RESEARCH IN FOCUS

Annex to "Strategically normative. Norms and principles in national cybersecurity strategies"

Dr Mika Kerttunen and Dr Eneken Tikk
Cyber Policy Institute
May 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

This analysis is part of Mika Kerttunen and Eneken Tikk (2019). "Strategically normative. Norms and principles in national cybersecurity strategies". Research in Focus. EU Cyber Direct, 13 April 2019, https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).

Methodological note

The following analysis covers the latest national policy documents that provide guidance on cybersecurity or information security. This guidance can be found, as explained above, in national cybersecurity or information security policies, strategies, doctrines, concepts, master plans or other formal governmental documents. A few ICT or digital strategies contain such guidance, but the majority of them do not - and are thus excluded from the analysis.

Also excluded are sectoral policy documents, for example national cyberdefence strategies, doctrines or manuals covering military network protection and principles, means and measures of cyber and information operations and electronic warfare. Similarly, documents containing specific guidance on incident or crisis management, market or frequency regulations and work force development, for example, are omitted from the study. One strategy we were not able to access, and five we had to leave unanalysed because we could not be sure of the level of translation.

In the following table, the notion of *objectives and issues* refers to key areas, concerns and objectives a government has stated in the document in question; *principles* refer to general, antecedent and foundational assumptions of the state or organising mode of affairs; and the notion of *norm* refers to expectations of behaviour or the desired state of affairs.

The analysis does not interpret the obviously contingent meanings of the words of choice, for example privacy, security, democracy or rule of law.[1] That some expressions do appear in two or even three categories (objectives and issues; principles; norms) is based on the contextual reading of how governments have used them and what they mean by these expressions. For example, 'transparency' may be an objective; an expected, fundamental state of affairs; or a norm depending on the actual circumstances of usage.

The governments in question are considered to be national or federal governments of UN member states (n=193) or factually functioning and to reasonable extent recognised, although not necessarily independent, states (n=3). This in effect excludes state, county or other sub-national governments as well as a few governments in mostly disputed areas within nation-states. The aforementioned inclusions and exclusions are not political statements. They are based on the factual capacity of a government to provide mid- to long-term political, administrative and regulatory guidance to national and subnational authorities and agencies.

Based on a common-sense geographical reading and for the sake of clarity, countries are grouped into five regions: Africa, Asia-Pacific, the Americas, Europe and The Middle East and the Gulf.

[1] Quentin Skinner, "Meaning and understanding in the history of ideas", (1969). Republished in Quentin Skinner, *Visions of Politics. Volume I. Regarding Method* (Cambridge: Cambridge University Press, 2002); Anthea Roberts, *Is International Law International* (Oxford: Oxford University Press, 2017), pp. 290-299.

Africa (53 countries, 16 national strategies or policies)		
Objectives and issues	**Principles**	**Norms**
Botswana, *National Cyber Security Strategy Draft 2016,* (not published; a presentation of the NCSS project)		
> Legal, policy and regulatory framework > Information security and infrastructure protection > Trust and confidence on ICT services > International collaboration > Socio-economic development > Awareness	> Rule of law > Centralized coordination and established roles and responsibilities > Multi-stakeholder approach > Cooperation > Prioritization	> Privacy and fundamental human rights and civil liberties > Confidentiality
Burkina Faso, *Plan national de cybersecurite de Burkina Faso, (2010)*		
> Regulative framework (7) > Reduction of vulnerability (12-16) > Situational awareness (17-18) > Culture of cybersecurity (19-20)	> Centralized coordination and established roles and responsibilities > (8-10) > Collaboration (16-17)	> Privacy and freedoms (7)
Cabo Verde, *Estratégia Nacional para a Cibersegurança*		
> Legal framework > Technical mechanisms and operational response to cybercrime > Critical information infrastructure protection > Institutional cybersecurity prowess	> National and international cooperation > Centralized coordination	> n/a
Côte d'Ivoire, *D'orientation de la soceiete de l'information en Cote d'Ivoire (2017)*		
> Legal and institutional frameworks (Art. 1, 16) > Critical infrastructure protection (Art. 1, 18) > Cybercrime (Art. 13)	> Centralized coordination (Art. 16) > Public-private cooperation (Art. 13)	> Human rights (Art. 1) > Integrity of information (7) > Transparency (Art. 3, 7)

Egypt, National Cyber Security Strategy 2017-2021		
> Socio-economic development (2) > Digital identity (4-5, 14) > Critical sectors (4-6, 13-14) > Awareness and preparedness (9-10) > Legislative, regulatory and executive framework (9-10, 13) > Human resources (14)	> International cooperation (11) > Public-private cooperation (10, 15) > Centralized coordination (12) > Multi-stakeholder approach (2)	> See the 2017 National ICT Strategy 2012-2017 on confidentiality and integrity (23), privacy (23-24) and social justice (20, 22)
Ghana, Ghana National Cyber Security Policy and Strategy 2015		
> Cyber crime, fraud (10, 17, 21) > Effective governance and legal framework (24) > Critical national information and information infrastructure with vital sectors (16, 20-23) > Capacity-building (25)	> Centralized coordination and enforcement (24-26) > Rule of law (24) > Public-private partnership (11, 17, 30) > International and regional cooperation, including joining international and regional conventions and harmonization of measures (24, 27)	> n/a
Kenya, Cybersecurity Strategy 2014		
> Development goals for and wealth employment (2, 9) > Economic growth (5-6, 8-9) > Transparent and efficient governance (7-8) > Information sharing (6, 8, 10) > Critical information infrastructure (6-7) > Formation of international rules explicitly on trade, property and privacy issues (9)	> Framework of governance (6-8) > Unified and holistic agenda (8-9) > International cooperation (9) > Public-private cooperation (1, 6-7)	> Property rights (9)
Mauritius, National Cyber Security Strategy 2014-2019		
> Information systems and network security (8) > National and societal vital services and functions (8, 11, 14) > Legal and administrative frameworks for implementation and national and international collaboration (10, 15, 19)	> Centralized governance and coordination (9-11) > Public-private cooperation (8-9, 14-15) > International cooperation including harmonization of measures (8, 14, 19)	> n/a

Morocco, Stratégie nationale en matière de cybersécurité (2012)		
> Critical information system and infrastructure protection (10-12) > Legal and regulatory frameworks (13 > Human resources (14)	> National and international cooperation (15-16) > Public-private cooperation (16)	> n/a
Mozambique, Mozambique's National Cybersecurity Strategy draft 2016		
> Socio-economic development (4-5) > Legal, regulatory, technical, and operational security frameworks (9, 10, 11-13, 15) > Information sharing, coordination and collaboration against cybercrime (9, 13-14)	> Rule of law (7, 8) > Multi-stakeholder approach (6, 8) > Shared responsibility (8, 10, 18-19) > Risk management (8) > Protection of vulnerable groups (16, 17) > International cooperation (8, 26, 31-32)	> Universal access to cyberspace (8, 16) > Confidentiality (17)
Nigeria National Cybersecurity Policy 2014 (referred by parts and sectors)		
> National critical information infrastructure including critical sectors (2.2.1, 4.3.2, 5.2.4, 7.1, 7.3, 7.5) > Legal framework and national governance mechanism including regional and international harmonized legislations (4.3.2, 4.4, 5.2.1, 9.3-9.5) > Economic growth, competitive advantage and foreign investments (5.4) > Child abuse and exploitation (10)	> Rule of law (4.5, 5.2.1) > Public-private partnership and multi-stakeholder approach (4.3.2, 5.2.7) > Assurance and monitoring mechanisms (8) > International and regional cooperation (1.2, 4.5, 5.2.2, 5.2.5, 5.2.7, 5.2.9, 6.6, 7.6) > Unified coordination of policies and strategies (5.2.2)	> Availability of information and privacy and intellectual property (4.3.2, 4.5) > Transparency in (of) the policy actions of the government (5.2.7) > National values, dignity, identity and image (5.4) > Patriotism (11)
Rwanda, National Cyber Security Policy 2015		
> Information and communication systems (25) > Awareness (25, 59) > National response capability (25, 57-60) > International cooperation > (25) > Legal and regulatory environment including a national cyber security strategy (26, 60)	> Integrated to national modernization and IT development ambitions and strategies (6-8, 13-14) > Centralized capabilities (57, 58) > Public-private interaction (12, 17, 56)	> Gender equality (12) > Good governance (12-13)

Senegal, *Stratégie nationale de Cybersécurité 2022*		
> Socio-economic development (12) > Legal and institutional frameworks (13-15) > Critical infrastructure protection (15-17) > Regional and international measures (22) > Human resources (19, 23)	> Rule of law (12) > Public-private partnership and cooperation (12, 24) > Risk-based approach (12) > Centralized planning, coordination and implementation (24) > Support from the defence sector (24)	> Confidentiality and integrity (18)
Sierra Leone, *Sierra Leone Cyber Security Policy (2016)*		
> Legal, regulatory and executive frameworks > Critical infrastructure protection > Incident response/emergency capacity	> n/a	> n/a
Uganda, *National Information Security Policy 2014*		
> Information and critical information infrastructure (6, 22-24, 28) > Information sharing (25)	> Accountability and responsibility (9, 14-16) > Rule of law (7-8) > Governance framework (12-13)	> n/a
South Africa, *National Cybersecurity Policy Framework for South Africa 2015*		
> Government led coherent cybersecurity approach (6, 11-12, 26-29) > Social and economic development (10, 13, 15) > Legal and regulatory frameworks (12, 14) > Cybercrime (15)	> Rule of law (12) > Centralized planning, coordination and response (6, 15-16) > Public-private partnership (6-7, 14, 29) > Balance between risks and effective usage (11) > International cooperation (15, 23-24)	> Privacy, security, dignity, access to information, the right to communication and freedom of expression (14) > Confidentiality (5)

The Americas (36 countries, 14 national strategies or policies)		
Objectives and issues	**Principles**	**Norms**
Argentina, *Estrategia Nacional de Ciberseguridad* (draft 2017)		
> Socio-economic development > Legal framework > Incident emergency capacity > Information security > Critical infrastructure protection > Awareness and workforce development	> Rule of Law > International Law > National and international cooperation > Public-private cooperation	> Human rights and freedoms
Brazil, *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018*		
> System of governance (39, 43, 47) > Critical infrastructure protection (53)	> Rule of law (20-33, 39, 48) > Centralized coordination (39) > Collaboration, public-private partnership (37, 50)	> Human rights, privacy (12, 15, 38) > Transparency (17, 26, 35)
Canada, *National Cyber Security Strategy 2018*		
> Cybercrime (10, 12-15) > Protection of critical public and private systems (6, 9, 17-18) > Innovation, research and development (19-25)	> Collaboration (6, 9-11, 31) > Federal leadership (26-29) > International cooperation (27, 31-32)	> Rights and freedoms (11, 32) > Privacy (10)
Chile, *National Cybersecurity Policy 2017*		
> Personal, social and community activities (12) > National information systems and services (12, 16) > Risk management (12, 16-18) > Institutional structure and governance (24)	> Rule of law (19, 25-28, 29-31) > Multi-stakeholder approach and cooperation (12, 17, 19) > Integration with foreign policy and national defence (15)	> Free and open cyberspace (11) > Freedom of speech, access to information, protection of the private life and personal property (12, 20) > Internet neutrality (20) > International law, democracy; human rights; conflict prevention; pacific resolution of disputes and the commitment to cooperate (21)

Colombia, *Policia Nacional de Seguridad Digital 2016*

- Socio-economic benefits (47)
- Institutional governance and legal frameworks (48-49)
- Cybercrime (48-49, 58-59)
- Critical infrastructure protection (49, 61-62)
- Rule of law (14-15, 20-21)
- Multi-stakeholder approach (28, 48, 53-57)
- National and international cooperation (48-49, 63-65)
- Risk management approach (28, 48)
- Centralized coordination (50-52)
- Support from the defence sector (60)
- Constitutional rights and freedoms (15, 27-28)
- Privacy, freedom of expression, free flow of information (20, 27-28)
- National sovereignty (18, 20, 60)

Costa Rica, Estrategia Nacional de Ciberseguridad de Costa Rica (2017)

- Socio-economic benefits (15-18, 32, 37)
- Legal frameworks (42)
- Information security (45-46)
- Cybercrime (33-34)
- Critical infrastructure protection (43-44)
- Public awareness (40)
- Work force development (41)
- Centralized coordination and cooperation with stakeholders (36, 38-39)
- International cooperation (47)
- Risk management approach (45)
- Human rights, freedom of expression, speech, opinion and association, right to privacy (35)

Dominican Republic, República Digital Ciberseguridad 2018-2021 (Referred by chapters)

- Economic growth (Preamble)
- Legal and administrative frameworks (5.1)
- Incident response and management capacity (6.3 – 6.4)
- Critical infrastructure protection (6.2)
- Cybercrime (5.2)
- General awareness and work force development (7)
- Centralized leadership (9-18)
- National, public-private cooperation (6.3, 7, 8)
- International cooperation (8)
- Basic human rights and freedoms, social justice, inviolability of communication (Preamble)
- Sovereignty (Preamble)

Guatemala, Estrategia Nacional de Seguridad Cibernética (2018)

- Cybersecurity governance system (25, 42-43)
- Capacity development (27)
- Legal framework (27)
- Work force development (27, 37)
- Cybercrime (27-28)
- Critical infrastructure protection (30-31)
- Rule of law (24, 27-28)
- Decentralized responsibilities (26, 38)
- International cooperation (26)
- Democracy and human rights (24-25, 29)
- Privacy (19-20, 35, 40)
- Transparency (5, 47)
- Cultural diversity (25)
- Proportionality (26)

Jamaica, *National Cyber Security Strategy 2015*

- National stability and development (9-10)
- Network infrastructure (5, 20)
- Cybercrime (in relation to stability and development) (10-14)
- Legal and regulative framework (5, 23)
- Centralized leadership (17, 27)
- Rule of law (13-14, 23)
- Multi-stakeholder approach with shared responsibilities (17)
- Risk management (17, 21)
- Regional and international collaboration (22, 23)
- Fundamental rights and freedoms (17, 24)
- Privacy (24)

Mexico, *National Cybersecurity Strategy 2017*

- Political, social and economic development (4, 14)
- Legal framework (23)
- Cybercrime (7, 20, 23)
- Critical infrastructure protection (22-23)
- Capacity and workforce development (19)
- Human rights (9, 17)
- Risk management approach
- Multidisciplinary and multi-stakeholder collaboration (9, 17)
- Centralized coordination (9, 17, 21, 25-26)
- Human dignity and integrity (4)
- Freedom of expression, access to information, respect for privacy, protection of personal data, health, education, and work (17, 19)

Panama, Estrategia Nacional de Seguridad Cibernética y Protección Infraestructuras Criticas (2013)

- Legal framework
- Governance structure
- Critical infrastructure protection (38, 39-41)
- Protection of the individual (36, 39)
- National (private-public) and international collaboration (38-39)
- Proportionality (42)
- Human rights and freedoms (36-39)
- Privacy (39)
-

Paraguay, Plan Nacional de Ciberseguridad: Retos, Roles y Comprimisos (2017)

- Governance system (18, 30-31)
- Awareness and competence (23-25)
- Critical infrastructure protection (26-27)
- Cybercrime (16-17, 29)
- Proportionality (22)
- Centralized coordination, decentralized responsibilities (22)
- Public-private cooperation (12, 15-16)
- International cooperation (22)
- Human rights and civil liberties (22, 36, 40)
- Transparency (33)

Trinidad and Tobago, National Cyber Security Strategy 2012		
> Governance framework (3-4, 12-15) > Incident management (4, 15-16 > Cybercrime legislation (4, 11, 19)	> Sustainable development (5, 11) > Centralized coordination, implementation, monitoring, continuous improvement and governance (11) > Multi-stakeholder approach (4, 16, 18) > Cooperation (4, 16-17) > Shared responsibility (16) > International collaboration (17)	> Confidentiality (6-7) > Privacy (4, 7, 11)
United States, National Cyber Strategy of the United States of America (2018)		
> Protection of federal networks, systems, functions and data (6-7) > Digital and prosperous economy (14-19) > Critical infrastructure protection (8-9) > Combating cybercrime (10-13) > Workforce development (17)	> Deterrence and consequences (21-23) > Centralized authority (6-7) > International law and non-binding norms of responsible state behaviour (20) > Transparency (14, 16, 21) > Multi-stakeholder approach (25) > International cooperation (25-26)	> Open internet (24) > Democracy (9) > Privacy (2, 9) > Civil liberties and human rights (2, 9, 21, 24)

Asia and the Pacific (46 countries, 25 national strategies or policies)

Objectives and issues	Principles	Norms
Afghanistan, National Cyber Security Strategy of Afghanistan 2014		
> National security and economic competitiveness, public order and national security (5) > Government ICT infrastructure and information security framework (7-8) > Cyber crime (7)	> Rule of law (9) > Centralized coordination (12) > Public-private partnership (7-8, 10-11) > International and regional cooperation (7, 11)	> Privacy (7, 10) > Confidentiality (8-9)
Armenia, National Cybersecurity Strategy 2017		

Australia, *Australia's Cyber Security Strategy 2016*; See also the 2017 Australia's International Cyber Engagement Strategy

> Growth and prosperity (8) > Malicious cyber activities (15-16) > Information sharing (28)	> Rule of law (25) > Public-private partnership (6, 21-25) > Resilience and responses (6, 27-33) > International cooperation (7, 39-43)	> Freedom of speech and information (17, 25, 39, 41) > Confidentiality, integrity and availability of systems (15) > Privacy (25)

Azerbaijan, *Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün MİLLİ STRATEGİYA (On the development of information society in the Republic of Azerbaijan for the National Strategy for 2014-2020)*

Bangladesh, *The National Cybersecurity Strategy of Bangladesh 2014*

> Economic security (2-4) > Critical information infrastructure protection (4, 8-9) > Establishment of cybersecurity framework and modernization of laws, procedures, and policy (5, 7-9)	> Rule of law (5-6) > Multi-stakeholder approach (6-7, 10, 13) > Centralized coordination (10) > International cooperation (4-5, 11)	> Confidentiality (9)

People's Republic of China, *National Cyberspace Security Strategy (2016)* (Referred by chapters)

> Political stability, economic, cultural and social security and overall national security (I, II, IV.4) > Sovereignty (III) > Peaceful cyberspace (III) > Strong cyber power (II) > Critical infrastructure protection (IV) > Unlawful practices (IV.5)	> Rule of law (Preamble, I, III.3) > Innovative, coordinated, green, open and shared development (II) > Risk and crisis consciousness (II) > Cooperation (IV) > International cooperation (IV.9)	> Peace (II) > Sovereignty (III) > Human rights, privacy (II) > Internal and external security (II, III) > Free flow of information (II)

Republic of China, *Taiwan National Strategy for Cybersecurity Development Program (2013-2016)*

India, *National Cyber Security Policy 2013* (referred by paragraphs)

> Cyber security framework (7) > Information security (II-IV B) > Critical information infrastructure (IV G) > Regulatory framework (III-3) > Socio-economic development (3, 5, III-1)	> Public-private partnership (IV A, C, G, L)	> Confidentiality, integrity (5) > Privacy (III-10, 12)

Indonesia, *National Cyber Security Strategy 2018*		
> Economic growth > Resilience > Public Service Security > Law Enforcement	> Centralized coordination > Multi-stakeholder approach	> Sovereignty, independence,
Japan, *Cybersecurity Strategy 2015*		
> Socio-economic vitality (3-6, 12) > National security (36-38) > National competitiveness (6-7) > International rules and norms (8, 35, 39) > Critical information infrastructure (21, 25-27) > Information sharing (27-28)	> Peace and stability (5, 35, 38-41), > Rule of law (8, 39) > Centralized coordination (52-53) > Multi-stakeholder approach (9, 13-14) > International cooperation (19-20, 35, 39, 41-44)	> Freedom of information (5, 8, 35) > Democracy (8, 35) > Autonomy in management (9, 15) > Diversity (35)
Kazakhstan, Concept of Information Security – Cyber Shield (An infosheet)		
> Economic growth > National security > Institutional reform > Legal and regulatory framework > Technical and socio-political aspects of information security > Combating corruption and cybercrime > Public awareness	> Centralized coordination > Centralized management of communication networks	> Integrity and confidentiality
Republic of Korea, National Cyber Security Masterplan (2011)		
> Joint public, private and military response system (1, 2) > Critical infrastructure protection (1, 3)	> Deterrence through international cooperation (1, 3) > Multi-stakeholder approach (2)	> n/a
Malaysia, *The National Cyber Security Policy 2006*		
> Legal and regulatory framework (3, 6) > Government systems and critical national information infrastructure (3, 6) > Effective governance (6) > Information sharing (6) > Social and economic well-being (2)	> Centralized coordination (6) > Public-private cooperation (3) > International cooperation (6) > Standardization (4-5)	> n/a

Mongolia, *Cybersecurity Policy in Mongolia 2014* (referred by slides)

> Legal framework (6, 8) > Information security and critical infrastructure protection (6, 7) > Governmental information security framework (6) > Cooperation (21) > Awareness (15)	> Rule of law (7) > Public-private partnership (7) > International cooperation (7)	> Privacy and human rights (7)

Nepal, *National Cybersecurity Policy 2016* (Referred by chapters)

> Institutional capacity (2.3, 7) > Legal frameworks (4.4, 7.4) > Incident emergency capacity (2.3, 5.2, 7) > Cybercrime (1.2, 5.6) > Critical infrastructure protection (1.3, 5.9, 9) > Child Online Protection (8) > Human resources (2.5)	> Millennium Development Goals (1.4) > Public-private partnership (2.4, 4.2) > Centralized coordination (6, 7.1.2, 10) > International cooperation (1.5, 7.7)	> Fundamental rights and freedoms (1.2, 5.6) > Privacy (5.11)

New Zealand, *New Zealand's Cyber Security Strategy 2015*; See also New Zealand's Cyber Security Action Plan 2015

> Economic well being, growth and competitiveness (3, 5-7) > National security (2, 7) > Cybercrime (6)	> Public-private partnership (4-7) > Rule of law (7) > International cooperation (6)	> Human rights (5, 7) > Open cyberspace, freedom of expression (6-7) > Integrity of information (7) > Privacy (7)

Philippines, *National Cyber Security Plan 2022*

> Information security (25) > Critical and national information infrastructure and systems (2, 26-28, 32, 35-36) > Cybercriminal ecosystems (8-9)	> Rule of law (21) > Centralized coordination (17-20) > Multi-stakeholder approach (20-22, 30) > International cooperation (21, 30)	> Autonomy and self-governance in management (21) > Confidentiality, integrity and availability of systems and services (17) > Freedom of information (21) > Privacy (21)

Samoa, Samoa National Cybersecurity Strategy 2016

> Socio-economic development (5) > Organizational structures (7) > Capability development (8) > Legal framework (9) > Awareness (10)	> Rule of law (6, 9) > Cooperation (11-12) > Multi-stakeholder approach (11)	> Privacy (2) > Fundamental rights (6, 9)

Singapore, *Singapore's Cybersecurity Strategy 2016*

> Critical information infrastructure (8-9, 12-13) > Governance and legislative framework (19, 23) > Cybercrime (23-29) > Collective global and regional security through cooperation, confidence building and norms development (46-47) > Security by design (12, 14-15)	> Centralized management (9) > Multi-stakeholder approach (6, 9, 12, 32-33) > International cooperation (42-47)	> Collective responsibility (32-33)

Sri Lanka, *Information and Cyber Security Strategy of Sri Lanka 2019-2022*

> Governance, legislative and regulatory frameworks (6-7, 8-9) > Workforce development (9-11) > Critical infrastructure protection (9, 12-14) > Cybercrime (8, 19) > Public awareness (14-16)	> Centralized coordination (6-7, 18) > Public-private partnership (16-19) > International cooperation (18-19)	> Privacy, freedom of expression (8, 9)

Tajikistan, *Concept of Information Security of the Republic of Tajikistan*

Thailand, *National Cybersecurity Strategy 2017-2021*

Vanuatu, *National Cybersecurity Policy 2013*

> Organizational structures (7-8) > Legal frameworks (6, 9-10) > Incident emergency capacity (7) > Critical infrastructure protection (8) > Cybercrime (8, 10)	> Millennium Development Goals (5) > Multi-stakeholder approach (5, 7) > Centralized coordination (7) > International cooperation (6, 11)	> Fundamental rights (6)

Vietnam, Decision approving the orientation, objectives and duties to ensure the cyber information security for the period 2016-2020 (2016) (referred by sections and paragraphs)

> Information security (I, III) > Awareness (II-1, IV-3) > National important information system (III) > Technical regulation and standard system (II-3, III-1b) > Regulatory and policy framework (III-2, IV-1) > Domestic product development (II-4, III-3)	> Rule of law (I-1, V) > Centralized planning and coordination (VI) > Mobilization of social resources (I-1) > Whole-of-society collectivism > Domestic, regional and international cooperation (IV-2)	> n/a

Europe (46 countries, 42 national strategies or policies)		
Objectives and issues	**Principles**	**Norms**
Albania, Strategjia për Mbrojtjen Kibernetike 2014 (in Albanian)		
Austria, Austrian Cyber Security Strategy 2013		
> Social prosperity and economic benefits (9) > Structures, processes and governance (10-12)	> Rule of law, subsidiarity, self-regulation and proportionality (7-8) > Centralized operational coordination (10-11) > Multi-stakeholder approach (7, 12-13) > International cooperation (9, 16)	> Human rights (4, 7, 16) > Privacy (7) > Confidentiality (9) > Personal responsibility (9)
Belgium, Cyber Security Strategy 2012 (in Flemish and French)		
> Critical infrastructure protection (8) > Work force development (11) > Response capacity (12) > Cybercrime (12)	> Decentralized responsibility and multi-stakeholder approach (10) > International cooperation (8-9, 10) > Confidentiality and integrity (8)	> Rights and freedoms (8) > Privacy (6) > Tolerance, respect and freedom of expression (8)
Bulgaria, National Cyber Security Strategy Cyber Resilient Bulgaria 2020 (2016) (in Bulgarian, a presentation in English)		
> National cyber security and resilience system > Network and information security and critical infrastructure protection > Information sharing > Legal and regulatory framework	> Rule of law > Multi-stakeholder approach > Centralized coordination – decentralized implementation > International cooperation	> Collective engagement > Confidentiality
Cyprus, Cybersecurity Strategy of the Republic of Cyprus 2012		
> Organizational and legal frameworks (14-18) > Network and information security (5-6)	> Rule of law (8-11, 18) > Multi-stakeholder approach (7, 18-20) > International cooperation (25-26)	> Confidentiality (5-6) > Trust (6, 7) > Human rights (11)

Czech Republic, *National Cyber Security Strategy of the Czech Republic 2015-2020*		
> Critical information infrastructure (7, 11) > Cooperative framework (8, 16) > Trust (10-11, 17, 19)	> Rule of law (6, 9, 20) > Public-private partnership (10, 18) > Subsidiarity and cooperation (9, 18) > International cooperation (7, 10, 17)	> Human rights and freedoms (9, 17) > Informational self-determination (9) > Privacy (9)
Germany, *Cyber Security Strategy for Germany 2015*		
> Economic and social prosperity (4, 13) > Framework conditions (4,) > International rules of conduct, standards and norms (4, 11) > Information sharing (5-6)	> Multi-stakeholder approach (5, > Coordinated response (8-9) > International cooperation (11)	> Confidentiality (4, 14)
Denmark, *Danish Cyber and Information Security Strategy 2018*		
> Technological preparedness (13) > Situational awareness (20-21, 23) > Regulatory frameworks (24) > Critical governmental ICT systems (24) > Cybercrime (24) > Protection of vital sectors (36-41, 43-45) > Public awareness (13, 28-33)	> Rule of law (41) > Governmental assistance, coordination and guidance (52) > Cooperation and coordination between responsible authorities > (13, 36-37, Appendix) > Sectoral responsibility, similarity, subsidiarity, cooperation and precaution (47) > Risk-based management (36)	> Privacy (5) > Citizens' rights (41)

Estonia, Küberturvalisuse strateegia 2019-2022		
> Digital governance and economy (1-2, 5-6, 20-25) > Combating cybercrime (7, 14) > International cybersecurity, incl. cyberoperations (7-8, 8-9) > Technological (inter)dependency (services, data storage) (8) > Workforce development (10-11, 33-37)	> Security and privacy design (3, 21) > Integration of cybersecurity into all state policies, incl. national defence (3-4, 13-14, images no. 1 and 2) > Centralized coordination (13, 16-17) > International cooperation (19-20, 29-32) > Rule of law (3-4, 10, 16, 23, 28) > International law (7-8, 14, 30, 31-32, 38) > State-private sector partnership (4, 9-10)	> Rights and liberties (2) > Privacy (21) > Free and secure cyberspace (8) > Transparency (3, 8)
Spain, National Cyber Security Strategy 2013		
> Competence of public authorities (10, 15, 30-33) > Economic potential, investments, jobs and competitiveness (i-ii, 10) > Organizational and regulatory framework (21, 43-45)	> Rule of law (17, 24) > Centralized leadership and coordination of efforts (15-16, 43-45) > Shared responsibility and public-private partnership (15-16, 36) > International cooperation (16, 26-27, 39)	> Proportionality- ty (16) > Human rights (17) > Trust
Finland, Finland's Cyber Security Strategy 2013; See also Implementation Programme for Finland's Cyber Security Strategy for 2017-2020		
> Vital functions (1-3) > Situational awareness (4-5, 7-8) > Distributed responsibilities and implementation (4-5, 7, 10) > Information exchange (7-10)	> Rule of law (5, 8, 10) > Public-private partnership (3, 6) > Multi-stakeholder participation (3, 6, 10) > International cooperation (5, 7-8)	> Self-defence (1, 8) > Privacy and confidentiality (10)

France, *French National Digital Security Strategy 2015*

> Fundamental interests, State information systems and critical infrastructures (14) > Awareness raising (26-27) > Digital technology businesses, industrial policy, export and internationalization (30) > European digital autonomy (30, 38) > Control of mass data (8, 20)	> Rule of law (17, 21, 38) > Multi-stakeholder approach (8-9, 14-15) > Multi-lateral cooperation (17, 23)	> Privacy (8, 20, 23) > Freedom of expression and action (9) > Individual rights (21, 39)

Georgia, *Cybersecurity Strategy of Georgia 2017-2018*

> Research and analysis (8-9, 12-12) > Legal and regulatory framework (9-11) > Critical infrastructure protection (3, 5-6, 9) > Public awareness (12-13)	> Public-private cooperation (3) > International cooperation (13-14) > Individual responsibility (3)	> Human rights and basic freedoms (2)

Greece, *National Cyber Security Strategy 2017*

> Critical infrastructure protection (5, 7) > Institutional framework (8)	> Rule of law (5) > Centralized coordination (3, 5) > Multi-stakeholder approach (6, 7, 10) > International cooperation (13-14)	> Fundamental rights and freedoms (4, 9) > Privacy (6)

Croatia, *The National Cyber Security Strategy of the Republic of Croatia 2015*

> Organizational and regulatory frameworks (4, 6) > Shared awareness (4, 7, 24) > Electronic communication and information infrastructure (9-10)	> Rule of law (6, 19) > Multi-stakeholder approach (4-5, 8, 15) > International cooperation (7, 22-24)	> Human rights and liberties, proportionality and subsidiarity (6) > Trust

Hungary, *National Cyber Security Strategy of Hungary 2013* (referred by paragraphs)

> National sovereignty, economy and society (1, 6) > Political and professional decision-making (4) > Secure and reliable cyberspace (8)	> Rule of law (2, 6) > Government coordination (1, 6, 10a) > Multi-stakeholder approach (6, 10b-c) > International cooperation (1, 7, 10e)	> Freedom (1, 6) > Democracy (6)

Iceland, Icelandic National Cyber Security Strategy 2015–2026 (summary in English)		
> Economic prosperity and development (3, > National capacity (3, 7-9) > Legislative framework (3, 11)	> Integrated systemic functioning (4) > Multi-stakeholder approach (4, 8) > International cooperation (3-6) > Inclusion of security and privacy from the outset in the design process (5)	> Human rights and freedoms (3)
Ireland, National Cyber Security Strategy 2015-2017		
> Prosperity, lifestyle and social development (4) > Organizational and regulatory frameworks (12-13)	> Rule of law (4, 8, 10) > Risk based approach (10) > Multi-stakeholder approach (2, > International cooperation (8-9, 13) > Civil-military cooperation (14)	> Human rights (4, 10) > Open and free access to cyberspace (4, 11) > Subsidiarity and proportionality (10, 11) > Trust (2) > Norms of State behaviour (8)
Italy, National strategic framework for cyberspace security 2013		
> Cyber crime (13-14, 20) > Critical information networks (15, 20) > National capacity (capabilities) (20-21)	> Rule of law (5, 30-39) > International law (16,2 2) > Multi-stakeholder approach (6, 11, 26-29) > Balance between privacy and countering criminal activities (12) > International cooperation (6, 20-23, 34) > Sectorial, thematic planning and coordination (30-39)	> Individual liberties, equality and freedom (5,) > Privacy and integrity (11, 24-25, 30) > Rules of behaviour (6, 16, 22)
Kosovo, National Cyber Security Strategy and Action Plan 2016-2019		
> Institutional development and capacity building (18-20) > Critical infrastructure (18)	> Rule of law (13-15) > Democracy (12) > Public-Private partnership (13, 21) > Subsidiarity (13) > National coordination (15) > International cooperation (13, 18, 22)	> Human rights and freedoms (12-13) > Privacy (12) > Confidentiality (13)

Latvia, *Cyber Security Strategy of Latvia 2014-2018*		
> Economic development and global competitiveness (2,) > National governance framework (5-10) > Cooperation with Defence Forces and integration of cyber security with national defence (7, 9, 14)	> Rule of law (10) > Multi-stakeholder approach (3, > Centralized coordination (7) > International cooperation (14-15)	> Human rights, fundamental freedoms and privacy (3, 10, 14)
Lithuania, *National Cyber Security Strategy 2018*		
> Risk identification and analysis (5, 6) > Cyber defence capabilities (2, 5) > Legal and regulatory frameworks (5) > Cybercrime (6-8) > Awareness and competences (8-11)	> Centralized coordination (14) > Public-private partnership (1, 12-15) > Integral security management system (4) > International cooperation (13-14)	> Human rights and freedoms (13)
Luxembourg, *National Cyber Security Strategy 2018*		
> Economic prosperity (23) > Protection of critical information infrastructure (19-22) > Cybercrime (17-18, 33)	> Rule of law () > Centralized coordination () > Public-private cooperation (11, 16, 26, 31) > National and international cooperation (21, 31-32)	> Privacy (15) > Confidentiality and integrity (7, 10)
Monaco, *Stratégie nationale pour la sécurité du numerique*		
> Competitive economic environment (22-24) > Critical infrastructure protection (10-11) > Cybercrime (14-15) > Awareness (18-19) > Stability and peaceful cyberspace including international norms (26-27)	> Multi-stakeholder approach (5, 11) > Centralized coordination (10-12) > International influence (27-28)	> Privacy (5, 16) > Confidentiality and integrity (5) > Human rights, freedom of expression (15)

Moldova, National Cyber Security Programme 2015 (An infosheet)		
> Information security > Regulatory frameworks and standards > Management system > Incident emergency capacity > Cybercrime > Cyber defence > Public awareness	> Centralized management > Shared and personalized responsibility > Public-private partnership > International cooperation	> Fundamental rights, freedom of speech
Montenegro, Cyber Security Strategy of Montenegro 2018-2021		
> Growth and property (25, 37) > Institutional and organizational structures (13-14, 18-21) > Critical infrastructure protection (14, 26-28) > Cybercrime (15) > The role of the defence sector (16) > Public awareness (16, 30-32) > Human resources (11, 17, 25)	> Rule of law (10, 27, 28, 29-30) > Centralized coordination (19-21) > Public-private partnership (16, 32) > Regional and international cooperation (33)	> Privacy and integrity (5)
North Macedonia, National Cyber Security Strategy 2018-2022		
> Economic prosperity (12-13) > Institutional and legal framework (4) > Resilient ICT infrastructure (18-19) > Cybercrime (4, 7-11, 22-23) > Cyber defence (24-25) > Public awareness (20-21)	> Centralized coordination (29-31) > Multi-stakeholder approach (12, 15) > National and international cooperation (26-28)	> Integrity and confidentiality (3) > Human rights and freedoms (4, 14) > Democracy, freedom of information and expression, privacy (14)
Malta, Malta Cyber Security Strategy 2016		
> Governance framework (17-19) > Legal and regulatory framework (20-21) > Awareness (24-26)	> Rule of law (12) > Multi-disciplinary and multi-stakeholder approach (12-13) > Shared responsibility (13) > Risk-based approach (13) > Self-regulation (5, 22) > National and international cooperation (27)	> Privacy, confidentiality, personal integrity, identity and well-being (13, 16) > Fundamental rights and freedoms (8, 12, 20) > Confidentiality (8)

Netherlands, National Cyber Security Agenda (2018)

> Economic and social opportunities (7, 9, 17) > Response capabilities (5, 19-20) > Resilient infrastructure (5, 31-33) > Espionage and sabotage (11-12) > Cybercrime (11, 35-36) > Secure hard and software (27-29) > International peace (23-24)	> Centralized coordination (5, 10) > Public-private approach (7, 13, 43-44) > Integration to national security (13) > Transparency (7, 14, 32) > International cooperation (5, 14)	> Human rights (9, 14, 23, 24) > Freedom (7, 14)

Norway, Cyber Security Strategy for Norway 2012

> Information security (10-11) > Incident management (21-22)	> Rule of law (11, 17) > Owner and sectorial responsibility (15, 26-27) > Multi-stakeholder approach (24, 26) > International cooperation (24, 26)	> Privacy (12, 14, 26) > Confidentiality (28) > Freedom of information (29)

Poland, National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022

> Social and economic development (4) > Legal environment (8-9) > Governance structures (9-10) > Critical infrastructure protection (11-12) > Cybercrime (15) > Capacity to perform military operations (16) > Competence development (18, 19-21)	> Centralized coordination (24) > Comprehensive and cooperative approach (10-11, 19) > Risk management approach (13, 14) > International cooperation (22-23)	> Rights and freedoms (7, 21) > Privacy (5)

Portugal, National Cyber Security Strategy 2015 (referred by paragraphs and "axes of intervention")

> Protection of critical infrastructure and vital information services (1, 3, Axis 3) > Awareness (2e, Axis 4) > Politico-strategic coordination mechanism (Axis 1,1-3)	> Rule of law (2, Axis 2,1 and 3, 11-12) > Subsidiarity (2a) > Complementarity (2b) > Cooperation (2c, Axis 6) > Proportionality (2d)	> Fundamental rights, freedom of expression and privacy (2, 3)

Romania, *Cyber security strategy of Romania 2013*

- National security interests (1, 5)
- Legal and regulatory framework (2, 5)
- National cyber security system (6)
- Cyber infrastructure protection (2, 5)
- Economic benefits (2, 5)
- Information exchange (5)
- Rule of law (1)
- Centralized coordination (1, 3, 7)
- International cooperation (2, 6)
- Public-private cooperation (5, 7-8)
- Accountability (4)
- Individual rights and freedoms (1)
- Privacy (4)
- Confidentiality (3, 7)

Russia, *Doctrine of Information Security of the Russian Federation 2016* (referred by paragraphs); See also the 2013 *Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020*

- National security in the information sphere (1-2, 20)
- Protection of the individual, society and the State against internal and external information threats (2)
- Information technology capacities used for politico-military purposes (10-12)
- Critical information infrastructure (8b)
- Dependence on foreign technologies (24-27)
- Rule of law (4)
- International law (19-20, 34e)
- Enhanced military capacity to deter, defend and respond (20-21, 23)
- Centralized coordination (6, 30-33)
- Balance between freedom of information and national security (34c)
- Human rights and freedoms (4, 8a, 35a)
- Sovereignty and political and social stability (22-23a)
- Moral and spiritual values (23j)

Serbia, *Strategy for the development of information security 2017-2020* (Referred by chapters)

- Information security (1.1, 2, 3)
- Regulatory framework (1.2)
- Cybercrime (1, 3.3)
- Protection of children (3.2.1)
- Work force development (1.1,
- Public-private cooperation (1.1, 3.1.5)
- International cooperation (3.5)
- Basic rights and freedoms (2)
- Privacy (3.2.2)

Slovakia, *Cyber Security Concept of the Slovak Republic for 2015-2020*

- Institutional framework and capability development (11-14, 16-17)
- Legal framework (15)
- Awareness (9)
- Integration to State's security system (7)
- Risk management (6, 17, 23)
- Multi-stakeholder approach (6, 9, 10)
- National and international cooperation (6, 9, 18)
- Privacy (9)
- Basic human rights and freedoms (9)
- Open cyberspace (2, 8)
- Integrity and confidentiality (23)

Slovenia, *Cyber Security Strategy 2016*

> National cyber security assurance and governance system (6, 8-9, 12) > Critical infrastructure (6, 14) > Safety of citizens (6, 13) > Defensive cyber military capabilities (6) > Awareness (10)	> Rule of law (3) > Public-private partnership (8) > International cooperation (6, 14-16)	> Privacy (7-8, 13) > Human rights and freedoms (3, 5, 13)

Sweden, A national cyber security strategy (2016)

> Information and cybersecurity (3-5) > National governance model (9-11) > Standards and requirements for services and information management (14-16) > Situational awareness (12) and incident management (19-21) > Critical infrastructure protection (18-19)	> Rule of law (4-5) > Centralized coordination (10-11, 20-21) > Sectorial responsibility and decentralized implementation (8, 10-12) > Public-private partnership (11-12) > International cooperation (28-29)	> Rights and freedoms of citizens (28-31) > International law and norms (29) > Privacy and integrity (22-24) > Confidentiality (4, 14)

Switzerland, *National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022* (in French, German, and Italian)

> Cybercrime (3) > Capacity to identify, reduce and prevent risks (8, 11-12, 18-19, 20) > Organizational structures (8) > Cybercrime (21-22) > Cyber defence (22-23) > Critical infrastructure protection (14-15)	> Risk-based approach (8) > Public-private cooperation (8-9, 18-19) > Decentralized implementation, subsidiarity (8) > International cooperation (8-9, 24-25) > Personal responsibility (17)	> Freedom, democracy (17, 24)

Ukraine, *Cyber Security Strategy 2016* (in Ukrainian)

> Information security (#1, 3) > National information security system (#1, 3, 4.2) > Critical infrastructure protection (#3, 4.3) > Cybercrime (#1)	> Rule of law (#1) > Transparency of government (#1) > Democratic control (#1) > Public-private cooperation (#1, 4.3) > International cooperation (#1) > Adherence to EU and NATO standards (#4.1)	> Civil liberties (#1)

United Kingdom, *National Cyber Security Strategy 2016-2021* (referred by paragraphs)

> Defence and resiliency (4.3, Chapter 5) > Deterrence (4.3, Chapter 6) > Industrial development (4.3, Chapter 7) > Cyber military capacity (1.10, 6.5.3) > International action (4.3, Chapter 8)	> Rule of law (4.5, > Centralized coordination (4.15, 6.2.3, 7.1.4, 7.4.3) > Multi-stakeholder approach (2.8, 4.5, > International cooperation (8.2)	> Privacy (4.5, 4.9, 8.2) > Individual rights and freedoms (4.5, 8.2) > Free, open and peaceful cyberspace (8.1, 8.4)

The Middle East and the Gulf (15 countries or authorities, 10 national strategies or policies)

Objectives and issues	Principles	Norms
Bahrain, *National Cybersecurity Strategy* (An infosheet)		
> Legislative and regulatory frameworks > Cybercrime > Critical infrastructure protection	> Centralized coordination of implementation > Public-private cooperation > Holistic approach > International cooperation	> Confidentiality, integrity > Ethical values > Rights and values of citizens
Israel, *Advancing National Cyberspace Capabilities (2011);* See also *National Cyber Concept for Crisis Preparedness and Management*		
> Establishment of cyber security authority (2, 3-7) > Regulate responsibilities (2, 8-9) > Infrastructure protection (1) > Capability and competence development (2, 3-5)	> Centralized steering (3-4) > National capacity (1, 4-5) > Exclusion of designated 'special bodies' (2)	
Jordan, *National Information Assurance and Cyber Security Strategy 2012*		
> Basic, unsystematic and insufficient information security systems and standards (4, 10-11) > National security and prosperity (6) > Information assurance and critical information infrastructure (5-6) > Legal and regulatory framework (11-12)	> Centralized coordination (18) > Public-private partnership (4) > Risk management (7-8) > International cooperation (13)	> Confidentiality (5) > Trust (6) > Transparency (9)

Kuwait, *National Cyber Security Strategy 2017-2020*

> Cybercrime (13, > Critical infrastructure protection (14, 19, 24) > Public awareness (18)	> Rule of law (28) > Centralized cooperation (25, 26) > National and international cooperation (20, 25) > Shared responsibility (27)	> Fundamental rights and freedoms, privacy (28)

Lebanon, *Lebanese National Cyber Security Policy Guidelines (2015)*

> Information and IT security (9-11) > Governance and management system (11-15)	> Confidentiality, integrity and availability of information (13-14) > Accountability and user responsibility (17-23) > Continuity of operations (43)	

Qatar, *Qatar National Cyber Security Strategy (2014)*

> Critical information infrastructure protection (10, 13) > Legal framework and regulations (11, 15) > Capability development (6-7, 12, 16)	> Rule of law (6, 11, 15) > Centralized coordination (17) > Multi-stakeholder approach (14)	> Societal rights and values (9, 17) > Privacy (5, 11, 17)

Saudi Arabia, *National Information Security Strategy 2011*

> National information security environment, framework and infrastructure (1-3, 18-20, 22, 29-30) > Integration of peoples, processes and technology (1) > Coordination and standardisation among government agencies (22) > Public awareness and workforce development (6, 12, 24-25, 37) > Information sharing (30) > Supply chain integrity (12) > Critical infrastructure protection and cybersecurity (as of being outside of the scope of the NISS) (2, 5, 80-81)	> Legal (regulative) and administrative (coordinating) frameworks (16, 18, 26-32, 77) > Multi-stakeholder approach (3, 12, 19, 35, 58-62) > National (58-62) and international cooperation (63-67) > Consensus of the top leadership (22)	> Confidentiality and integrity of information (1, 19, 28) > Transparency (2, 7, 19) > Privacy (27-28) > Trust (2, 38, 42)

Syria, *National Information Security Policy*

Turkey, *National Cyber Security Strategy 2016-2019*		
> Awareness (15, 20) > Legal and regulatory framework (20) > Critical infrastructure (17) > Information security (17-19)	> Strong central authority and coordination (21) > Integration of cyber security to national security (3, 23) > Public order (3, 8-9) > Multi-stakeholder approach (6) > Cooperation (10-11) > Risk assessment (15) > International cooperation (16)	> Privacy and confidentiality (11-12, 16) > Transparency (16) > Ethical values (16)
United Arab Emirates, *Cyber Security Strategy for the United Arab Emirates;* See also: *Dubai Cyber Security Strategy (2017)*		
> Awareness (20-21) > Information security practices (10, 13, 24) and architecture (16) > Work force development (20-21)	> Free flow of information (13) > Rule of law (16) > Collaboration of stakeholders (15) > International collaboration (15, 28-29)	> Transparency (9, > Privacy (13, 19) > International rules and norms (16)

About the authors

Dr. Mika Kerttunen and **Dr. Eneken Tikk** are co-founders of the Cyber Policy Institute, advisers to the ICT4Peace Foundation and Senior Research Scientists at the Tallinn University of Technology. **Dr Mika Kerttunen** specialises in policy and strategy processes, academic education and in the politics of international cyber security. **Dr Eneken Tikk** heads the Cyber Policy Institute's normative, power and influence studies. She holds PhD in Law and is a specialist in the development of national legislation and international cyber diplomacy.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.