

## Annex A: Mapping of cybersecurity strategies (September 2014)

| Country    | Objectives   | Focal areas of action  | Inputs¹  | Outputs <sup>2</sup>  | Stakeholder involvement  | Outcomes   | Review/evaluati on 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/imp rove processes & coordinating structures; | Examples Annual reports; Minimum cybersecurity standards; Improved regulatory frameworks;   | Government; Private-Public cooperation as a guiding principle; Private sector: enhance competitiven ess of business overall → Strengthenin g support and tools for SMEs; | Increased resilience against cyberthreats and attacks; Strengthened capabilities protecting critical information infrastructure , communicati on 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<br>standards and<br>norms,<br>legislation;<br>Threats<br>tracking, risk<br>assessment<br>and response;<br>Security of<br>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<br>evaluation of<br>security<br>policies;               |

<sup>1</sup> 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.

 $<sup>^2</sup>$  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<br>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 & organisationa   components; Establish/imp rove 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<br>and efficient<br>functioning of<br>critical<br>information<br>infrastructure<br>;<br>Education<br>and training;<br>Awareness<br>raising; | Develop standards and norms, legislation; Competence and capabilities building of involved actors;  | Legislative measures; Implementati on 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 implementati on 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<br>cybersecurity<br>standards;  | Academic<br>institutions;   | Improved capabilities (processes, tools and coordinating structures)  Support research & development;   | Regular<br>progress<br>reports;   |
|------------|--|---|---|---|---|---|---|
| 5. Finland | Preparedness, resilience and adequate response to cyber threats and attacks; Safe use of information and communicati on 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 competitiven ess of business overall:  Information sharing; Business & private actors responsible for implementing and promoting secure systems; | Creation of an internationall y 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 implementati on 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<br>measures;<br>Strategic<br>investment to<br>strengthen<br>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<br>mentioned  |



|            | T  | T   | T  | T  |  |   |   |
|------------|--|---|--|--|--|---|---|
|            | 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 , communicati on networks and services;  |   |
| 7. Germany | Safe use of information and communicati on 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; Implementati on 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 competitiven ess 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 infrastructure s, communicati on networks and services;  Ability to counter | Regular review; Cyber Security Council or Security Committee assesses the implementati on 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 communicati on 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/imp rove processes & coordinating structures;  Tools & organisationa   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<br>, resilience<br>and adequate<br>response to   | Competence<br>and<br>capabilities<br>building of  | Examples  Tools & organisationa   components;   | Public-private partnerships; Improved capabilities (processes,   | Government; Private – Public sector cooperation;                        | Strengthened capabilities protecting critical information  | Promote the use of questionnaire s among stakeholders |



|            | ا جاء العامانية   | incontrol of   |   | Anala !  |  | :£   | And the second second second   |
|------------|---|--|---|--|--|--|--|
|            | 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 , communicati on 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/imp rove processes & coordinating structures; Guidelines and internal information on information security; Implementati on 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 confidentialit y, 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 infrastructure s, communicati | Regular<br>review  |



| Lithuania nat inforces  Pro ano fur crit info info;  Saf info ano cor on cyb by bus and aut  Est impleg fra                                   | mmunicati in the ber domain citizens, sinesses  | and innovation; Threats tracking, risk assessment and response 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 | Legislative measures; Tools & organisationa   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 confidentialit y, integrity and accessibility of electronic information and services; Strengthened capabilities protecting critical information infrastructure , communicati on 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. Luxembou rg Resagade ress cyk and dat pro aga ade res cyk and Pro | silience ainst and equate sponse to ber threats d attacks; cizens' rception of fficient |   | Examples Tools & organisationa   components; Establish/improve | Action and emergency response plans; Improved capabilities (processes, tools and  | Industry involvement for education and awareness; Academic institutions;   |  | Regular<br>review;  |
| and<br>fur  |   |   | rove<br>processes &  |   | Government;  | Greater<br>confidence in<br>safety of  |   |



|                      | information infrastructure ;  Safe use of information and communicati on 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<br>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 Netherlan ds | 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<br>progress<br>reports; |



| 14. Poland | Quality of IT and communicati on 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 & organisationa   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 | Specific measures to evaluate the effectiveness of projects; Regular progress reports; |
|------------|---|--|---|--|--|---|--|
|            |   |  |   |  |  | lower costs of countering   |  |
|            |   |  |   |  |  | cyberspace by citizens, businesses, public sector; Awareness and a culture of security among  |  |



|                 |   |   |  |   |   | citizens and institutions;  |                                 |
|-----------------|---|---|--|---|---|---|---------------------------------|
| 15.<br>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 communicati on 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; Implementati on 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.<br>Slovakia | Preparedness, resilience and adequate response to cyberthreats and attacks; Quality of IT and communicati on 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; Implementati on 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<br>progress<br>reports; |



| 17. Spain | and secure cyberspace;  Safe use of information and  | cyberspace; Protect critical information structure; Strategic collaboration between authorities, business and academics; International cooperation; Competence and capabilities building of involved actors; Threats tracking, risk assessment | Examples Participation in   | between guaranteeing civil & human rights and cybersecurity in legislation;  Examples International cooperation; | Government; Private-Public cooperation                                | self- education tools for citizens; Minimum cybersecurity standards;  Greater confidence in safety of   | Regular review; |
|-----------|--|--|---|--|---|---|-----------------|
|           | communicati on in the cyber domain by citizens, businesses and authorities;  Quality of IT and communicati on 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; | 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; | international and regional cooperation;  Tools & organisationa I components;  Incentives and funding for initiatives supporting secure systems; | Support research & development;  | as a guiding principle; International community; Individual citizens. | 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 infrastructure s, communicati |                 |



| cybercrime; Education and training; Awareness raising; Awareness raising;  Awareness raising;  Protect critical increasing law critical pace to do business; Secure, safe place to do business; Tackle aplace to do business; Tackle cybercrime; Resilience against and adequate response to cybercrime; Strategic collaboration and academics; International cooperation; Counter national and international cooperation; Counter cybercrime; Sustemation in the cyber domain by citizens, businesses and authorities; Sustainability: Counter national and international cooperation; Counter and criminal by citizens, businesses and authorities; Sustainability: Liejslation; shape an onen stable increasional cooperation; competence of public and provate competence of public and provate activity; Ability to counter continer activities; awareness and a culture of security; Ability to counter continer activities; business and activities; busin |         | Tackle                                 |   |             |             |                          | on networks   |          |
|--|---------|--|---|-------------|-------------|--------------------------|---------------|----------|
| tautation and training:  Awareness raising:  Awareness raising:  Protect response to business, Tackle place to do business, and attacks;  Safe use of information and academics, thereafted to the top  |         |  |   |             |             |                          | and services; |          |
| Awareness raising;  Awareness raising;  It. 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 threats and attacks;  Safe use of information and communication in the cyber domain by citizens, businesses and authorities;  Sustainability: Shape an neen stable competence of public and private actors involved in the information infrastructure security;  Ability to counter of security among citizens and institutions;  Improved capabilities (processes, tools and conditating structures); cols and enforcement tracking, risk and response to cyber domain by citizens, business and attacks;  Safe use of information and communication in the cyber domain by citizens, businesses and authorities;  Sustainability: Shape an neen stable competence of public and private actors into the information infrastructure security;  Awareness and a culture deapabilities (processes, tools and laudiciary structures); colaboration business and disudiciary structures); colaboration business and attacks;  Safe use of information and communication in the cyber domain by citizens, businesses and authorities; businesses and authorities; businesses and authorities; businesses and authorities; collaboration businesses and authorities; collaboration businesses and authorities; collaboration business and authorities; collaboration businesses and authorities; considerational consperation; constitutes and response to cyber domain by citizens, businesses and authorities; considerational consperation; communication in the cyber domain by citizens, businesses and authorities; considerational consperation; constitutes; considerational consperation; constitutes, co |         | Education                              |   |             |             |                          |               |          |
| 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 authorittes; Sustainability; Shape an new stable part of the communication in the cyber domain by citizens, Susinesses and authorittes; Sustainability; Shape an new stable part of the competence against and authorities; Sustainability; Shape an new stable part of the competence and authorities; Sustainability; Shape an new stable part of the competence and standards and authorities; Sustainability; Shape an new stable part of the competence and standards and authorities; Sustainability; Shape an new stable part of the competence are also and authorities; Sustainability; Shape an new stable part of the competence are also and authorities; Susporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Sustainability; Shape an new stable part of the competitive supporting authorities; Susporting aut |         | and training;                          |   |             |             |                          |               |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; Tackle cybercrine; Resilience against and adequate response to cyber threats and datacks; Safe use of information and communicati on in the cyber domain by citizens, Susinesses and authorities; Susinesses and authorities; Sustainability: Shape an noen stable competence should be supported authorities; Sustainability: Shape an noen stable competence should be supported authorities; Sustainability: Shape an noen stable competence should be supported authorities; Sustainability: Shape an noen stable competence should be supported authorities; Sustainability: Shape an noen stable competence should be supported authorities; Sustainability: Shape an noen stable competence should be supported and competence should be supported and competence should be supported and competitive supporting authorities; Sustainability: Shape an noen stable competence should be supported and competitive shape an noen stable competence should be supported and competitive shape an noen stable competitive shape and noen stable competitive shape and noen stable shape shape and noen stable shape  |         |  |   |             |             |                          | •             |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; Tackle cybercrime; and assessment and adequate response to cyber threats and attacks; Safe use of information and communicati on in the expression sinces and academics; International communicati on in the cyber domain by citizens, businesses and authorities; Sustianisability. Sustainability shape an nonen stable competence are sustainability. Sustainability shape an nonen stable competence are sustainability. Competence are sustainab |         | raising,                               |   |             |             |                          |               |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; Information structure; Trackle cybercrime; Resillence against and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens business; Safe use of information and communicati on in the cyber domain by citizens business and authorities, Susiness and authorities, Susiness and authorities, business and attacks; Sustainability; Sape an nonen stable competence supporting activities; Develop standards and norms, Sustainability; Sape an nonen stable competence supporting activities; Develop standards and norms, Sustainability; Sape an nonen stable competence supporting activities; Develop standards and norms, Sustainability; Sape an nonen stable competence supporting activations; and activatives; Competence supporting activatives; Capabilities to counter cybercrime; Support supporting succure systems; and structures; Capabilities to counter cybercrime; Support supporting succure systems; activatives and funding of infigrative security; Adaility to counter criminal activities; Capabilities (processes, tools and sum coordinations structures); Capabilities to counter cybercrime; Support supporting supporting supporting succure systems; activate systems; activates; activ |         |  |   |             |             |                          |               |          |
| 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 of the cyber and authorities; Sustainability; shape an open stable of the cyber competence of the cyber domain and the cyber domain by citizens, businesses and authorities; Sustainability; shape an open stable of the cyber cyb |         |  |   |             |             |                          |               |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; Tackle cybercrime; Resilience against and adequate response to cyber threats and attack; Safe use of information and communicati on in the cyber domain by citizens, businesses and attack; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an one notatible.  |         |  |   |             |             |                          |               |          |
| 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 communicati on in the cyber domain by citizens, businesses and authorities; Sustainability; shape an one national and norms, legislatior; Sustainability; shape an one national and norms, legislation; Competence substances and activities; Legislative measures; capabilities and response; cortical measures; capabilities and institutions; and a culture of security among citizens and institutions; and a culture of security among citizens and institutions; and a culture of security among citizens and institutions; and a culture of security among citizens and institutions; and judiciary capabilities of cap |         |  |   |             |             |                          | •             |          |
| 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 communicati on in the cyber domain by citizes, businesses and authorities; Sustainability; shape an open stable.  Develop standards and norms, legislatior; Sustainability; shape an open stable.  |         |  |   |             |             |                          | =             |          |
| 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 communicati on in the cyber domain by citizens, businesses and adards and numb, by citizens, businesses and authorities; Sustainability: shape an open stable competence are supported and propersion and compens to cyber threats and authorities; Sustainability: shape an open stable competence are supported and propersion and compension an |         |  |   |             |             |                          |               |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; tracking, risk adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an open stale competence in the cyber of man and authorities; Sustainability: shape an open stale competence in the cyber of man and authorities; Sustainability: shape an open stale competence in the cyber of man and authorities; Sustainability: shape an open stale competence in the cyber of standards and authorities; Sustainability: shape an open stale competence information and instructors; and instructors; capabilities (processes, tools and capa |         |  |   |             |             |                          |               |          |
| 18. United Kingdom  International leadership position; Secure, safe place to do business; tracking, risk experiment and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an open staled sent and nor service and tracking and norm stale learned and tracks; Sustainability: shape an open staled service and content and citizens and institutions;  Improved capabilities (processes, tools and capabilities; capabilities; capabilities; capabilities; and information and content end for initiatives supporting activents and stacks; sustainability: shape an open stale learned and tracks and stacks; sustainability: shape an open stale learned and stacks and stacks; sustainability: shape an open stale learned and stacks; sustainability: shape an open st |         |  |   |             |             |                          |               |          |
| 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 communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an open stable and none in table of the communication of the cyber domain by citizens, businesses and authorities; Sustainability: shape an open stable and response to communication of the cyber domain by citizens, businesses and authorities; Sustainability: shape an open stable and none in table communication.  International critical measures; (processes, tools and coordinating structures); capabilities (processes, tools and coordinating structures); capabilities to counter counter cybercrime; Supporting secure systems;  Capabilities to counter counter cybercrime; Supporting infrastructure sunder threat requires business divities; businesses and authorities; Sustainability: shape an open stable communication.  Counter counter cybercrime; Supporting and promoting economic and social prosperity; A cyberspace; Intellegence and coordinating structures); Capabilities to counter cybercrime; Supporting infrastructure sunder threat requires businesses driven solutions; private sector solutions; private sector, government and citizens are each for societal development; solutions; private sector, government and citizens are each for societal development; solutions; private sector, government and citizens are each for securing cyberspace; Intellegence agencies are each for securing cyberspace; Intellegence agencies are government and citizens are each for securing cyberspace; Intellegence agencies are government and citizens are government and citizens are each for societal development; security and private sector. Solutions are each for societal development; security |         |  |   |             |             |                          |               |          |
| 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 communicati on in the cyber domain by citizens, businesss businesss and authorities; businesss businesss businesses and authorities; business businesses and authorities; Sustainability: shape an open stable of the place to do business and tracking, risk assessment and judiciary capabilities; condinating structures); Capabilities to counter cybercrime; Support research & development; Support sector, government and citizens and tracks; Sustainability: shape an open stable of the place to do business afable of the place to do business afable of the place to do business; and tracking, risk assessment and judiciary capabilities; capabilities to counter cybercrime; Support secure capabilities to counter capabilities to counter cybercrime; Support sevence development; Support sector, government and citizens are each responsible for securing cyberspace; Intelligence agencies:   |         |  |   |             |             |                          | among         |          |
| 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 communicati on in the cyber domain by citizens, businesses and authorities; Susinesses and authorities; Sustainability: shape an one postate in the cyber chartest and authorities; Sustainability: shape an one postate in the cyber chartest and and and and authorities; Sustainability: shape an one postate in the cyber chartest and and and and and and and properties and authorities; Sustainability: shape an one postate in the cyber chartest and attacks; Sustainability: shape an one postate in the cyber chartest and attacks and authorities; Sustainability: shape an one postate in the cyber chartest and attacks and authorities; Sustainability: shape an one postate in the cyber chartest and attacks; Sustainability: shape an one postate in the cyber chartest and attacks; Sustainability: shape an one postate in the cyber chartest and attacks; Sustainability: shape an one postate in the cyber chartest and attacks; Sustainability: shape an one postate in the cyber chartest and authorities; shape an one postate in the cyber chartest and judiciary capabilities to counter cyberdities to counter cyberorime; Susporting and judiciary capabilities to counter cyberorime; Support research so development; Support researc |         |  |   |             |             |                          |               |          |
| 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 communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an one position; Secure, safe place to do business; Cybercrime; Resilience against and adequate response to cyber domain by citizens, businesses and authorities; Sustainability: shape an one position; Secure, safe place to do business it racking, risk assessment and response; Tackle cybercrime; Resilience against and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an one position; Sustainability: shape an one position; Secure, safe place to do business sectors and funding for initiatives and judiciary capabilities; locate and funding for initiatives supporting authorities; sunder threat requires business- driven solutions; private sector, government and citizens are each responsible for securing cyberspace; located and judiciary capabilities; sunder threat requires business- driven and citizens are each responsible for securing cyberspace; located threat sector: enhance compensitives doubtiness obusiness obusiness sector and coordinating structures; Support development;  Supporting advendence overall expanding digital evenomy; Maintaining and promoting sector owning business overall expanding digital evenomy; Supporting and funding infrastructures pusiness-driven and citizens are each responsible for securing cyberspace; located threat sectors owning business of the private sector owning the sector owning threat counter cybercime; Supporting and funding for social development; sector owning threat counter cybercime; Supporting and funding for social development; sector owning threat  |         | International                          | Protect                                 | Legislative | Improved    | Government;              |               | Regular  |
| Secure, safe place to do business; Tackle cybercrime; Resilience against and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: Sustainab | Kingaom | -                                      |   | measures;   | · ·         | Private                  |               | progress |
| place to do business;  Tackle cybercrime; Resilience against and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape a an open stable.  Different sassessment and judiciary capabilities; assessment and judiciary capabilities; assessment and judiciary capabilities; capabilities; and funding for initiatives supporting supporting such research & development;  Private sector and expanding digital economy;  Maintaining and promoting exponding digital economy;  Support research & development;  Support research & development;  Support research & development;  Support research & development;  Counter national and international criminal activities;  Develop standards and norms, legislation;  Competence  Private sector owning infrastructure, solutions;  Develop standards and norms, legislation;  Develop standards and norms, legislation;  Competence  |         |  |   | _           | **          |                          | •             | reports; |
| Tackle cybercrime;  Resilience against and adequate response to cyber threats and attacks;  Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: shape an open stable  Dusiness;  Trackle capabilities; capabilities; collaboration and response; lincentives and funding for initiatives supporting secure systems; and different communicati on in the cyber domain authorities; businesses and authorities; collaboration between academics; linternational cooperation; competence lineatives and funding for initiatives supporting secure supporting support research & development; support research & development; support research & development; sunder threat requires business driven solutions; optimal for social prosperity; intelligence agencies:  Support research & development; support research & development; supporting sunder threat requires business driven solutions; optimal for social prosperity; intelligence and outhorities; optimal for societal development;   |         | · ·                                    | Threats                                 |             | _           |                          |               |          |
| rackle cybercrime; cybercrime; Strategic collaboration against and adequate response to cyber threats and attacks; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; businesses and authorities; businesses and authorities; Sustainability: Sustainability: Strategic collaboration between authorities, business and academics; International cooperation; Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: legislation; Competence Incentives and funding for initiatives supporting secure supporting  |         | business;                              | _                                       |             |             |                          |               |          |
| Resilience against and adequate response to cyber threats and attacks;  Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities;  Support research & development;  Sustainsbility:  Support research & development;  Support requires positions and promoting economical social prosperity;  Support requires positions.  In |         |  |   | -           |             |                          |               |          |
| against and adequate response to cyber threats and attacks;  Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities;  Sustainability: Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Sustainability: Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities; Competence  Competence  Competence  Competence  Collaboration between supporting supporting secure systems; Susport research & development;  Frivate sector owning infrastructures sunder threat requires business-driven solutions;  Private sector owning infrastructures sunder threat requires business-driven solutions;  A cyberspace optimal for societal development;  A cyberspace optimal for societal development;  Susport research & development;  Support research & development;  A cyberspace optimal for societal development;  Support research & development;   |         | -                                      | Strategic                               |             | cybercrime; |                          |               |          |
| adequate response to cyber threats and attacks;  Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities;  Sustainability: shape an open stable   |         | against and                            |   |             |             |                          |               |          |
| cyber threats and attacks;  Safe use of information and communicati on in the cyber domain by citizens, businesses and authorities;  Sustainability: shape an open stable of information and academics;  International academics; International cooperation;  Counter national and international criminal activities; business and academics; International cooperation; Counter national and international criminal activities; businesses and authorities; Counter national and international criminal activities; businesses and authorities; Competence systems;  s under threat requires business-driven solutions; A cyberspace optimal for societal development;  by citizens, businesses and academics; International cooperation; Counter national and international criminal activities; business-driven solutions; A cyberspace optimal for societal development;  by citizens, businesses and academics; International cooperation; International cooperation; Soutions; A cyberspace optimal for societal development;  International cooperation; International cooperati |         |  | authorities,                            | secure      |             | _                        | and           |          |
| Safe use of information and cooperation;  Counter national and international cyber domain by citizens, businesses and authorities;  Sustainability: shape an open stable   |         | cyber threats                          |   | systems;    |             | s under threat           |               |          |
| Safe use of information and cooperation;  Counter national and international criminal by citizens, businesses and authorities;  Sustainability: shape an open stable cooperation;  Cooperation;  Counter national and international criminal and international criminal activities;  Develop standards and norms,  Legislation;  Cooperation;  driven solutions;  A cyberspace optimal for societal development;  A cyberspace optimal for societal development;  A cyberspace optimal for societal development;  Intelligence agencies:   |         | ·                                      |   |             |             | •                        | social        |          |
| and communicati on in the cyber domain by citizens, businesses and authorities;  Sustainability: shape an open stable on in the communicati on in the cyber domain by citizens, businesses and authorities;  Counter national and international criminal activities;  Develop standards and norms, legislation;  Competence optimal for societal development;  A cyberspace optimal for societal development;  Intelligence agencies:  |         |  |   |             |             | driven                   |               |          |
| communication in and international criminal by citizens, businesses and authorities;  Sustainability: shape an open stable on in the cyber domain by citizens, activities;  Develop standards and norms,  Sustainability: shape an open stable on the cyber domain criminal international criminal societal development;  Societal development;  societal development;  Intelligence agencies:   |         | and                                    |   |             |             |                          |               |          |
| cyber domain by citizens, businesses and authorities; Sustainability: shape an open stable cyber domain by citizens activities;  Competence government and citizens are each responsible for securing cyberspace;  Intelligence agencies:  |         |  |   |             |             |                          | societal      |          |
| businesses and authorities;  Sustainability: shape an open stable  Develop standards and norms, legislation;  Competence  are each responsible for securing cyberspace;  Intelligence agencies:  |         | cyber domain                           | criminal                                |             |             | government               | development;  |          |
| and standards and norms,  Sustainability: legislation; legislation; legislation; Competence Competence agencies:   |         | -                                      |   |             |             |                          |               |          |
| authorities;  Sustainability: legislation; shape an open stable  Competence  authorities; norms, cyberspace; Intelligence agencies:  |         | businesses                             | D 1 -                                   |             |             |                          |               |          |
| shape an competence Competence agencies  |         | and                                    | •                                       |             |             | -                        |               |          |
| onen stable Competence agencies  |         | and<br>authorities;                    | standards and norms,                    |             |             | for securing             |               |          |
| and agenties)  |         | and<br>authorities;<br>Sustainability: | standards and<br>norms,<br>legislation; |             |             | for securing cyberspace; |               |          |



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