Council**
Legal form and members	Comprised of all ministers who touch upon cybersecurity.
Governance	Operation is ensured by the National Cyber Security Policy Coordination Section of the Ministry of Defence
Funding	State funding.
Tasks	• Coordinates the development of cyber security policy and planning • Implementation of objectives and measures • Platform for exchange of information and cooperation between the public and private sector
Name	**Cyber Defence Unit**
Legal form and members	
Governance	Operates under the Ministry of Defence.
Funding	
Tasks	Support in crisis situations.
Name	**CERT.LV**

Legal form and members	
Governance	Operates under the auspices of Institute of Mathematics and Computer Science, University of Latvia, with authority delegated by and under supervision of the Ministry of Defence of the Republic of Latvia.
Funding	Financed by the Ministry of Defence.
Tasks	• Coordinating security and incident response measures across all Latvian networks • Research • Organizes educational events and training • Supervises the implementation of obligations specified in the Law on the Security of Information Technology • National competent authority for network and information security in Latvia • Contact point for reporting cyber security incidents
Public-Private Partnerships	
Name	**Information Technology and Information Systems Security Expert Group - DEG**
Legal form and members	Consists of information technology and information systems security experts from various organizations in Latvia
Governance	Initiative of CERT.LV
Funding	
Tasks	• Enhance IT/IS security level in the Republic of Latvia • Facilitate information exchange among the members of the group on IT/IS security threats • Encourage and support professional growth of the group members • Educate general public on IT/IS security topics • Support CERT.LV

17. LITHUANIA

Public Entities	
Name	**Ministry of National Defence**
Legal form and members	
Governance	Minister of National Defence supported by 4 vice-ministers.
Funding	
Tasks	Formulate, coordinate and implement the organisation of the organisation of the state cybersecurity policy
Name	**National Cyber Security Centre (NCC)**
Legal form and members	Public authority, but direct contact with the public sector and with operators of critical information infrastructure.

Governance	Under the ministry of National Defence.
Funding	
Tasks	• manages the cyber security information sharing network which is used to exchange cyber security related information among the community of interest (CISN) • maintains a system of sensors to monitor cyberspace with a focus on protection of critical information infrastructure • contact point for cyber security officers or cyber security units of institutions • Cyber security incidents have to be reported to the NCC
Name	**CERT-LT**
Legal form and members	
Governance	Operated by the NCC
Funding	
Tasks	Coordinating security and incident response measures across all Lithuanian networks.
Public-Private partnerships	
Name	**Advisory Council on Cyber Security**
Legal form and members	Includes representatives from the public, private and academic sectors.
Governance	Chaired by the Ministry of National Defence.
Funding	
Tasks	• National level advisory group • Prepare and submit proposals to the CISN regarding priorities, areas of focus for further activity, propose goals and means to achieve them • Prepare and submit proposals to the CISN for wider public, private and research cooperation in the area of cyber security • Analyze cyber security implementation methods and provide the CISN proposals for more effective management of cyber incidents • Submit the CISN with recommendations for strengthening cyber security
Name	**Cyber Security Stakeholder Information Sharing Network (CISN)**
Legal form and members	Volunteer community of experts with individual membership, independently from the organisations they represent.
Governance	Managed by the NCC.
Funding	
Tasks	Gathers cybersecurity experts in one place to share knowledge, expertise and information about threats.
Private initiatives	
Name	**Infobalt**: association of Lithuanian ICT Companies

18. LUXEMBOURG

Public Entities	
Name	**ANSSI – The National Agency for the Security of Information Systems**
Legal form and members	
Governance	Under the office of and operated by the High Commissioner for National Protection.
Funding	Government funding.
Tasks	Defines policies and guidelines for the security of classified and unclassified information, ensures that norms and standards are established, that the measures regarding the security of information systems are implemented and that the application is guaranteed
Name	**CSB – Cyber Security Board Luxembourg**
Legal form and members	Composed of representatives of the relevant Ministries.
Governance	Under the Ministry of Communications and Media.
Funding	
Tasks	Defines a strategy for the security of information systems
Name	**Cybersecurity Coordination Committee**
Legal form and members	Members of the main state entities involved in national cybersecurity.
Governance	Chaired by the High Commissioner for National Protection, who also acts as a secretariat.
Funding	
Tasks	• Coordinate the implementation of initiatives and policies • Advise the government on cybersecurity
Public-Private partnerships	
Name	**SMILE – Security Made in Luxemburg**
Legal form and members	Composed of companies form Luxembourg and non-Luxembourg companies which can deliver high quality services in cybersecurity.
Governance	Created by the Ministry of Economy in 2010. Management board and president are from the government.
Funding	Government subsidies.
Tasks	• Assisting the ministry • provide support in the areas of GDPR and NIS • operates CASES: promotion of information security in companies • operates C3: National Centre for Cybersecurity Skills • operates CIRCL: Coordination and Post-incident Action Unit, which also acts as a CERT for private and non-governmental entities and communes
Name	**CIRCL**

Legal form and members	
Governance	Operated by SMILE but under the auspices of, and with authority delegated by, the Grand Duchy of Luxembourg.
Funding	Government funding.
Tasks	National CERT.

19. MALTA

Public Entities	
Name	**National Cyber Security Strategy Steering Committee**
Legal form and members	
Governance	Operates under the Prime minister.
Funding	
Tasks	Coordinates and oversees the implementation of the National Cyber Security Strategy.
Name	**MITA - Malta Information Technology Agency**
Legal form and members	
Governance	Operates under the Prime minister. Bodies: • Executive chairman • MITA Board of Directors • MITA Executive Committee
Funding	State funding
Tasks	• Deliver and implement the assigned programmes as set out in the Digital Malta National ICT strategy • Manages the implementation of IT
Name	**Malta Communications Authority**
Legal form and members	Independent government agency.
Governance	• Board of Directors • Chairman • Management Committee
Funding	Government funding, EU funding (projects) and revenues from communication companies, spectrum and licensing.
Tasks	Regulation of the electronic communications sectors. Deals with Cybersecurity in this area.
Name	**CSIRTMalta**

Legal form and members	
Governance	Established within the MaltaCIP Unit (Critical infrastructure protection), Cabinet Office, Office of the Prime Minister.
Funding	
Tasks	• Promotes sharing of unclassified information which may be useful against cyber attacks • Provides alerts and warnings to its constituents
Public-Private partnerships	
Name	**Innovation Hub**
Legal form and members	Composed of experts in entrepreneurship, marketing and management.
Governance	Run by MITA.
Funding	
Tasks	Guidance for start-ups.

20. THE NETHERLANDS

Public Entities	
Name	**National Cyber Security Centre**
Legal form and members	
Governance	Falls under the responsibility of the Ministry of Justice and Security. Consists of a general manager and 3 teams for incident response, knowledge services and organizational development. National Coordinator for Security and Counterterrorism (NCTV) at the Ministry is commissioner for NCSCNL.
Funding	
Tasks	• Operates the national CERT • Response to threats and incidents • Perception and action prospects • Improving crisis management • Cyber security collaboration platform
Public-Private partnerships	
Name	**Cyber Security Council**
Legal form and members	Formal independent strategic advisory council created in 2011. Composed of high-placed representatives of the industry, public administration and academia.
Governance	Co-chairmanship between the public and private sector, secretariat provided by the government.
Funding	Government subsidies.
Tasks	• Give solicited and unsolicited advice to the Dutch government • Monitor the Cyber Security Strategy implementation • Give strategic advice

	• Contribute to research in the scope of the Dutch Cyber Security Research Agenda

21. POLAND

Several public bodies have cyber security roles: Ministry of justice, Ministry of the Interior and Administration, the internal Security Agency, the Government Centre for Security, office of Electronic Communications, Financial Supervision Authority, The Inspector General for the Protection of Personal Data, the National Security Bureau.

Public Entities	
Name	**Ministry of Digital Affairs – Department of cyber Security**
Legal form and members	
Governance	Ministry: Policy level. Responsible for coordinating the implementation of the cybersecurity policy Council for Digitization: gives its opinion on strategic documents Department of cyber security
Funding	
Tasks	Tasks of the Department • development and implementation of strategic documents and legal acts in the field of cyber security; • national and international cooperation (especially with European Union institutions); • development of guidelines and standards for the appropriate measures of IT systems protection; • preparation of analyses on cyber security and related risks to state security; • development of central training plans, exercises and tests. • cooperation with universities, institutes, NGO's and the private sector
Name	**NASK – Research and Academic Computer Network**
Legal form and members	
Governance	Supervised by the Department of cyber security.
Funding	State funded.
Tasks	• Ensuring the security of the internet • Responding to cybersecurity threats at an operational level • Education • Research and development
Name	**CERT.PL**
Legal form and members	

Governance	Operated by the NASK.
Funding	
Tasks	• recording and handling of events that violate network security • active response in case of direct threats to users • cooperation with other CERT / CSIRT teams in Poland and in the world • participation in national and international projects related to the subject of IT security • research activity in the field of methods of detecting security incidents • analysis of malware and hazard information exchange systems • developing own tools to detect, monitor, analyze and correlate threats • regular publication of the CERT Polska Report on the security of Polish Internet resources • information and education activities aimed at increasing awareness in the field of IT security
Public-Private partnerships	
Name	**National Cyber Security Centre (Rzadowe Centrum CYBERBezpieczenstwa – NCCyber)**
Legal form and members	Governmental institution, established by the Crisis Management Act, that consults the providers of critical infrastructures.
Governance	Operates within the NASK.
Funding	
Tasks	Collecting and analysing, as part of the National Cyberspace Protection System, information about cyberthreats, submitted by institutions participating in the initiative.
Private initiatives	
Name	National Chamber of Commerce for Electronics and Telecommunications (KIGEit).
Name	Polish Chamber of Information Technology and Telecommunications (PIIT)

22. PORTUGAL

Public Entities	
Name	**The national security office (GNS)**
Legal form and members	
Governance	Headed by a Director General (the National Security Authority) and two deputy Directors-general.
Funding	
Tasks	• ensuring the security of information classified at the national level and of international organizations of which Portugal is a party • accreditation • operating the CSCS

Name	**Higher Council for the Security of the Cyberspace**
Legal form and members	High-ranking officials of the Portuguese state.
Governance	
Funding	
Tasks	Political-strategic coordination
Name	**Centro Nacional De Cibersegurança Portugal (CSCS) – National Cyber Security Centre**
Legal form and members	
Governance	Operates under the GNS, one of the subdirector-generals of the GNS is the coordinator of the CSCS.
Funding	
Tasks	• Operational coordination • Crisis management • Develop the national capacities for the prevention, monitoring, detection, analysis and correction designed to cope with cybersecurity incidents and cyberattacks. • Contribute for the security of the information and communication systems of the State entities, Operators of Essential Services and Digital Service Providers. • Promote the training and qualification of human resources in the area of cybersecurity, with the objective of creating a community of knowledge and a national culture of cybersecurity. • Promote and ensure the coordination and cooperation between the various actors involved and responsible in the area of the national cybersecurity. • Support the development of technical, scientific and industrial capabilities, promoting projects for the innovation and development in the area of cybersecurity. • Ensure the planning of the cyberspace use in situations of crisis and in war situations within the frame of the emergency civil planning, as defined in the Decree-Law 73/2013, of May 31. • Coordinate the international cooperation on cybersecurity issues, in coordination with the Ministry of Foreign Affairs. • Coordinate the transposition of the Directive (EU) 2016/1148 of the European Parliament and of the Council, concerning measures to ensure a high common level of network and information security across the Union, to the internal legal order. • Reviews cybersecurity policies • Recommendations for the capacity building of CSIRTs • Recommendations for carrying out internal cybersecurity audits • Promotion of training and awareness actions • Liaising with the private sector

	• Operates the CERT.PT, the national CERT
Name	**CERT.PT**
Legal form and members	
Governance	Operated by the CSCS.
Funding	
Tasks	Responsible for the prevention of incidents and the coordination of incident response measures across all Portuguese networks.

23. ROMANIA

Public Entities	
Name	**National Cyberint Center**
Legal form and members	
Governance	Under the Romanian Intelligence Service.
Funding	
Tasks	Aims to correlate technical defense systems with intelligence capabilities in order to identify and provide legal beneficiaries with the necessary information to prevent, contain and/or preclude the consequences of any attack against the IT&C systems that are part of critical infrastructure.
Name	**The National Cyber Security System/Centre (SNSC) (unclear whether operational)**
Legal form and members	Composed of representatives from public institutions, cooperation with academia and business, professional associations and organizations NGOs.
Governance	Coordinated by the Supreme Council of National Defense.
Funding	
Tasks	• building and maintaining a range of cybersecurity measures. • knowledge, prevention, coordination and counteracting of threats, vulnerabilities and specific risks specific to the cyberspace that may affect national cyber security infrastructure
Name	**The Operative Council for Cyber Security (unclear whether operational)**
Legal form and members	Composed of representatives from Romanian government ministries (Special Telecommunications Service, Foreign Intelligence Service, Protection and Guard Service, the National Registry Office for Classified Information (ORNISS) and the Secretary of the Supreme Council of National Defense) and Romanian intelligence services.
Governance	
Funding	
Tasks	• oversees the SNSC in its duties

	• responding in the event of critical cybersecurity incidents
Name	**CERT-RO**
Legal form and members	Government institution
Governance	
Funding	
Tasks	National CERT. Responsible for the prevention of incidents and the coordination of incident response measures across all Romanian networks. Research, development and expertise in the field of cyber-security.
Private initiatives	
Name	**The Cyber Security Research Centre (CCSIR)**
Legal form and members	NGO. Members are natural and legal persons active in the field of cybersecurity.
Governance	
Funding	
Tasks	Committed to the development and research of cybersecurity

24. SLOVAKIA

All state authorities deal with cybersecurity when relevant for their subject. Besides the Ministry of finance, also the ministry of interior and other authorities have roles in cybersecurity.

Public Entities	
Name	**National Security Council**
Legal form and members	Composed of the ministers of Slovakia.
Governance	The prime minister holds the chair.
Funding	
Tasks	Drafts the cyber security strategy. Advises the government.
Name	**National Security Authority**
Legal form and members	
Governance	Controlled by Special Parliamentary Control Committee for the Control of NSA Activities. Bodies: • Director: responsible for the activities, management and representation • NSA office: coordinates the Authority's individual units and provides and conducts essential administrative and organisational activities connected with the management and function of the Authority. • Security Clearance Department

	• **Technical Department: accreditation and certification processes, responsible for cybersecurity and operates the CERT.SK** • Regulation and Supervision Division • Economy and operations Department • Internal Security Division • Internal auditor
Funding	
Tasks	The national competent authority or network and information security. Focusses on classified information.
Name	**Ministry of Finance – Information Society Section**
Legal form and members	
Governance	Several divisions and departments: • Department of Information Society Strategy • Department of Information of Public Administration • Department of Implementation Programmes of Development of Information Society • Department of Management Programmes of Development of Information Society • Department of Information Technology • Department of Management IT resources of Public Administration
Funding	
Tasks	• input on the legislative process • analyzing various aspects including financial and business environment of the impact on information society development • represents the Ministry of Finance on matters of internet governance, standards, and information security in the Legislative Council of the Slovak Government, but also at the EU and other institutions • oversees standards implementation in the public administration sector and its information systems
Name	**Committee for Information Security**
Legal form and members	Representatives from the Information Society Section of the Ministry of Finance, the Office of the Government, the Ministry of Interior, NSA, Slovak National Accreditation Service, IT Association of Slovakia, Slovak Association for Information Security, and a representative of an academic research institution in information security.
Governance	Under the Ministry of Finance
Funding	
Tasks	Facilitates communication between several actors, advisory and coordinating role, preparing strategic and technical materials on information security.
Name	**CSIRT.SK**

Legal form and members	

Governance	Operates as an independent department of DataCentrum.
	
	Bodies:
	• headed by a Director
	• Information Specialist: contact point
	• 3 departments:
	  ○ the Technical Department responsible for monitoring and gathering information about cyber security threats and risks;
	  ○ the National Information and Communication Infrastructure (NICI) Department which deals with incident handling;
	  ○ Education Department, which develops and implements education concepts for the security managers and ICT security staff of state and public institutions, and for the general public and cyber security professionals

Funding	Financed from the budget of the Ministry of Finance.
Tasks	• coordinating incident response measures for Slovak state authorities and entities engaged with critical infrastructure • including alerts and warnings based on analysis of security threats and vulnerabilities; manuals for addressing the most common incidents; analysis of incidents and malware; response to incidents and malware; and incident response coordination • education, information distribution, awareness-building and consultancy in information security; threat monitoring in the field of ICT, infiltration detection, and information dissemination about threats and vulnerabilities; as well as configuration and infrastructure maintenance, and technology watch.
Public-Private Partnerships	
Name	**Cyber Security Commission (CSC)**
Legal form and members	Representatives of public sector, private sector and academia.
Governance	Operates under the NSA.
Funding	
Tasks	Advisory body of the National Security Authority's Director created in 2016 by the Cyber Security Concept and Action Plan. Addresses the needs and knowledge of private sector and academia before strategic issues are discussed at the political level. • Prepares the concept of state policy in the area of cyber security and directs its implementation in individual administration sectors, • Prepares drafts of generally binding regulations and methodology, prepares rules for accrediting incident resolution units, • Methodically directs the preparation of operating procedures for reactions to cyber threats at a national level,

	• Coordinates the preparation of action plans for material areas with relevant central state administration bodies, • Coordinates, monitors, controls and evaluates the execution of tasks in the area of cyber security at a national level, • Serves as the national contact point for the EU and NATO in the area of cyber security/defence, • Provides and coordinates the execution of tasks implied by international cooperation, represents the Slovak Republic internationally in the area of cyber security, • Based on documents from other sectors, processes and prepares consolidated opinions for the Slovak Republic in the area of cyber security, • Prepares Reports on the state of cyber security in the Slovak Republic and submits them for approval to the Cyber Security Committee of the Security Council of the Slovak Republic, • In crisis management of the Slovak Republic, proposes and submits procedures for the case of cyber attacks, • Continuously monitors the national cyber space and analyses potential and current threats, • Performs state supervision over the activities of incident resolution units.
Private initiatives	
Name	**IT Asociacia Slovenska (ITAS)**
Legal form and members	Represents Slovak and international information technology companies
Governance	
Funding	Membership fees.
Tasks	Engages with cybersecurity in the course of its operations.

25. SLOVENIA

Information Security Sector within the IT Directorate at the Ministry of Public Administration, the Ministry of Defence for defence systems and protection against natural and other disasters, Slovenian Intelligence and Security Agency (SOVA) in counter-intelligence activities, and the Police within its IT and telecommunications Office and the Criminal Police Directorate, mainly in the Centre for Computer Investigations with the capacities to combat cybercrime.

Public Entities	
Name	**The Communications Networks and Service Agency (AKOS)**
Legal form and members	Independent government entity.
Governance	Director and Deputy Director, supported by Advisors.
Funding	
Tasks	National competent authority and regulator for network and information security

Name	**SI-CERT**
Legal form and members	
Governance	Operates within the framework of the Arnes (Academic and Research Network of Slovenia), a public institute that provides network services to research, educational and cultural organizations, and enables them to establish connections and cooperation with each other and with related organizations abroad. ARNES: • Board of Directors is appointed by the Government of the Republic of Slovenia. The Board of Directors adopts the Operating Plan and the Final Accounts, • Technical Board deals with programme and development issues.
Funding	SI-CERT is financed from the fund provided to the Arnes public institute by the Directorate for Information Society of the Ministry of Education, Science and Sport.
Tasks	National cyber security incident response center. Coordination of security procedures and incident response measures across all Slovenian networks.
Public-Private partnerships	
Name	**Slovenian Digital Coalition**
Legal form and members	Forum of public sector and industry and academic stakeholders working in the field of digitalisation of trade and industry, smart cities, e-commerce, e-skills, e-inclusion, cyber security, internet and other areas related to developing the digital society.
Governance	Management Board made up of stakeholder representatives.
Funding	
Tasks	• Shape and guide digitalization • Co-ordinate strategies and concepts • Seek stakeholder synergies and integration • Support and promote digital transformation • Participation in lectures, public meetings and annual forum • Participation in business visits and international links • Support Slovenia digital references
Name	**Centre for Safer Internet**
Legal form and members	Run by a consortium consisting of the Faculty of Social Sciences, ARNES, Slovenian Association of Friends of Youth and the Youth Information and Counselling Centre of Slovenia - MISSS
Governance	

Funding	Financed by the Directorate-General Connect of the European Commission and the Ministry of Education, Science and Sport.
Tasks	Promoting and ensuring a better internet for kids
Private initiatives	
Name	**Digital Innovation Hub (DIH)**
Legal form and members	Stakeholder platform: universities, research and business institutes, companies, ICT providers and business support organizations
Governance	
Funding	Membership fees, structural funds and EU financing.
Tasks	Creates awareness and provide services to grow digital competencies, share digital experience and case studies locally, regionally and internationally, influence the government to adapt regulation and open its data to foster entrepreneurship.

26. SPAIN

Public Entities	
Name	**The national Centre for Infrastructure Protection and Cybersecurity (CNPIC)**
Legal form and members	Government agency, working closely with the industry.
Governance	Operates under the Spanish Ministry of the Interior. Accountable to the Secretary of State of Security.
Funding	
Tasks	Responsible body for the promotion, coordination and supervision of all politics and activities related to the protection of critical infrastructures and cybersecurity.
Name	**National Advisory Council on Cybersecurity (CNCCS)**
Legal form and members	Public authorities that touch upon cybersecurity. Representatives from the information technology and critical infrastructure sectors.
Governance	Supported by the Department of National Security in its capacity as Technical Secretariat and permanent working body of the National Security Council.
Funding	
Tasks	• Support the decision making of the National Security Council on cybersecurity through the analysis, study and proposal of initiatives both nationally and internationally. • Strengthen coordination, collaboration and cooperation between the different public authorities with competences related to the field of cybersecurity, as well as between the public and private sectors. • Contribute to the development of regulatory proposals in the field of cybersecurity for consideration by the National Security Council.

	• Provide support to the National Security Council in its function of verifying the degree of compliance with the National Security Strategy in relation to cybersecurity and promoting and promoting its revisions. • Verify the degree of compliance with the National Cybersecurity Strategy and inform the National Security Council. • Carry out the assessment of risks and threats, analyze possible crisis scenarios, study their possible evolution, prepare and maintain updated response plans and formulate guidelines for conducting crisis management exercises in the field of cybersecurity and evaluate the results of its execution, all in coordination with directly competent bodies and authorities. • Contribute to the availability of existing resources and carry out studies and analysis on the means and capacities of the different public authorities and agencies involved in order to catalog the effective response measures in line with the available means and the missions to be carried out, all this in coordination with the bodies and authorities directly competent and in accordance with the competences of the different public authorities and agencies involved in the field of cybersecurity. • Facilitate the operative coordination between the organs and competent authorities when situations that affect the Cybersecurity require it
Name	**INCIBE - Spanish National Cybersecurity Institute**
Legal form and members	State commercial company.
Governance	Under the Ministry of Economy and Business, through the Secretariat of State for Digital Advance.
Funding	State Funding.
Tasks	Strengthen cybersecurity, trust, and the protection of privacy with respect to services offered within the information society, providing value to the public, businesses, the Spanish Government, the Spanish academic and research network, the information technology sector and strategic sectors in general.
Name	**INCIBE-CERT**
Legal form and members	
Governance	Operated by The Spanish National Cybersecurity Institute (INCIBE), under the Ministry of Economy and Business (MINECO) through the Secretary of State for Digital Advancement (SEAD).
Funding	
Tasks	National CERT. In the case of incident management affecting critical private sector operators, INCIBE-CERT is jointly operated by INCIBE and CNPIC,
Public-Private partnerships	
Name	**Spanish Technology Platform on Industrial Safety**

Legal form and members	Set up under Spanish law in 2007, as third sector associations.
Governance	Led by a private research entity, the Ministry of Economy participates in the board.
Funding	Government subsidies and mandatory member fees.
Tasks	• Research and development of new technologies to increase the level of security in the private sector • Participate with the government to create cybersecurity strategy and initiatives
Name	**Spanish Technology Platform on Industrial Safety**
Legal form and members	Platform created by the industry in 2008, involving INCIBE.
Governance	Governed by members from the industry in the management board, who are equally represented. Work is organized in working groups, for which chairs are elected.
Funding	Government subsidies and mandatory member fees.
Tasks	Promoting Spanish cybersecurity products and services and get access to EU funding.
Private initiatives	
Name	**Centre for Industrial Cybersecurity (CCI)**
Legal form and members	Non-profit organization
Governance	Management team, Coordinators and Experts.
Funding	Membership fees, structural funds and EU financing.
Tasks	Provide and improve awareness of cybersecurity issues and to facilitate communication channels between industry and lawmakers and to improve cybersecurity outcomes.
Name	**The Spanish Association for the Promotion of Information Security - AES**
Legal form and members	Non-profit organization.
Governance	
Funding	
Tasks	Organizes multiple information security initiatives. The Cyber Security Spanish Institute, which publishes reports on cybersecurity in Spain, is one such initiative.

27. SWEDEN

Public Entities	
Name	**MSB – Swedish Civil Contingencies Agency**

Legal form and members	
Governance	Operates under the Ministry of Defence, Cybersecurity and Critical Infrastructure Protection Department.
Funding	
Tasks	• Strategic support and analysis section • Information Security Governance Section • Critical Infrastructure Protection and Critical Information Infrastructure Protection • Operational Cybersecurity and IT Incident Response Section
Name	**SAMFI**
Legal form and members	Consists of a number of central government authorities that have particular tasks in the area of cyber security: the Swedish Civil Contingencies Agency (MSB), the Swedish Defence Materiel Administration, the National Defence Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Police Authority, the Swedish Post and Telecom Authority (PTS) and the Swedish Security Service.
Governance	MSB has administrative responsibility for the group. Representatives from the authorities in SAMFI meet approximately 6 times a year to discuss current work and issues within the field of societal information security. After consensus in SAMFI, working groups can be appointed to work on current issues. A SAMFI authority is entitled but not obliged to participate in these working groups.
Funding	
Tasks	Guarantee societal information assets as regards the abiltiy to maintain the desired levels of confidentiality, accuracy and availability. Through exchanges of information and cooperation the authorities in SAMFI support each other's work on societal information security.
Name	**National Cooperative Council against Serious IT Threats (NSIT)**
Legal form and members	Consists of the Swedish Security Service, FRA and the Swedish Armed Forces through its Military Intelligence and Security Service (MUST).
Governance	
Funding	
Tasks	Analyses and assesses threats and vulnerabilities regarding serious or qualified cyberattacks against the most security-sensitive national interests. NSIT
Name	**CERT-SE**
Legal form and members	
Governance	Operated by MSB.
Funding	
Tasks	• National CSIRT with the task of supporting society in the work of managing and preventing IT incidents.

	• Act promptly on the occurrence of IT incidents by spreading information and, if necessary, coordinating measures and participating in work that is required to remedy or alleviate the effects of it. • Collaborate with authorities with specific tasks in the field of information security. • contact point towards the corresponding functions in other countries and develop the cooperation and the information exchange with them.
Public-Private partnerships	
Name	**National Telecommunications Coordination Group (NTSG)**
Legal form and members	Composed of representatives from entities engaged with electronic communications critical infrastructure and public authorities.
Governance	The chair is elected by the Group itself. Chair held by the Swedish Post and Telecom Authority (PTS), who is also providing administrative support.
Funding	
Tasks	Protecting the critical infrastructures in the event of crisis.
Private initiatives	
Name	**IT & Telekomforetagen**
Legal form and members	Forum for Swedish companies in the information technology and telecom sector.
Governance	
Funding	Membership fees
Tasks	The mission is to create the best possible conditions for a competitive Swedish IT and Telecom industry. Engages with cybersecurity in the course of its operations

28. UNITED KINGDOM

National policy leadership lies with Prime minister, Cabinet Office, Department for Digital, Culture, Media and Sport, Ministry of Defence, etc.

Public Entities	
Name	**NCSC – National Cyber Security Centre**
Legal form and members	
Governance	Part of **GCHQ** (Government Communications Headquarters), a foreign-focused signals intelligence agency.
Funding	
Tasks	• The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. We also work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners. • Responsible for protecting government networks and key parts of the Critical National Infrastructure and Defence.

	• Cyber security advice both on a high level as on the level of consumer safety. Does not handle every complaint or fraud incident, handles major incidents above a certain threshold of national-scale significance. • Guidance • Threat assessment • Incident response • Information sharing • Support for regulators • Support for national skills programmes • Accreditation • Education and research • Direct role in defence of non-military government networks and some parts of Critical National Infrastructure and Defence • CERT-UK and GovCERT • Accreditation of Academic Centres of Excellence, Cyber first schemes, incubators and accelerators for cyber start-ups, Cyber Security Body of Knowledge project (determines the areas of knowledge essential to Cybersecurity), Cyber Essentials certification scheme • GCHQ and MOD (Defence of Military Networks) jointly run National Offensive Cyber Programme.
Public-Private partnerships	
Name	**Cyber Growth Partnership**
Legal form and members	Composed of national and international companies with a large presence or investment in the UK.
Governance	Created by the government in 2013 on initiative of the private sector. co-chairmanship between a Minister and the CEO of a large-scale company, the board consists out of industry members and the secretariat is provided by the government.
Funding	Government subsidies.
Tasks	• Identify the barriers for the growth of the cybersecurity industry. • Promotion of UK cybersecurity products and services abroad • Now mainly providing strategic advice and guidance to the government
Name	**Industry 100**
Legal form and members	Collaboration between the government and the private sector, brings together secondees from several sectors and NCSC officials.
Governance	
Funding	The secondees should be paid by the individual organizations.
Tasks	Exchange of expertise and data.
Private initiatives	
Names	• UK Cyber Security Forum • ADS • Business Continuity Institute (BCI) • Council of Registered Ethical Security Testers (CREST)

	• Crypto Developers Forum • Information Assurance Advisory Council (IAAC) • Information Assurance Collaboration Group (IACG) • Information Systems Security Association (ISSA) • Institute of Information Security Professionals (IISP) • ISACA • (ISC)² • NDI UK • TechUK • Tigerscheme • UK Council for Electronic Business • British Computer Society (BCS) • Cyber Scheme • Academic • Academic Centres of Excellence in Cyber Security Research • University of South Wales Information Security Research Group • De Montfort University Cyber Security Centre