Annex A: Mapping of cybersecurity strategies (September 2014)

Country	Objectives	Focal areas of action	Inputs[1]	Outputs[2]	Stakeholder involvement	Outcomes	Review/evaluation mechanisms

1. Austria	Establish and implement legislative framework;
	Establish and clarify roles in collaboration between the public and private sector involved in cybersecurity;
	Secure, safe place to do business;
	Citizens' perception of sufficient data protection;
	Awareness raising;
	Preparedness, resilience and adequate response to cyberthreats and attacks;
		Develop standards and norms, legislation;
		Create a culture of security: inform, educate, raise awareness;
		Strategic collaboration between authorities, business and academics;
		Protect critical information infrastructure;
		Research, development and innovation;
		International cooperation;
			Examples
			Legislative measures;
			Establish/improve processes & coordinating structures;
				Examples
				Annual reports;
				Minimum cybersecurity standards;
				Improved regulatory frameworks;
					Government;
					Private-Public cooperation as a guiding principle;
					Private sector: enhance competitiveness of business overall
					→
					Strengthening support and tools for SMEs;
						Increased resilience against cyberthreats and attacks;
						Strengthened capabilities protecting critical information infrastructure, communication networks and services;
						Prevention of threats;
						Greater confidence in safety of using cyberspace by citizens, businesses, public sector;
						A cyberspace optimal for societal development;
							Regular progress reports;
							Strategy adjustments based on review.

2. Belgium	Secure cyberspace with respect for fundamental rights and values.
	Protection and efficient functioning of
		Develop standards and norms, legislation;
		Threats tracking, risk assessment and response;
		Security of information
			Legislative measures;
			Increasing law enforcement and judiciary capabilities;
				International cooperation;
				Public-private partnerships;
				Capabilities to counter cybercrime;
					Government;
					Academic institutions;
					Private – Public sector cooperation;
					Private sector: facilitating
						A secure, credible and reliable cyberspace for all users;
						International cooperation;
						Stimulate technological capabilities
							Regular evaluation of security policies;

[1] In many cases these have not been specified by area of action or specific measure; therefore we have made a selection of examples that illustrate the Member States' inputs related to the NCSS.

[2] Similarly, the outputs are not always mapped against the objectives and/or areas of action. We present a non-exhaustive list of prospective outputs mentioned in the NCSSs.

	critical information infrastructure ;
	Preparedness , resilience and adequate response to cyber threats and attacks;
		and services delivered in cyberspace;
		Protect critical information structure;
		Counter national and international criminal activities;
		Research, development and innovation;
					local economy security providers
					ICT service providers and network operators;
					International community;
					Individual citizens;
						and national academic initiatives in security and privacy knowledge;
						Maintaining and promoting economic and social prosperity;	

3. Czech Republic	Awareness raising;
	Establish and implement legislative framework;
	Protection and efficient functioning of critical information infrastructure ;
		Develop standards and norms, legislation;
		International cooperation;
		Protect critical information structure;
			Examples
			Tools & organisational components;
			Establish/improve processes & coordinating structures;
				Improved regulatory frameworks;
				A balance between guaranteeing civil & human rights and cybersecurity in legislation
				Improved capabilities (processes, tools and coordinating structures);
					No structured stakeholder involvement mechanism;
					private sector, government and citizens are individually responsible for securing cyberspace;
					Shared definition & enforcement of minimum standards between business and government;
						A balance between privacy, fundamental rights and liberties, free access to information with the need to guarantee security;
						Better cybersecurity practices and procedures;
						Establishing a cost-effective structure avoiding excessive burden on private entities;
							Regular evaluation of security policies;
							Testing the efficiency of processes designed to deal with security risks;

4. Estonia	Protection and efficient functioning of critical information infrastructure ;
	Education and training;
	Awareness raising;
		Develop standards and norms, legislation;
		Competence and capabilities building of involved actors;
			Legislative measures;
			Implementation plans;
			Introduce cybersecurity in curricula of education system;
				Action and emergency response plans;
				Improved regulatory frameworks;
				International cooperation;
					Government;
					International community;
					Private – Public sector cooperation;
					Law enforcement authorities;
						A secure, credible and reliable cyberspace for all users;
						Public-private partnerships;
						Minimum cybersecurity standards;
							Cyber Security Council or Security Committee assesses the implementation and progress of specified objectives;

	Establish and implement legislative framework; International leadership position;	International cooperation; Create a culture of security: inform, educate, raise awareness;		Minimum cybersecurity standards;	Academic institutions;	Improved capabilities (processes, tools and coordinating structures) Support research & development;	Regular progress reports;

5. Finland	Preparedness , resilience and adequate response to cyber threats and attacks; Safe use of information and communication in the cyber domain by citizens, businesses and authorities;
	International leadership position;
	Secure vital national functions and interests against cyber threats and attacks;
		Strategic collaboration between authorities, business and academics;
		Create a culture of security: inform, educate, raise awareness;
		Protect critical information structure;
		Counter national and international criminal activities;
		International cooperation;
		Develop standards and norms, legislation;
			Examples
			Establish/improve processes & coordinating structures;
			Tools & organisational components;
			(one moved to outputs)
				Action and emergency response plans;
				Improved capabilities (processes, tools and coordinating structures);
				Training & material supplied by security companies to individual businesses;
					Government;
					Private-Public cooperation as a guiding principle;
					Shared definition & enforcement of minimum standards between business and government;
					Private sector: enhance competitiveness of business overall:
					Information sharing;
					Business & private actors responsible for implementing and promoting secure systems;
						Creation of an internationally recognised competitive and exportable cybersecurity cluster;
						Increased resilience against cyber threats and attacks;
						A secure, credible and reliable cyberspace for all users;
						International leadership position;
							Regular review;
							Cyber Security Council or Security Committee assesses the implementation and progress of specified objectives;

6. France	International leadership position;
	Protect digital national information resources;
		Threats tracking, risk assessment and response;
		Competence and capabilities building of
			Legislative measures;
			Strategic investment to strengthen industry;
				People: professional training and education tools for citizens;
				Improved capabilities
					Government;
					Private – Public sector cooperation;
					International community.
						A cybersecurity policy consistent for all the involved agents;	Not mentioned

	Protection and efficient functioning of critical information infrastructure; Sustainability: shape an open, stable and secure cyberspace;	involved actors; Protect critical information structure; Develop standards and norms, legislation; International cooperation; Create a culture of security: inform, educate, raise awareness;		(processes, tools and coordinating structures); Improved regulatory frameworks;		Strengthened capabilities protecting critical information infrastructure, communication networks and services;	

7. Germany	Safe use of information and communication in the cyber domain by citizens, businesses and authorities;
	Promote economy reliant on digitalised industry;
	Education and training;
	Awareness raising;
		Protect critical information structure;
		Security of information and services delivered in cyberspace;
		Threats tracking, risk assessment and response;
		International cooperation;
		Counter national and international criminal activities;
		Competence and capabilities building of involved actors;
			Examples
			Guidelines and internal information on information security;
			Implementation plans;
			Incentives and funding for initiatives supporting secure systems;
				Improved regulatory frameworks;
				International cooperation;
				Minimum cybersecurity standards;
				Improved capabilities (processes, tools and coordinating structures)
				Capabilities to counter cybercrime;
					Government;
					Private sector: enhance competitiveness of business overall
					Task force IT security in industry;
					Cooperation to fight criminal activities
					Industry cooperation in fighting cybercrime;
						Maintaining and promoting economic and social prosperity;
						A secure, credible and reliable cyberspace for all users;
						Better coordination and greater competence of public and private actors involved in the information infrastructure security;
						Strengthened capabilities protecting critical information infrastructures, communication networks and services;
						Ability to counter
							Regular review;
							Cyber Security Council or Security Committee assesses the implementation and progress of specified objectives;

						online criminal activities;
						International cooperation;
						Stimulate technological capabilities and national academic initiatives in security and privacy knowledge;	

8. Hungary	Resilience against and adequate response to cyber threats and attacks;
	Protect digital national information resources;
	Quality of IT and communication products and security standards;
	Education and training;
	Awareness raising;
	Secure cyberspace with respect for fundamental rights and values.
	Invest in ICT and innovation for cybersecurity and privacy;
		Strategic collaboration between authorities, business and academics;
		International cooperation;
		Create a culture of security: inform, educate, raise awareness;
		Research, development and innovation;
			Establish/improve processes & coordinating structures;
			Tools & organisational components;
			Legislative measures;
			Participation in international and regional cooperation;
			Support research & development;
			Incentives and funding for initiatives supporting secure systems;
				Support research & development;
				Improved regulatory frameworks;
				People: professional training and education tools for citizens;
				Improved capabilities (processes, tools and coordinating structures)
					Government;
					Academic institutions;
					Private – Public sector cooperation;
						A cyberspace optimal for societal development;
						Development of effective and innovative ebusiness solutions;
						Innovative public services;
							Not mentioned;

9. Italy	Preparedness, resilience and adequate response to	Competence and capabilities building of	Examples
			Tools & organisational components;
				Public-private partnerships;
				Improved capabilities (processes,
					Government;
					Private – Public sector cooperation;
						Strengthened capabilities protecting critical information	Promote the use of questionnaires among stakeholders

	cyber threats and attacks; Establish and clarify roles in collaboration between the public and private sector; Endorse and respect certain rules of behaviour in the digital arena consistent with national values;	involved actors; Protect critical information structure; Strategic collaboration between authorities, business and academics; Create a culture of security: inform, educate, raise awareness; Counter national and international criminal activities; International cooperation	Introduce cybersecurity in curricula of education system; Participation in international and regional cooperation;	tools and coordinating structures); Minimum cybersecurity standards;	Ministries responsible for implementing sector specific elements of the NCSS;	infrastructure, communication networks and services; Stimulate technological capabilities and national academic initiatives in security and privacy knowledge; A culture of security among citizens and institutions; Ability to counter online criminal activities; International cooperation;	to understand their training needs; Enhance and evaluate education and on the job training programmes; Presidency of the Council of Ministers drafts a text on the activities in relation to cyberspace protection Annexed to the Annual Report to the Parliament on national security strategy and policies

10. Latvia	Establish and implement legislative framework
	Preparedness, resilience and adequate response to cyber threats and attacks
	Protection and efficient functioning of critical information infrastructure
		Counter national and international criminal activities;
		Create a culture of security: inform, educate, raise awareness;
		Develop standards and norms, legislation;
		International cooperation;
		Protect critical information infrastructure;
		Research, development
			Establish/improve processes & coordinating structures;
			Guidelines and internal information on information security;
			Implementation plans;
			Legislative measures;
			Participation in international and regional cooperation
				Improved capabilities (processes, tools and coordinating structures)
				Improved regulatory frameworks;
				International cooperation;
				People: professional training and self-education tools for citizens
				Support research & development
					Industry involvement for education and awareness;
					Academic institutions;
					Government
					Incident response mechanisms;
					Private-Public cooperation as a guiding principle;
						Ensure confidentiality, integrity and accessibility of electronic information and services;
						Reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society;
						Strengthened capabilities protecting critical information infrastructures, communicati
							Regular review

		and innovation; Threats tracking, risk assessment and response				on networks and services;	

11. Lithuania	Protect digital national information resources;
	Protection and efficient functioning of critical information infrastructure;
	Safe use of information and communication in the cyber domain by citizens, businesses and authorities;
	Establish and implement legislative framework;
	Resilience against and adequate response to cyber threats and attacks;
	Citizens' perception of sufficient data protection;
		Strategic collaboration between authorities, business and academics;
		Develop standards and norms, legislation;
		Protect critical information structure;
		International cooperation;
		Create a culture of security: inform, educate, raise awareness;
		Security of information and services delivered in cyberspace;
			Legislative measures;
			Tools & organisational components;
				Improved capabilities (processes, tools and coordinating structures);
				People: professional training and education tools for citizens;
					Government;
					Ministries responsible for implementing sector specific elements of the NCSS;
					Law enforcement authorities;
						Ensure confidentiality, integrity and accessibility of electronic information and services;
						Strengthened capabilities protecting critical information infrastructure, communication networks and services;
						Protection of personal data and privacy;
						A secure, credible and reliable cyberspace for all users;
							Participating institutions provide a status update;
							Regular review;
							Regular progress reports;

12. Luxembourg	Resilience against and adequate response to cyber threats and attacks;
	Protection and efficient functioning of critical
		Protect critical information structure;
		Security of information and services delivered in cyberspace;
			Examples
			Tools & organisational components;
			Establish/improve processes &
				Action and emergency response plans;
				Improved capabilities (processes, tools and coordinating structures);
					Industry involvement for education and awareness;
					Academic institutions;
					Government;
						Foster a growing business sector and expanding digital economy;
						Greater confidence in safety of
							Regular review;

	information infrastructure; Safe use of information and communication in the cyber domain by citizens, businesses and authorities; Promote economy reliant on digitalised industry;	Develop standards and norms, legislation; International cooperation; Strategic collaboration between authorities, business and academics; Create a culture of security: inform, educate, raise awareness;	coordinating structures;			using cyberspace by citizens, businesses, public sector; Reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society;	

13. The Netherlands	Resilience against and adequate response to cyber threats and attacks;
	Tackle cybercrime;
	Invest in ICT and innovation for cybersecurity and privacy;
	Establish and clarify roles in collaboration between the public and private sector involved in cybersecurity;
	Education and training;
	Awareness raising;
	Secure vital national functions and interests against cyber threats and attacks;
		Strategic collaboration between authorities, business and academics;
		International cooperation;
		Competence and capabilities building of involved actors;
		Threats tracking, risk assessment and response;
			Legislative measures;
			Introduce cybersecurity in curricula of education system;
				Improved capabilities (processes, tools and coordinating structures);
				Public-private partnerships;
				Minimum cybersecurity standards;
				People: professional training and self-education tools for citizens;
					Government;
					Private – Public sector cooperation;
					Private sector, government and citizens are each responsible for securing cyberspace;
						Stimulate technological capabilities and national academic initiatives in security and privacy knowledge;
						International cooperation;
						A balance between privacy, fundamental rights and liberties, free access to information with the need to guarantee security and better cybersecurity practices and procedures;
						Allow citizens and businesses to safely handle their affairs with the government;
							Regular progress reports;

14. Poland	Quality of IT and communication products and security standards;
	Preparedness, resilience and adequate response to cyber threats and attacks;
	Establish and clarify roles in collaboration between the public and private sector involved in cybersecurity;
	Education and training;
	Awareness raising;
		Threats tracking, risk assessment and response;
		Security of services delivered in cyberspace;
		Develop standards and norms, legislation;
		Strategic collaboration between authorities, business and academics;
		Create a culture of security: inform, educate, raise awareness;
			Legislative measures;
			Tools & organisational components;
				Annual reports;
				Improved capabilities (processes, tools and coordinating structures);
				Action and emergency response plans;
				People: professional training and education tools for citizens;
					Government;
					Ministries responsible for implementing sector specific elements of the NCSS;
					Incident response mechanisms
						Enhanced national security;
						A secure, credible and reliable cyberspace for all users;
						Increased resilience against cyber threats and attacks;
						A cybersecurity policy consistent for all the involved agents;
						Lower effectiveness of internet terrorism and lower costs of countering internet terrorism;
						Better coordination and greater competence of public and private actors involved in the information infrastructure security;
						Greater confidence in safety of using cyberspace by citizens, businesses, public sector;
						Awareness and a culture of security among
							Specific measures to evaluate the effectiveness of projects;
							Regular progress reports;

						citizens and institutions;	

15. Romania	Establish and implement legislative framework;
	Protection and efficient functioning of critical information infrastructure;
	Preparedness, resilience and adequate response to cyber threats and attacks;
	Quality of IT and communication products and security standards;
	Establish and clarify roles in collaboration between the public and private sector;
	Education and training;
	Awareness raising;
		Competence and capabilities building of involved actors;
		International cooperation;
		Counter national and international criminal activities;
		Develop standards and norms, legislation;
		Create a culture of security: inform, educate, raise awareness;
			Legislative measures;
			Implementation plans;
			Participation in international and regional cooperation;
				Warning & reporting systems;
				Improved capabilities (processes, tools and coordinating structures);
				Public-private partnerships;
				People: professional training and education tools for citizens;
					Government;
					Private – Public sector cooperation;
					Private sector: facilitating local economy security providers
					ICT service providers and network operators;
						Enhanced national security;
						A secure, credible and reliable cyberspace for all users;
						Increased resilience against cyberthreats and attacks;
						Greater confidence in safety of using cyberspace by citizens, businesses, public sector;
						Foster a growing business sector and expanding digital economy;
						A cyberspace optimal for societal development;
							Regular review;

16. Slovakia	Preparedness, resilience and adequate response to cyberthreats and attacks;
	Quality of IT and communication products and security standards;
	Sustainability: shape an
		Develop standards and norms, legislation;
		Create a culture of security: inform, educate, raise awareness;
		Security of information and services
			Legislative measures;
			Introduce cybersecurity in curricula of education system;
			Implementation plans;
				Improved capabilities (processes, tools and coordinating structures);
				Action and emergency response plans;
				Support research & development;
					Government;
					Private sector: facilitating local economy security providers
					Funding private sector cybersecurity initiatives;
						A secure, credible and reliable cyberspace for all users;
						A cybersecurity policy consistent for all the involved agents;
						People: professional
							Regular progress reports;

	open, stable and secure cyberspace;	delivered in cyberspace; Protect critical information structure; Strategic collaboration between authorities, business and academics; International cooperation; Competence and capabilities building of involved actors;		A balance between guaranteeing civil & human rights and cybersecurity in legislation;		training and self-education tools for citizens; Minimum cybersecurity standards;	

17. Spain	Safe use of information and communication in the cyber domain by citizens, businesses and authorities;
	Quality of IT and communication products and security standards;
	Protection and efficient functioning of critical information infrastructure;
	Secure, safe place to do business;
	Preparedness, resilience and adequate response to cyber threats and attacks;
		Threats tracking, risk assessment and response;
		Protect critical information structure;
		Counter national and international criminal activities;
		Create a culture of security: inform, educate, raise awareness;
		Research, development and innovation;
		International cooperation;
			Examples
			Participation in international and regional cooperation;
			Tools & organisational components;
			Incentives and funding for initiatives supporting secure systems;
				Examples
				International cooperation;
				Support research & development;
					Government;
					Private-Public cooperation as a guiding principle;
					International community;
					Individual citizens.
						Greater confidence in safety of using cyberspace by citizens, businesses, public sector;
						Reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society;
						Increased resilience against cyberthreats and attacks;
						Strengthened capabilities protecting critical information infrastructures, communicati
							Regular review;

	Tackle cybercrime;
	Education and training;
	Awareness raising;
						on networks and services;
						Better coordination and greater competence of public and private actors involved in the information infrastructure security;
						Ability to counter online criminal activities;
						Awareness and a culture of security among citizens and institutions;	

18. United Kingdom	International leadership position; Secure, safe place to do business; Tackle cybercrime; Resilience against and adequate response to cyber threats and attacks; Safe use of information and communication in the cyber domain by citizens, businesses and authorities; Sustainability: shape an open, stable	Protect critical information structure; Threats tracking, risk assessment and response; Strategic collaboration between authorities, business and academics; International cooperation; Counter national and international criminal activities; Develop standards and norms, legislation; Competence and	Legislative measures; Increasing law enforcement and judiciary capabilities; Incentives and funding for initiatives supporting secure systems;	Improved capabilities (processes, tools and coordinating structures); Capabilities to counter cybercrime; Support research & development;	Government; Private sector: enhance competitiveness of business overall Private sector owning infrastructures under threat requires business-driven solutions; private sector, government and citizens are each responsible for securing cyberspace; Intelligence agencies;	Enhanced national security; Foster a growing business sector and expanding digital economy; Maintaining and promoting economic and social prosperity; A cyberspace optimal for societal development;	Regular progress reports;

	and secure cyberspace;	capabilities building of involved actors; Create a culture of security: inform, educate, raise awareness;			Ministries responsible for implementing sector specific elements of the NCSS;		