ASSESSING NATIONAL CYBERSECURITY STRATEGIES FROM A HUMAN RIGHTS PERSPECTIVE

GLOBAL PARTNERS DIGITAL

Contents

Foreword

Cybersecurity and human rights are closely linked. Appropriate measures taken to enhance cybersecurity have the clear potential to strengthen the protection of individuals' human rights, and to mitigate the risk of breaches resulting from cyber attacks, particularly when it comes to the rights to privacy and freedom of expression. However, measures taken in the name of cybersecurity can also pose risks to human rights.

National Cybersecurity Strategies (NCSS) are an increasingly popular instrument used by states to respond to cyber threats. Despite this, there is little guidance on how to ensure that an NCSS also supports the respect, protection and promotion of human rights. The aim of this tool is to fill that gap, by looking at the critical components of an NCSS, identifying how the substance of those components can and should respect, protect and promote human rights, and providing examples of good practice seen in existing NCSSs.

This tool can be used to help inform the development of an NCSS. It can also be used to assess the text of an NCSS (or draft NCSS).

01

The approach of this tool

There is no single standardised structure for an NCSS, nor an exhaustive list of the elements that one should contain. There is, however, considerable overlap in the suggested structures and elements contained within key guidance on the development of NCSSs.

The components of an NCSS

In developing the framework set out in this guide we have reviewed six of the most widely used guidance documents that have been published.

These are:

- *Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity* (International Telecommunication Union (ITU), and others, 2021;
- *National Cybersecurity Strategy Guide* (ITU, 2012)
- *NCSS Good Practice Guide* (ENISA, 2016);
- *Approach for Developing National Cybersecurity Strategies* (CTO, 2015);
- *Cybersecurity Capacity Maturity Model for Nations* (GCCS 2016) and
- *Developing a National Cybersecurity Strategy* (Microsoft, 2013)

Based on this review, , we mapped out six core components which should be used in developing an NCSS.

Those six components are, in summary:

1. **Framing, vision, objectives and definitions**: The government's overall approach towards (or vision of) cybersecurity, as well as aims objectives, principles and definitions of key terms.
2. **Roles and responsibilities**: the roles and responsibilities of different actors in developing and implementing an NCSS.
3. **Cyber resilience**: the actions that the government will take to protect infrastructure, networks, systems, information and users from cyber attacks and cyber threats—e.g. measures to protect critical national infrastructure, proactive measures by Computer Incident Response Teams (CIRTs), cybersecurity exercises, research and development, and capacity building.
4. **Cyber incident response**: the actions that the government will take when a cyber attack occurs—e.g. contingency plans, reactive measures by CIRTs, and resourcing to law enforcement agencies, and supporting affected businesses and individuals.
5. **Cybercrime**: how the government will tackle cybercrime. This primarily involves developing and implementing cybercrime legislation, and supporting its enforcement by law enforcement agencies.
6. **International cooperation**: how the government will work with other governments, as well as international and regional organisations, on cybersecurity issues. This usually involves collaboration to deal with shared threats, but may also include promoting the government's particular values and foreign policy priorities at international and regional forums where cybersecurity is discussed.

While all components have links to human rights, not every section within each component will do; some parts of an NCSS will be hugely important from a human rights perspective, others will have little or no relevance (particularly purely administrative arrangements such as how government departments will coordinate internally). As such, the recommendations set out below do not touch upon all aspects of a state's NCSS, but focus instead on those with the clearest and strongest links to human rights.

Human rights analysis and good practice examples

The methodology used to undertake the analysis is based on international human rights law, primarily the International Covenant on Civil and Political Rights (ICCPR) as well as its elaboration and interpretation by the UN Treaty Bodies.

As is well-established under international human rights law, any measure which interferes with either the right to privacy or the right to freedom of expression will amount to a breach of those rights unless it can be justified.

In order to be justified, any restriction must meet a three-part test:

1. there is a clear legal basis for the restriction
2. it pursues a legitimate aim
3. it is necessary and proportionate to achieve that aim.

As well as setting out criteria for how an NCSS can respect, protect and promote human rights, the Annex of this tool also includes a number of examples of existing good practice for each of the criteria.

In determining which examples to include, a review of approximately 100 existing NCSSs was undertaken, applying the criteria.

From the list of instances where the criteria were met in an NCSS, examples were chosen which we considered to most strongly meet the criteria, while ensuring a range of regional and national contexts.

As such, there are many further instances of good practice which are not highlighted in this tool, and so the examples included should not be considered exhaustive.

02

Respecting, protecting and promoting human rights through an NCSS

(1) Framing, vision, objectives and definitions

Criterion 1A: The section which frames cybersecurity and/or sets out the government's vision of cybersecurity should explicitly recognise the role that cybersecurity plays in protecting people's human rights

Most, if not all, NCSSs start with a section which frames the strategy, as well as the government's vision of cybersecurity within the particular jurisdiction. The framing of cybersecurity, while not forming the substance of the NCSS, is nonetheless critically important from a human rights perspective. There may be a range of ways that cybersecurity is framed - such as to protect national security or to support the digital economy. However, unless human rights also form an integral part of a state's understanding and vision of cybersecurity, the substantive sections are less likely to support the respect, protection and promotion of human rights. The section of the NCSS which frames cybersecurity, or sets out the government's vision (or both), should therefore explicitly recognise the role that cybersecurity plays in protecting people's human rights.

Criterion 1B: One of the objectives of the cybersecurity strategy, or one of the principles which underpins it, should be to respect, protect and promote the human rights of persons within the jurisdiction of the state concerned

Many NCSSs also contain a section setting out a range of high-level objectives for the NCSS. The explicit recognition of the role that cybersecurity plays in protecting human rights should be complemented by a clear and specific objective of ensuring the protection of human rights. Such an objective helps ensure that those tasked with implementing the NCSS consider the impact upon human rights of all actions and activities undertaken, as well as factoring human rights into the measurement of the NCSS's success. Other NCSSs contain a set of principles which underpin the NCSS itself; in these cases, one of the principles should be compliance with the state's international, regional and/or national human rights obligations.

Criterion 1C: The strategy should include a definition of cybersecurity which is consistent with human rights and international best practice

As well as human rights playing a part in the framing/vision and objectives of the NCSS, any definitions of cybersecurity (and, if appropriate, cybercrime) should be consistent with relevant international best practice, such as the definition of cybersecurity developed by Working Group 1 of the Freedom Online Coalition.

(2) Roles and responsibilities

Criterion 2A: Implementation of the NCSS should involve representatives of all stakeholder groups, including the private sector, the technical community and civil society

Cybersecurity is not the preserve of one particular actor. While governments play a critical role in ensuring the cybersecurity of a particular state, other actors - including the private sector, the technical community and civil society - all have specific roles as well.

From a human rights perspective, the role of civil society is particularly important. States have obligations under international human rights law to ensure that they respect, protect and promote human rights within their jurisdictions. However the expertise on human rights that can be found within civil society makes their involvement in the state's cybersecurity activities more likely to lead to outcomes which respect, protect and promote human rights. As such, regardless of the involvement of these different actors in the development of the NCSS, its implementation should also involve representatives of all relevant stakeholder groups, including civil society.

(3) Cyber resilience

Criterion 3A: There should be an explicit commitment to the principle of legality when it comes to measures taken to promote cyber resilience

Criterion 3B: There should be an explicit commitment to the principle of proportionality when it comes to measures taken to promote cyber resilience

The measures that a state takes to ensure resilience to cyber threats can have a significant impact upon the human rights of that state's population. Permitting broad government surveillance powers or imposing restrictions on the use of encryption, for example, may make it easier for security and law enforcement agencies to monitor individuals and their communications, and therefore prevent cyber threats from occurring. But they would also have highly adverse impacts on the ability of individuals to exercise and enjoy their human rights, particularly to privacy and freedom of expression, in the online environment.

Although there a wide range of potential measures that a state could take to increase its resilience to cyber threats, and which will vary from state to state, the NCSS should recognise that any measures to be taken to increase resilience to cyber threats will comply with basic principles of international human rights law, particularly the principles of legality (i.e. that measures will only be taken where clearly permitted under national law) and proportionality (i.e. that any adverse impacts upon human rights which result from measures taken will be proportionate to the legitimate aim that is being used to justify them).

Criterion 3C: The strategy should commit the government to the development of, where it does not already exist, appropriate, proportionate and effective data protection legislation, consistent with Council of Europe Convention 108, OECD Guidelines on Privacy, and other international best practice

Criterion 3D: There should be a clear commitment to promoting the digital literacy and security of the population, with particular emphasis paid, where necessary, towards vulnerable groups such as children, older persons and persons with disabilities

Two particular measures should be taken to increase a state's cyber resilience and which will have particularly positive impacts on individuals' human rights the development, where it does not already exist, of appropriate, proportionate and effective data protection legislation, consistent with Council of Europe Convention 108, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and other international best practice the promotion of the digital literacy and security of the population, with particular emphasis paid, where necessary, towards vulnerable groups such as children and older persons.

(4) Cyber incident response

Criterion 4A: There should be an explicit commitment to the principle of legality when it comes to measures taken to respond to cyber incidents

Criterion 4B: There should be an explicit commitment to the principle of proportionality when it comes to measures taken to respond to cyber incidents

The responses that a state is prepared to take when faced with a cyber incident can also have a significant impact upon the human rights of that state's population. If networks are shut down or restricted, for example, the ability of individuals to communicate, and impart and search for information - core elements of the right to freedom of expression - will be greatly reduced.

While NCSSs rarely set out the actions that the state will take in the event of a cyber incident in great detail, the NCSS should nonetheless recognise that measures to be taken in response to cyber incidents will comply with basic principles of international human rights law, particularly the principles of legality (i.e. that measures will only be taken where clearly permitted under national law) and proportionality (i.e. that any adverse impacts upon human rights which result from measures taken will be proportionate to the legitimate aim that is being used to justify them).

(5) Cybercrime

Criterion 5A: If the strategy includes a definition of cybercrime, that definition should be consistent with human rights and international best practice

Criterion 5B: The strategy should commit the government to the development of, where it does not already exist, appropriate, proportionate and effective cybercrime legislation consistent with the Budapest Convention

While the definition of 'cybercrime' is an important aspect where it is included within an NCSS and should be consistent with human rights and international best practice, the approach that the NCSS takes towards addressing cybercrime, particularly when it is through legislation, is also important. Appropriate, proportionate and effective criminal legislation to combat cybercrime may help protect human rights by protecting individuals from cyber threats. However, cybercrime legislation can also adversely impact upon human rights. The criminalisation of certain acts or behaviour can, in and of itself, be a restriction of human rights. Alternatively, overly broad definitions of certain crimes, or criminal offences with disproportionate penalties, can also lead to restrictions on human rights. While the precise crimes will likely be set out in specific legislation, rather than in the NCSS, the NCSS should, itself, recognise the importance of tackling cybercrime through appropriate, proportionate and effective criminal legislation, in line with international good practice, such as the Budapest Convention.

(6) International cooperation

Criterion 6A: There should be an unambiguous commitment to promoting a free, open and secure internet as part of the state's foreign policy

Criterion 6B: There should be an unambiguous commitment to the multi-stakeholder approach of internet governance as part of the state's foreign policy

Criterion 6C: There should be an unambiguous commitment to the principle that state behaviour in cyberspace is governed by international law

Criterion 6D: The section should identify relevant international and regional forums and policymaking spaces where co-operation on cybersecurity takes place, and where that foreign policy can be advanced

While NCCSs focus primarily on action that is being taken at the national level, the global nature of cyberspace means that many threats are also global in nature, affecting many - or even all - states. As such, NCCSs will often set out the means by which the government intends to work with other states on cybersecurity issues.

The approach taken towards states collectively, whether at the global or regional level, may have an impact upon human rights in the same way as national-level approaches. This is particularly true where states collectively develop joint frameworks whether they take the form of international law, such as treaties, non-binding documents or more informal initiatives. Such frameworks may set international standards or commit states to undertake certain action at the national level. Either way, there may be adverse impacts upon human rights.

It is therefore essential that just as the national-level frameworks and actions set out in the NCSS should respect, protect and promote human rights, so too should global and regional frameworks, and this approach should be explicitly reflected in an NCSS. This should be done through:

- Including an unambiguous commitment to promoting a free, open and secure internet as part of the state's foreign policy;
- Including an unambiguous commitment to the multistakeholder approach of internet governance as part of the state's foreign policy;
- Including an unambiguous commitment to the principle that state behaviour in cyberspace is governed by international law as part of the state's foreign policy; and
- Identifying relevant international and regional forums and policymaking spaces where co-operation on cybersecurity takes place, and where that foreign policy can be advanced.

03

Good practice examples

(1) Framing, vision, objectives and definitions

Criterion 1A: The section which frames cybersecurity and/or sets out the government's vision of cybersecurity should explicitly recognise the role that cybersecurity plays in protecting people's human rights

Argentina: The Argentinian NCSS (2019) states that:

"However, this horizon also shows us serious threats and effective damage to the rights of individuals and organisations, especially with regard to the privacy of their personal data, as well as the potentially devastating risks to international peace and security."

Canada: The Canadian NCSS (2018) states that:

"There is recognition that cyber security serves to protect personal information — and by extension, privacy". (p. 10)

Chile: The introduction to the Chilean NCSS (2017) notes that:

"Chile must stay up-to-date in security matters, as any mistake, or any successful breach to our systems, may harm our people's welfare or our rights, it may negatively affect our interests, or it may hinder or even impede the operation of critical services for the country." (p. 5)

"The policy reflects a central tenet: security and freedom are complementary. Combating cybercrime and other threats on the Internet cannot become an excuse to trample human rights such as privacy and freedom of expression on the contrary, they are means to fully guarantee these rights in cyberspace." (p. 9)

In setting out the needs for a cybersecurity strategy, the Chilean NCSS (2017) includes:

"A. To protect people's security in the cyberspace: People are to be ensured a security level allowing them to carry out their normal personal, social and community activities in the cyberspace, such as well as to exercise their fundamental rights as freedom of speech, access to information, protection of the private life and personal property." (p. 12)

Costa Rica: The introduction to the Costa Rican NCSS (2017) recognises:

"The protection of freedom of expression and privacy on the internet as a core principle of cybersecurity". (pp. 11-12)

European Union: The principles for cybersecurity in the European Union's Cybersecurity Strategy (2013) include:

"Protecting fundamental rights, freedom of expression, personal data and privacy

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and Systems." (p. 4)

France: The French NCSS (2015) notes that:

"Individual rights are applicable in the same way «on-line» and «off-line». Cyberspace should therefore remain a place of free expression for all citizens, where abuses can only be prevented within the limits set by the law and in line with our international agreements."

Greece: The introduction to the Greek NCSS (2018) states that:

"Open and free internet access, and the confidentiality, integrity, availability and resilience of ICT systems are the basis for prosperity, national security but also for the safeguarding of fundamental rights and freedoms." (p. 4)

Kosovo: The Kosovan NCSS (2015) notes that:

"Increased cyber security may improve, for instance, the protection of the privacy and property of network users." (p. 12).

Lithuania: The Lithuanian NCSS (2018) states that:

"Our aim is to raise public awareness and enhance the resistance of the Lithuanian society to cyber incidents which pose national security threats, present risks (…) to personal data protection and to the fundamental rights and freedoms of individuals." (p. 3)

New Zealand: The New Zealand NCSS (2019) has a section dedicated to the value of human rights, stating that:

"People are secure and human rights are respected online

The openness of the internet is part of its unique value – allowing for unrestricted participation and the free flow of information. People need to be able to operate in the digital world confident that their privacy will be protected and that their private and financial details will be protected. They should be able to engage online without suffering harm or unlawful interference, and be able to pursue criminal and consumer redress when things go wrong.

Human rights should be protected online as they are offline. International and domestic law similarly apply online as offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law."

North Macedonia: The North Macedonian NCSS (2018) notes that:

"Activities, social interactions, economy, as well as basic human rights and freedom at large depend on ICT usage; hence, it is necessary to ensure the existence of an open, safe and secure cyberspace."

Norway: The Norwegian NCSS (2019) has, as its vision:

"In Norway, it is safe to use digital services. Private individuals and companies have confidence in national security, and trust that the welfare and democratic rights of the individual are being safeguarded in a digitalised society."

Spain: The Spanish NCSS (2019) notes that:

"On the one hand, cyberspace makes universal connectivity possible and eases free flow of information, services and ideas." (p. 18)

"A fundamental dimension of stability involves continued defence of constitutional and democratic values and principles plus citizens' fundamental rights in cyberspace, particularly in terms of protecting their personal data, privacy, freedom of expression and access to truthful, good quality information." (p. 20)

"[D]igital information has become an asset with a high added value. Analysis of personal data on the Net is used for a wide range of purposes form sociological studies to advertising campaigns. (…) Furthermore, exploiting personal data breaches represents infringement of this data's security, affecting people's privacy and their data's integrity and confidentiality." (p. 27)

Sweden: The Swedish NCSS (2017) notes that:

"The open democratic society is dependent on the ability to maintain the desired confidentiality, authenticity and availability when handling information. This means that both the information itself and the systems used to store and transfer that information must be protected. (...) Ultimately, cyber security involves safeguarding fundamental societal values and goals, such as democracy, human rights and freedoms, Sweden's freedom, security and right to autonomy, and growth and economic stability.

If individuals are to be able to exercise their rights and freedoms, they need access to accurate and readily available information. This is a prerequisite for being able to make well-founded decisions and raises the quality and effectiveness of all types of activities and contacts in society.

Some information in society is sensitive and therefore needs to be protected. If sensitive information is lost, stolen, manipulated or disseminated to unauthorised persons, this can have serious consequences. There are large quantities of information that are of decisive importance to the functioning of society or that contain information sensitive with respect to privacy." (p. 5)

Criterion 1B: One of the objectives of the cybersecurity strategy, or one of the principles which underpins it, should be to respect, protect and promote the human rights of persons within the jurisdiction of the state concerned

NCSSs which contain goals or objectives:

Afghanistan: Objective 8 of the Afghanistan NCSS (2014) is:

"To safeguard data privacy of government, businesses and citizens by enabling the protection mechanisms for the data at rest and data at transit." (p. 7)
Argentina: One of the objectives of the Argentinian NCSS (2019) is:

"Objective 3) Development of the regulatory framework

Adapt and generate the legal norms, regulatory frameworks, standards and protocols, to face the challenges posed by the risks of cyberspace, ensuring respect for fundamental rights."

Chile: The Chilean NCSS (2017) also has a specific policy objective related to human rights:

"Respect for and promotion of fundamental rights

All measures proposed by the policy should be designed and executed with a focus on fundamental rights –because of their fundamental nature and indivisibility, and on the basis that cyberspace is an environment where people have the same rights as in the physical world. Therefore, the policy includes and promotes the following:

- The Internet is a global public asset; therefore, users may not be deprived from accessing the network but for reasons of force majeure duly based, with access never being denied by vague reasons such as public order, national security, or for the honour of any individual despite their capacity or title.
- Regarding the foregoing, and taking into account that information availability is an essential characteristic of cybersecurity, this policy will support public and private efforts made for the access to information and culture by the population through digital channels.
- Related with the above, the principle of respecting Internet neutrality is also included, so that Internet service providers may not discriminate or arbitrarily restrict the access to any content whatsoever, unless there is a legal justification to do that.
- This policy also respects and promotes the respect for freedom of speech, by taking into consideration not only communication media but also the population as a whole, the intermediaries making possible to communicate these messages and social networks. Any interference with this right shall be carried out in accordance with national and international standards in the field of human rights.
- The protection of private life and the inviolability of user communication in the cyberspace, including the protection against the unauthorised gathering, process and publication of personal data; transparency in the management of such data by private and public stakeholders, and as mentioned above, the protection of essential technologies to ensure that users may safely and confidently use the cyberspace.
- The protection of due process with regard to the measures affecting information security, seeking that surveillance and criminal prosecution measures in cyberspace comply with international standards with regard to protection such as the principles of suitability, need and proportionality. These measures will not only be applicable to criminal prosecution by the State, but also to the actions of all its bodies, thus safeguarding the application of this right among the users of cyberspace. Massive and indiscriminate surveillance of cyberspace is a serious attempt against fundamental rights.

Efforts in the field of fundamental rights will especially take into account the rights of vulnerable groups, such as, inter alia, boys, girls and young people, the elderly, disabled persons and ethnic minorities. There will be also a gender focus making possible to visualise and address the inequalities faced by different users in cyberspace.

The policy will seek that all people may enjoy a safe cyberspace free from abuses such as online bullying, the theft of personal information, large-scale surveillance and other practices affecting especially the most

underprivileged members of society. Particularly, efforts will be carried out at all levels so that cybersecurity is not considered luxurious for people or the country's organisations." (pp. 19-20)
Ireland: The Irish NCSS (2019) includes, as part of its vision:

"We will (…) [P]rotect the State, its people and critical national infrastructure from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs."

Mexico: The Mexican NCSS (2017) includes as an objective:

"Society and rights

Generate the conditions for the population to carry out their activities responsibly, freely and reliably in cyberspace, in order to improve their quality of life through digital development in a framework of respect for human rights such as freedom of expression, private life and protection of personal data, among others." (p. 18)

Portugal: The Portuguese NCSS (2015) includes an objective:

"To protect fundamental rights, freedom of expression, personal data and the privacy of citizens." (p. 4)

Slovakia: The Slovakian NCSS (2015) includes, as one of the elements of its overall goal:

"The adopted measures are adequate and respect the protection of privacy and basic human rights and freedoms." (p. 9)

Spain: The Spanish NCSS (2019) includes as its general goal:

"Spain will guarantee secure, reliable use of cyberspace, protecting citizens' rights and freedoms and protecting socio-economic progress." (p. 34)

NCSSs which contain principles:

Argentina: One of the principles of the Argentinian NCSS (2019) is:

"Respect for Individual Rights and Freedoms

The protection of people in matters of cybersecurity must include respect for the individual rights and freedoms enshrined in the national constitution and the international treaties to which Argentina is party."

Austria: One of the principles of the Austrian NCSS (2013) is:

"The rule of law: Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection as well as the freedom of expression and the right to information." (p. 7)

Costa Rica: One of the guiding principles of the Costa Rican NCSS (2017) is:

"Respect for human rights and privacy
Guaranteeing respect for human rights, especially those related to access to ICTs, access to information and respect for privacy, is fundamental. The measures and actions resulting from this strategy must at all times safeguard human rights and the privacy of information of the country's inhabitants.

Therefore, this strategy has been developed taking into account the need to balance the protection of inhabitants and respect for basic and fundamental human rights, with the need to implement measures to keep them safe online. This includes respect for freedom of expression, freedom of speech, the right to privacy, freedom of opinion and freedom of association." (p. 36)

Czech Republic: One of the principles of the Czech NCSS (2015) is:

"Protection of fundamental human rights and freedoms and of the democratic rule of law principles
In ensuring cyber security, the Czech Republic abides by fundamental human rights, democratic principles and values. It respects the Internet's open and neutral character, safeguards the freedom of expression, personal data protection and the privacy rights. It therefore strives for a maximal openness in access to information and for a minimal interference in individuals' and private entities' rights." (p. 9)

Estonia: One of the principles in the Estonian NCSS (2019) is:

"1. We consider the protection and promotion of fundamental rights and freedoms as important in cyberspace as in the physical environment."

Jamaica: One of the principles of the Jamaican NCSS (2015) is:

"Protection of Fundamental Rights and Freedom: This Strategy will not impair citizens' rights under Chapter 3 of the Constitution". (p. 17)

Kosovo: The Kosovan NCSS (2015) includes a principle of "human rights and freedoms":

"Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity regardless of ethnicity, gender, age, religion throughout all stages." (p. 13)

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation." (p. 12)

Mexico: The Mexican NCSS (2017) includes as one of its principles:

"Human rights perspective

Considering in the different actions in cybersecurity the promotion, respect and fulfillment of human rights; among others, freedom of expression, access to information, respect for privacy, protection of personal data, health, education and work." (p. 16)

Panama: One of the pillars of the Panamanian NCSS (2013) is:
"To protect the privacy and fundamental rights of citizens in cyberspace." (p. 6)

Spain: The Spanish NCSS (2013) notes in its section setting out the guiding principles that:

"They all respect and strengthen the protection and full enjoyment of the fundamental freedoms enshrined in our Constitution and in international instruments as important as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms." (p. 17)

Turkey: The Turkish NCSS (2016) includes as one of its principles:

"All stakeholders must pay regard to the rule of law, freedom of expression, fundamental human rights and freedoms as well as principles of protection of privacy in their efforts to ensure cyber security." (p. 16)

Ukraine: The Ukrainian NCSS (2016) includes as one of its principles:

"[T]he rule of law and respect for human and civil rights and freedoms".

United Kingdom: The UK NCSS (2016) includes as principles:

"[W]e will rigorously protect and promote our core values. These include democracy; the rule of law; liberty; open and accountable governments and institutions; human rights; and freedom of expression;

[W]e will preserve and protect UK citizens' privacy". (p. 25)

Criterion 1C: The strategy should include a definition of cybersecurity which is consistent with human rights and international best practice

n/a

(2) Roles and responsibilities

Criterion 2A: Implementation of the NCSS should involve representatives of all stakeholder groups, including the private sector, the technical community and civil society

Australia: The Australian NCSS (2016) contains a section setting out the roles and responsibilities of different actors in the implementation of the NCSS:

"Leadership and advocacy of this work will be driven by a new position in the Department [of the Prime Minister], the Prime Minister's Special Adviser on Cyber Security. The Special Adviser will lead the development of cyber security strategy and policy, provide clear objectives and priorities to operational agencies and oversee agencies' implementation of those priorities. The Special Adviser will also ensure the Government is partnering effectively with Australian governments, the private sector, non governmental organisations, the research community and international partners." (p. 24)

Costa Rica: The Costa Rican NCSS (2017) includes as a guiding principles:
"Coordination and co-responsibility of multiple stakeholders

Cybersecurity is a shared responsibility of all actors involved in the digital ecosystem, which includes users. It is imperative that all actions derived from this strategy consider, whenever relevant, the participation and contribution of all stakeholders, the co-responsibility of these and the need for coordination between the different actors.

For the implementation process, the support of all sectors is fundamental, therefore, public-public, public-private and public-civil society models must be considered and promoted; according to the suitability, requirements and scope of the objectives to be implemented." (p. 36)

Czech Republic: The Czech NCSS (2015) includes as a principle:

"Trust building and cooperation among public and private sector, and civil society

The state and its agencies cannot bear the sole responsibility for cyber security; an active cooperation of the Czech Republic's citizens, private legal persons and individual entrepreneurs is needed.

Cyberspace and, particularly, a part of the CII are largely owned and operated by the private sector. The security policy for this area is therefore based on inclusive cooperation between the public and the private sectors, civil society, as well as with academia. A trustworthy environment enabling cooperation is crucial. Trust among the state, private subjects, and civil society in general is essential in order to provide cyber security efficiently.

Due to the increasingly blurred lines between internal and external threats and risks, and hence between internal and external security, the Czech Republic shall aim at coordination of activities and enhance mutual trust among stakeholders both at the national and international levels." (p. 10)

Guatemala: The Guatemalan NCSS (2018) includes, as a principle:

"Shared responsibility

It is understood that the promotion and protection of cybersecurity belongs in a concerted manner to each and every one of the social actors, public and private, governmental or not, who must cooperate with each other at all times to achieve this objective." (p. 31)

Hungary: The Hungarian NCSS (2013) notes that:

"[T]he freedom and security of cyberspace is ensured through the close cooperation and coordinated activities between Government, academia, business sector and civil society based on their shared responsibility." (p. 2)

Jamaica: The Jamaican NCSS (2015) includes, as one of its guiding principles:

"All users, in enjoying the benefits of ICTs, should take reasonable steps to secure their own

Information Technology (IT) systems, exercise care in the communication and storage of personal and sensitive data and respect the data and IT systems of other users. This Strategy through its development and implementation supports a multi-stakeholder approach with shared responsibility for a secure cyber framework."

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The pervasive nature of cyber-space, essentially calls for a multi-stakeholder approach towards its security – both at a national level as well as beyond Malta's shores. Hence, on a national level, cooperation and collaboration of various stakeholders, including the public sector, the private sector, academia and civil society is necessary." (p. 12)

The NCSS also notes, in the section dealing with implementation that:

"The implementation of the Strategy is expected to involve multiple stakeholders within the public and the private sector as well as cooperation and coordination with civil society." (p. 31)

Slovakia: The Slovakian NCSS (2015) includes an implementation tool:

"Cooperation and partnerships at national and international levels of all relevant entities from public, private and academic sectors and the civil society." (p. 10).

Ukraine: The Ukrainian NCSS (2016) includes as one of its principles:

"[P]ublic-private partnership, broad cooperation with civil society in the field of providing cyber security and cyber defence".

(3) Cyber resilience

Criterion 3A: There should be an explicit commitment to the principle of legality when it comes to measures taken to promote cyber resilience

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress." (p. 12)

Kosovo: The Kosovan NCSS (2015) includes, as a guiding principle:
"Principle of Constitutionality and Legality – Actions undertaken in order to enhance cyber security must be based on the provisions provided for in the Constitution of the Republic of Kosovo, legislation in force and international agreements." (p. 13)

Criterion 3B: There should be an explicit commitment to the principle of proportionality when it comes to measures taken to promote cyber resilience

Guatemala: The Guatemalan NCSS (2018) includes, as a principle:

"Effectiveness and Proportionality

This refers to a focus on measures that are adequate to guarantee people's safe use of cyberspace and the exercise of their rights, prioritising the opportunities it offers, through risk management that is done to identify, prevent and respond proportionately to threats effectively." (p. 31)

Ireland: The Irish NCSS (2015) includes, as a principle:

"Measures to increase the level of protection need to be informed by an assessment of the risks and threats facing us, as individuals, businesses, public sector bodies and the State as a collective whole. Furthermore such measures will need to be proportionate to the respective risks and threats that we face." (p. 10)

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress." (p. 12)

Paraguay: The Paraguayan NCSS (2017) includes, as a principle:

"Proportionality: The measures to be applied must be adequate, necessary and proportionate, respecting fundamental rights, especially the rights to intimacy, privacy, freedom of expression and freedom of association, which are the highest priority of the State." (p. 22)

Portugal: The Portuguese NCSS (2015) includes, as a pillar:

"Proportionality: The risks inherent to cyberspace must be assessed and appropriately managed, ensuring proportionality of means and measures for their exercise." (p. 5)

Spain: The Spanish NCSS notes, as a guiding principle, that:

"[I]t is necessary to manage the risks derived from the use of technology in a dynamic manner, balancing opportunities and threats and ensuring proportionality in the protection measures adopted, which must be confidence-building elements and not hindrances to the development of new services." (p. 16)

Ukraine: The Ukrainian NCSS (2016) includes as one of its principles:

"[A]dequacy and proportionality of cyber security measures to actual and potential risks".

Criterion 3C: The strategy should commit the government to the development of, where it does not already exist, appropriate, proportionate and effective data protection legislation, consistent with Council of Europe Convention 108, OECD Guidelines on Privacy, and other international best practice

Guatemala: The Guatemalan NCSS (2018) includes, as an action:

"To create, approve and implement a law on privacy and data protection with reference to international conventions on human rights." (p. 36)

Sri Lanka: The Sri Lankan NCSS (2018) includes, as actions:

"Currently, the number of cases on stealing customer data is on the rise. However, Sri Lanka lacks appropriate laws to protect customer data. We will, therefore, introduce a data protection law which governs the collection, use, and disclosure of citizens' personal data by government and private sector organizations.

Through this act, we will ensure that all government organizations and private sector firms which maintain citizens' data have adequate security controls in place and make them liable for privacy violations." (p. 8)

Criterion 3D: There should be a clear commitment to promoting the digital literacy and security of the population, with particular emphasis paid, where necessary, towards vulnerable groups such as children, older persons and persons with disabilities

Australia: The Australian NCSS (2016) has a section on building the cybersecurity skills of the population:

"The Government will partner with other Australian governments, businesses, researchers and community groups to deliver a sustained, national awareness-raising campaign, encompassing a range of activities, which enables all Australians to be secure online.

The program will seek to educate Australians on the real-world impacts of cyber risks and the way this affects our current and future prosperity." (p. 55)

Bangladesh: The Bangladeshi NCSS (2014) has a section on creating a national culture of cybersecurity, which includes:

"Encouraging cybersecurity culture development in business enterprises [and] adding cybersecurity awareness to the national education curriculum as a way of spreading knowledge to pupils and their relatives". (p. 14)

Denmark: The Danish NCSS (2018) includes the following commitments and initiatives:

"Improve digital judgment and digital skills among children and young people.

Joint efforts will be launched throughout the educational system, focusing on raising awareness of security challenges for children, young people and teachers. Continuing and further education and training programmes will be developed, as well as teaching material
and awareness drives on cyber and information security aimed at teachers, pupils and students.

Raise awareness of cyber and information security among citizens, businesses and public authorities.

An information portal will be established which will contain readily accessible information and advice, specific tools for citizens, businesses and authorities regarding information security and data protection, as well as information on how to comply with current legislation. The content of the portal will be dynamic, current and regularly updated with the most recent knowledge." (p. 32)

(4) Cyber incident response

Criterion 4A: There should be an explicit commitment to the principle of legality when it comes to measures taken to respond to cyber incidents

Kosovo: The Kosovan NCSS (2015) includes, as a guiding principle:

"Principle of Constitutionality and Legality – Actions undertaken in order to enhance cyber security must be based on the provisions provided for in the Constitution of the Republic of Kosovo, legislation in force and international agreements." (p. 13)

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress." (p. 12)

Criterion 4B: There should be an explicit commitment to the principle of proportionality when it comes to measures taken to respond to cyber incidents

Guatemala: The Guatemalan NCSS (2018) includes, as a principle:

"Effectiveness and Proportionality

This refers to a focus on measures that are adequate to guarantee people's safe use of cyberspace and the exercise of their rights, prioritising the opportunities it offers, through risk management that is done to identify, prevent and respond proportionately to threats effectively." (p. 31)

Malta: The Maltese NCSS (2016) includes, as a guiding principle:

"The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress." (p. 12)

Paraguay: The Paraguayan NCSS (2017) includes, as a principle:

"Proportionality: The measures to be applied must be adequate, necessary and proportionate, respecting fundamental rights, especially the rights to intimacy, privacy, freedom of expression and freedom of association, which are the highest priority of the State." (p. 22)

(5) Cybercrime

Criterion 5A: If the strategy includes a definition of cybercrime, that definition should be consistent with human rights and international best practice

Australia: The Australian NCSS (2016) defines cybercrime as:

"[C]rimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software" as well as "crimes where computers are part of an offence, such as

online fraud." (p. 15)

New Zealand: The New Zealand NCSS (2019) defines cybercrime and cyber-enabled crime as:

"Cybercrime: Crimes that are committed through the use of computer systems, and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing.
Cyber-enabled crime: Crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are cyber-enabled fraud and the online distribution of child exploitation material." (p. 16)

North Macedonia: The North Macedonian NCSS (2018) defines cybercrime as:

"Cyber crime - acts against the law conducted in the cyber space, e.g. crime that may only be conducted through the use of ICT devices and systems, where the systems and devices are either used as tools for the criminal act, or they are the primary target; crime enabled by the cyber space, such as traditional criminal acts and materials for child abuse, which increases with the growing use of computers, computer networks or other forms of ICT." (p. 35)

Switzerland: The Swiss NCSS (2018) notes that:

"In a narrower sense, cybercrime refers to criminal offences that are committed with the help of ICT or that exploit the vulnerabilities of these technologies and are thus only possible because of ICT. In a broader sense, cybercrime also includes all criminal offences in which ICT is used as a means of perpetration or storage medium, but which would also be possible without the use of ICT." (p. 3)

United Kingdom: The UK NCSS (2016) notes two types of cybercrime:

"[C]yber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and

[C]yber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)." (p. 17)

Criterion 5B: The strategy should commit the government to the development of, where it does not already exist, appropriate, proportionate and effective cybercrime legislation consistent with the Budapest Convention

Bangladesh: The Bangladeshi NCSS (2014) provides, in the section dealing with cybercrime, that:

"It is recommended that the text of National Cybercrime law be drafted to comply with the provisions of the Convention on Cybercrime (2001)". (p. 5)

Costa Rica: The Costa Rican NCSS (2017) states:
"In order to further improve the Costa Rican regulatory framework and to take greater action against computer crime, Costa Rica has finalised the process of accession to the Cybercrime Convention known as the "Budapest Convention" through the signing of Executive Decree N° 40546-RREE on 3 July 2017 which helps in the fight

against computer crimes." (p. 23)

France: The French NCSS (2015) has, as an activity:

"Reinforcing the operational mechanisms of legal international mutual aid and universalising the principles of the Budapest Convention on Cybercrime.

The Budapest Convention, which was adopted in 2001 in the framework of the Council of Europe, has become a reference instrument that enables States of the five continents to cooperate in the combat against cybercrime. Ratified by 46 States, including 7 nonmembers of the Council of Europe, this instrument now unites 125 States for one reason or another (signatories, States invited to become members, States receiving technical assistance in view of future membership, States that have adapted their internal law to the model of the Convention). It is now essential to universalise and consolidate the base of norms as well as the tool of cooperation that this text is composed of."

Ireland: The Irish NCSS (2015) states, in the section dealing with cybercrime, that:

"The Minister for Justice and Equality will shortly bring forward legislation to give effect to the provisions of the Budapest Convention on Cybercrime and Directive 2013/40/EU on attacks against information systems." (p. 14)

New Zealand: The New Zealand NCSS (2019) states that:

"Key areas of focus will include (…) seeking Cabinet agreement to accede to the Budapest Convention." (p. 15)

Sri Lanka: The Sri Lankan NCSS (2018) states, in the section dealing with cybercrime, that:

"On 1st September 2015, Sri Lanka ratified the Council of Europe's Convention on Cybercrime (Budapest Convention) and became the first country in South Asia to become a party to the Convention. The Budapest Convention is the only internal legally binding treaty on Cybercrime in the world today and seeks to harmonize national laws, adopt improved investigative powers based on international standards, enhance criminal justice cooperation among State Parties in order to effectively combat the threat against cybercrime. We will take initiatives to implement and comply with the Budapest Convention requirements and will continuously work with member countries to build a secure cyber space."

(6) International cooperation

Criterion 6A: There should be an unambiguous commitment to promoting a free, open and secure internet as part of the state's foreign policy

Australia: The Australian NCSS (2016) contains a section on global responsibility and influence which notes that:

"Australia has consistently advocated for an open, free and secure Internet based on our values of freedom of speech, right to privacy and rule of law. Australia will continue to promote the opportunities provided by the Internet to be available to all, advocating against state censorship of the Internet." (p. 41)

Austria: The section of the Austrian NCSS (2013) on international cooperation notes that:

"Austria advocates a free Internet at international level. The free exercise of all human rights must be guaranteed in virtual space, and particularly the right to freedom of expression and information must not be restricted unduly in the Internet. This is the position Austria will adopt in international forums. Hence, Austria will participate actively in developing and establishing a transnational code for governance in cyber space, which will include measures to build confidence and security." (p. 16)

Canada: The Canadian NCSS (2018) states that:
"The Government of Canada will work with its international partners to advance Canadian interests. This includes advocating for an open, free, and secure internet (...)". (p. 32)

Chile: The Chilean NCSS (2017) states that:

"Efforts must be focused on promoting digital as a free, open and safe environment for all users in the cyberspace." (p. 22)

Czech Republic: One of the goals of the Czech NCSS (2015) is:

"To contribute to fostering an international consensus, within formal and informal structures, on legal regulations and behaviour in cyberspace, safeguarding of an open Internet, and human rights and freedoms." (p. 17)

France: The French NCSS (2015) states that:

"Individual rights are applicable in the same way «on-line» and «off-line». Cyberspace should therefore remain a place of free expression for all citizens, where abuses can only be prevented within the limits set by the law and in line with our international agreements. In international proceedings, France advocates this approach aimed at preserving a free and open cyberspace."

Ireland: One of the objectives of the Irish NCSS (2019) is:

"To continue to engage with international partners and international organisations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development.

Based on our support for an open, free, peaceful and secure cyberspace, we will advocate for preventative diplomacy in our international engagement." (p. 44)

Netherlands: The Dutch NCSS (2018) states that:

"The Netherlands continues to build and broaden the international coalition which subscribes to the vision of an open, free and secure internet." (p. 23)

New Zealand: The New Zealand NCSS (2019) states that:

"New Zealand's interests will be advanced and protected through our international activity. We will continue

to champion a free, open, secure internet. New Zealand's voice in international discussions related to cyber issues will support the international rules-based order and promote peace and stability in cyberspace."

North Macedonia: The North Macedonian NCSS (2018) includes as a goal:

"Republic of Macedonia to protect its cyber space through cooperation and exchange of information at national and international level, in order to facilitate an open, free, stable and secure cyber space." (p. 27)

Spain: The Spanish NCSS (2018) includes as a line of action:

"Contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests."

Sweden: The Swedish NCSS (2017) includes, as an objective:

"International cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights." (p. 24)

The Swedish NCSS also notes that:

"The Government's goal for the development of the internet is a global, accessible, open and robust internet characterised by freedom and respect for human rights." (p. 25)

(...)

Access to an open, free and secure internet constitutes an important instrument for the global enhancement of human rights, democracy, the rule of law and development. The internet opens new channels for people to communicate, interact and express their opinions and to promote their interests in a globalised world to an extent that has not previously been possible. Greater access to information and knowledge also promotes gender equality. Digital transformation and developments in information technology are increasingly a significant engine for economic and social development, not least in terms of creating conditions for the independence of poor people and women and their opportunities for work, and for innovative solutions to development problems in education, finance, agriculture, health and the environment." (p. 26)

Switzerland: The Swiss NCSS (2018) states that:

"A coherent foreign cyber security policy is indispensable for minimising cyber risks. The overriding goal of such a policy is a free, open and secure cyberspace." (p. 24)

United Kingdom: The UK NCSS (2016) states that:
"The UK aims to safeguard the long-term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning the UK's national security." (p. 63)

United States of America: One of the objectives of the US NCSS (2018) is:

"Promote an Open, Interoperable, Reliable, and Secure Internet

The global Internet has prompted some of the greatest advancements since the industrial revolution, enabling great advances in commerce, health, communications, and other national infrastructure. At the same time, centuries-old battles over human rights and fundamental freedoms are now playing out online. Freedoms of expression, peaceful assembly, and association, as well as privacy rights, are under threat. Despite unprecedented growth, the Internet's economic and social potential continues to be undermined by online censorship and repression. The United States
stands firm on its principles to protect and promote an open, interoperable, reliable, and secure Internet. We will work to ensure that our approach to an open Internet is the international standard. We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism." (p. 24)

Criterion 6B: There should be an unambiguous commitment to the multi-stakeholder approach of internet governance as part of the state's foreign policy

Australia: The Australian NCSS (2016) states that one of the core principles guiding Australia's international cyber engagement is that:

"The current way the Internet is governed, involving the private sector and the community as equal partners with governments, is the most effective model. This multi-stakeholder model of internet governance delivers economic benefit and social opportunity while balancing fundamental human rights, such as freedom of expression and privacy." (p. 41)

Chile: The Chilean NCSS (2017) states that:

"Efforts must be focused on promoting digital as a free, open and safe environment for all users in the cyberspace. The country needs to strengthen its work in this field, taking into consideration the special challenges faced in terms not only of the technical conditions, and the global nature and decentralised character of the network, but also regarding its political scope, and with a system of Internet governance including multiple stakeholders where the private sector and civil society have a special role." (p. 22)

European Union: The European Union's Cybersecurity Strategy (2013) states that:

"The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach." (p. 4)

Japan: The Japanese NCSS (2015) states that:
"[I]in the view of Japan, international law and other international rules and norms are applicable to cyberspace, and thus cyberspace should be governed by the rule of law in an international context as well." (p. 8)

New Zealand: The New Zealand NCSS (2019) states that:

"New Zealand's international engagement on cyber security issues will:

influence to support the rules-based international order and a free, open, multi-stakeholder internet." (p. 13)

Spain: The Spanish NCSS (2018) includes as a measure:

"In the sphere of the United Nations, promote the search for consensus to fully abide by the United Nations Charter and application and implementation of International Law and States' rules for responsible behaviour. Likewise, move forward in adopting and implementing Confidence-Building Measures in cyberspace." (p. 54)

Sweden: The Swedish NCSS (2017) states that:

"There are also fundamental tensions between states in their view of the roles and responsibilities of non-state actors. The Government wants to counteract a state-led administration of the internet and stresses the central roles and responsibilities of non-state actors for a free and secure internet, where the private sector and civil society can assert their legitimate interests. It is clear that both vulnerabilities and security measures concern and involve the private sector and civil society as a whole. Cooperation and dialogue with non-state actors thus need to continue being developed at the international level." (p. 25)

United Kingdom: The UK NCSS (2016) states that:

"[T]he UK will continue to: champion the multi-stakeholder model of internet governance". (p. 63)

United States of America: The US NCSS (2018) states that:

"The United States will continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet. The multi-stakeholder model of Internet governance is characterized by transparent, bottom-up, consensus-driven processes and enables governments, the private sector, civil society, academia, and the technical community to participate on equal footing. The United States Government will defend the open, interoperable nature of the Internet in multilateral and international for a through active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers, the Internet Governance Forum, the United Nations, and the International Telecommunication Union." (p. 25)

Criterion 6C: There should be an unambiguous commitment to the principle that state behaviour in cyberspace is governed by international law

Australia: The Australian NCSS (2016) states that one of the core principles guiding Australia's international cyber engagement is that:

"State behaviour in cyberspace is governed by international law and reinforced by agreed norms of state behaviour and practical confidence building measures to reduce the risk of conflict." (p. 41)

Chile: The Chilean NCSS (2017) states that:
"Although there are practically no specific regulation instruments, the cyberspace is actually regulated both

by the existing national laws and by the general applicable international regulations; therefore, the challenge lies particularly on being able to identify and interpret the relevant regulations of the applicable international law." (p. 22)

France: The French NCSS (2015) states that:

"Participation in multilateral negotiations on cybersecurity (UNO, OSCE) will be intensified in order to consolidate a global base of commitments to good conduct in cyberspace for the States, in compliance with international law."

Ireland: The Irish NCSS (2019) states that:

"The applicability of international law, including international humanitarian law, and respect for human rights will guide our international commitment to cybersecurity."

New Zealand: The New Zealand NCSS (2019) states that:

"New Zealand considers that existing international law applies online as it does offline and supports the development and implementation of norms for responsible state behaviour to maintain a peaceful and stable online environment."

Sweden: The Swedish NCSS (2017) states that:

"Within the UN, there is consensus in principle that international law is applicable in cyberspace, but that there are significant difficulties and challenges in ensuring that the rules are interpreted in unison. Against this background, international discussions are being held on the interpretation and application of international law in cyberspace and on the possibility to establish voluntary international standards and confidence-building measures for the responsible behaviour of states. There is also discussion in this context on the possibility of using international regulations, standards and agreements to verify, designate and demand accountability. The Government stresses the importance of Sweden taking an active role in these discussions and processes, with the aim of preventing conflicts and supporting international consensus on standards for the responsible behaviour of states." (p. 25)

United States of America: The US NCSS (2018) states that:

"The United States will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity. These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework." (p. 20)

Criterion 6D: The section should identify relevant international and regional forums and policymaking spaces where co-operation on cybersecurity takes place, and where that foreign policy can be advanced

Austria: The Austrian NCSS (2013) states:

"Global networking and international cooperation are key factors of the ACSS [Austrian Cyber Security Strategy]. Security in cyber space may be achieved only through a coordinated policy mix at national and international level. Austria will therefore engage in an active "cyber foreign policy" and pursue its interests in the framework of the

EU, UN, OSCE, Council of Europe, OECD and NATO partnerships based on a coordinated and targeted approach." (p. 16)

Czech Republic: One of the goals of the Czech NCSS (2015) is:

"To engage actively in international discussion taking place in the fora, programes (sic) and initiatives of the EU, the NATO, the UN, the Organization for the Security and Cooperation in Europe, the International Telecommunication Union and other international organizations." (p. 17)

United Kingdom: The UK NCSS (2016) states that:

"There are a range of relationships and tools we will continue to invest in to deliver and underpin all our international cyber objectives; we cannot achieve our objectives in isolation. These include (...) using our influence with multilateral organisations such as the United Nations, G20, European Union, NATO, OSCE, Council of Europe, the Commonwealth and within the global development community." (p. 64)

United States of America: The US NCSS (2018) states that:

"Given its importance, the United States will encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member." (p. 25)