Search for Cyber Norms – Where to Look?
#1 National Cybersecurity Strategies

At the UN, two working groups will be discussing responsible state behavior in cyberspace this year. Russia initiated an open-ended working group, where participation is open to all states, while the US opted for another group of 25 government experts to discuss voluntary and non-binding standards of behavior. Aiming at shared expectations towards responsible use of ICTs by States, there is hardly a better source for detecting the existence or emergence of such expectations than the cybersecurity strategies adopted since 2007, the year that led to securitization of the use of ICTs.

Finding normative aspirations in national cyber and information security strategies is possible by applying a reading to these documents that seeks to identify either explicit references to existing or aspired norms, or implicit preferences and priorities for normative action and overarching principles of national, even universal, conduct.

Strategies and policies point out principles and directions that governments claim to be adhering to or aspiring towards. They offer ways to reinforce, complement, and perhaps even correct, the current focus in the international cyber norms discourse. Principles and norms expressed in these instruments reveal promises and pleas of certainty, predictability and transparency.

A normative reading of national strategies reveals relative coherence in the leading principles that are believed to lead to reducing cyber threats and achieving cybersecurity. The majority of strategies emphasize **cooperation** in achieving both national and international cybersecurity goals. Cooperation is expected both between national authorities and stakeholders, and between authorities of different states in preventing and mitigating cyber incidents.

National strategies also send a clear message about **the rule of law in cybersecurity**, strengthening the proposition that legal certainty and predictability is needed in national and international cyber affairs. Strong emphasis on **responsibility and accountability** fortifies the proposition that the starting point for that certainty is to be found in existing law, both national and international. There is an equally strong thrive towards **public-private and multi-stakeholder formulas** of cybersecurity that involve the private sector, users and academia alongside governments.

Strategies are less coherent when it comes concrete calls for normative action. Perhaps the single most important observation, in this context, is heavy emphasis on **privacy and confidentiality**, something that has not been discussed in the UN GGE or the Global Commission on the Stability of Cyberspace.

By way of critique, normative pleas in cyber security policies do not indicate the level and quality of following those norms and principles. It is difficult to dissect a uniform understanding of the concepts – something that might inform the implementation of the part of the UN and OSCE mandates of clarifying relevant national concepts. For example, the principle of multi-stakeholder approach can be understood either as harnessing the private sector and academia to support governmental activities or as the private sector, academia and civil society participating in policy formulation and implementation. However, different national approaches and experience will be valuable for pointing out possible modalities of implementing the recommendations of the 2014-2015 UN GGE.

To build coherence and uniformity on responsible state behavior, the international cyber norms discussion must be informed by national cybersecurity strategies as the first-hand instruments of directing and guiding solutions to critical national cybersecurity issues.

	Region[1]					Score
	Africa	**Americas**	**Asia-Pacific**	**Europe**	**Middle East**	
Principles[2]						
Cooperation	9	11	13	31	4	**68**
Rule of law	7	6	9	28	3	**53**
Coordination	5	5	7	19	5	**41**
Multi-stakeholder approach	3	6	6	20	4	**39**
Public-Private Partnerships	7	6	3	13	-	**29**
Norms[3]						
Privacy	5	7	8	21	4	**45**
Confidentiality	4	2	5	17	3	**31**
Freedom of information and transparency	2	3	5	3	-	**13**
Integrity of information	1	-	4	2	1	**8**

Table 1. Barometer of norms and principles in national cybersecurity strategies

[1] Countries are grouped into five geographical regions: 1) Africa, 2) the Americas, 3) Asia and the Pacific, 4) Europe, 5) the Middle East and the Gulf.

[2] The notion of principle refers to *general, antecedent and foundational assumptions of the state or organizing mode of affairs.*

[3] The notion of norm refers to *expectations of behavior or desired state of affairs*.

Summary of a Normative Reading of National Cybersecurity Strategies
(report forthcoming in 2019)

Tikk & Kerttunen

	Principles[4]	**Norms**[5]
Africa	Cooperation (9)[6] Rule of law (7) Private-Public Partnership (7) Coordination (5) Responsibility (4) Harmonization, integration, unity, holistic agenda (4) Multi-Stakeholder Approach (3) Framework of governance (3) Risk management (2)	Privacy (5) Confidentiality (4) Human rights and freedoms (2) (Intellectual) property (2) Availability of information (2) Dignity (2)
	Also mentioned: Prioritization, balance between Human Rights and security, protection of vulnerable groups, Integrity, universal access to cyberspace, social justice, transparency of governmental actions, good governance, gender equality, freedom of expression	
Americas	Cooperation (11) Multi-Stakeholder Approach, limited government role (6) Rule of law (6) Responsibility (5) Coordination (5) Private-Public Partnership (3) Leadership (2) Proportionality (2) Sustainable development (2)	Privacy (7) Human rights (6) Transparency (3) Democracy (2) Confidentiality (2)
	Also mentioned: International frameworks, technical rules and standards, self- and collective defence, risk management, integration, governance, information sharing and sensing, deterrence, Freedom of speech, protection of personal property, Internet neutrality, free and open cyberspace, conflict prevention, peaceful settlement of disputes, cooperation, accountability, cultural diversity, proportionality	
Asia	Cooperation (13) Rule of law (9) Coordination (7) Private-Public Partnership (6) Multi-Stakeholder Approach (6)	Privacy (8) Confidentiality (5) Integrity (4) Freedom of information (3) Human rights (3) Freedom of speech (2) Availability (2) Autonomy in management (2)
	Also mentioned: Resilience, mobilization of social resources, sovereignty, shared governance, peace and stability, deterrence, standardization, order, non-use of force, democracy, collective responsibility, diversity, peaceful settlement, open cyberspace.	
Europe	Cooperation (31)	Human Rights (25)

[4] The notion of principle refers to general, antecedent and foundational assumptions of the state or organizing mode of affairs.
[5] The notion of norm refers to expectations of behaviour or desired state of affairs.
[6] The number in brackets indicates how many strategy or policy documents emphasized the principle or norm in question.

	Rule of law (28) Multi-Stakeholder Approach (20) Coordination (19) Private-Public Partnership (13) Responsibility (6) (shared, personal) Subsidiarity (5) International Law (3) Risk-based approach (3) Self-regulation (2) Harmonization with western/EU/NATO rules and standards (2) Democracy (2) Proportionality (2)	Privacy and informational self-determination (21) Confidentiality (17) Trust (4) Free cyberspace (4) Democracy (3) Proportionality (3) Freedom of expression (3) Integrity (3) Open cyberspace (2) Personal responsibility (2) Peaceful cyberspace (2) Equality (2) Freedom (2) Transparency (2) Self- and collective defense (2) Freedom of information (2) Subsidiarity (2)
	Also mentioned: Complementarity, integrated national defense, active defense, leadership, security and privacy by design, confidentiality, civil-military cooperation, integrity, balance between privacy and law enforcement, transparency, balance between freedom of information and national security, multi-disciplinary approach, integration of diplomacy, development and self- and collective defense, military defensive and deterrence capacity, tolerance, moral and spiritual values, collective engagement, self-regulation in management, public int'l law, sovereignty, political and social stability	
Middle East	Coordination (5) Cooperation (4) Multi-Stakeholder Approach (4) Rule of law (3) Risk management (2)	Transparency (4) Privacy (4) Confidentiality (3) Trust (2)
	Also mentioned: Integration in national security, public order, societal rights and values, ethical values, integrity of information	

Table 1. Principles and norms as expressed in national cyber and information security strategies and policies. Authors' compilation.