RESEARCH IN FOCUS

Strategically normative. Norms and principles in national cybersecurity strategies

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

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

It is hard to overestimate the role of a national cybersecurity or information security strategy. Balancing between infinite ambitions and finite resources, these instruments legitimise demands, level expectations and reinforce rights and freedoms. Strategies constitute effective administrative tools to create a division of responsibility and labour between governmental agencies and between the public and private sector. This paper applies a normative reading to 106 national cybersecurity strategies, most of them adopted after the cyberattacks against Estonia in 2007, an event that marked a strong shift toward securitisation of the use of information and communication technologies (ICTs). The paper identifies and discusses countries' qualifications of afforded and expected standards of behaviour in the context of both national and international cybersecurity. The analysis is intended to contribute to the international debate around cybernorms and responsible behaviour in state use of ICTs.

Key points

- National strategies inform domestic and global audiences of the normative foundations and goals of governmental policies.
- Such information is essential for developing understanding of mutual expectations of responsible behavior, formulating positions for regional and global negotiations and calibrating capacity building in the field.
- Countries need to study what other governments are doing and why. Such mutual learning, supported by regional organisations and academic communities, improves the overall awareness of similar challenges and issues that states have to address amid contingent ambitions and resources.
- Better awareness and understanding may lead to better appreciation of differing approaches and ultimately contribute to international peace, security and stability.

Acknowledgements

The authors thank Aapo Cederberg, Xymena Kurowska, Marja Lehto, Eric Luiijf, Patryk Pawlak and Agnieszka Wierzbicka for their critical and constructive comments. All errors, omissions or unconventional views are the authors' own. In addition to the available strategies themselves, our analysis, conclusions and recommendations are based on exchanges with experts we had the opportunity to meet thanks to the cybersecurity capacity building of the ICT for Peace Foundation and the George C. Marshall European Center for Security Studies. We are grateful to these organisations for providing us with direct access to hundreds of national information and cybersecurity experts. The rich body of views and experiences they represent - from the biggest of nations to the some of the tiniest, all keen to develop national cyber resilience and prowess - provided a valuable sounding board for our thinking and conceptual analysis.

Introduction

Boundaries of responsible state behaviour are being drawn even amid claims of the internet as a lawless space, the international information infrastructure as a highway without traffic rules and international law as a contested or even rejected framework for addressing cyber threats, conflict and war. Guidance for behaviour may be found in numerous clues: state practice delineates the tolerable and intolerable, from how governments handle significant cyber incidents to how they design their technological (in)dependence. Court rulings may likewise apply beyond their original scope, clarifying particular questions but also articulating broader societal values and context. National legislation indicates areas and issues where certainty and predictability are required. Yet, any argument or proposed measure leans on the foundational values and belief system of the state actor in question. National cybersecurity strategies present an illustration of the values and beliefs of an increasing number of states.

The analysis presented in this paper provides a conceptual and contextual normative reading of over a hundred national cybersecurity and information security policies and strategies.[1] It focuses on normative goals, foundations and guidance expressed in national cybersecurity and information security strategies. The authors identify principles and specific norms governments are adhering to, or advancing, as points of departure for the development of national and international cybersecurity norms. An evaluation of the feasibility or implementation of the political, normative or technical objectives promoted by individual states is beyond the scope of this paper. Our main findings are presented and discussed below, and a more detailed account of national policy documents is presented in the Annex.

Although other governmental documents - policies and strategies - may contain similar guidance and information, issuing national cyber or information strategies has become standard; in our mind it should become a norm of expected and responsible behaviour. National cyber or information strategies, alongside a handful of specific international cyber strategies, offer a argued, consolidated and substantiated view of national policies. Moreover, as the documents by default focus on security issues, they contain guidance and information essential across administrative and jurisdictional boundaries.

The analysis covers 193 United Nations member states and three countries or authorities outside of the UN system, all grouped into five geographical regions. As of February 2019, 106 states had issued a national cybersecurity (or information security) strategy (or doctrine, plan, policy or program). The majority of them have published an official document, but in a few cases the analysis is based on summaries and presentations given by high-ranking officials.

1. Evolution of national cyber strategy: the shift toward security

After the 2007 cyberattacks against Estonia, a significant shift occurred in national and international information technology policy. Until then, government efforts had focused largely on digital agendas, the development of information societies and countering cybercrime. After the attacks, this rather narrow and precise focus on data protection, information assurance, information security and critical infrastructure protection was subsumed by the wider, and more opaque, concept of *cybersecurity*. Digital and information security agendas became subordinate to cybersecurity. Further proliferation of, and reliance on, smart and connected technologies only accelerated the quest for security.

[1] Most governments label these documents and programs strategies, but doctrines, plans and concepts that contain similar legitimising, guiding and informing force are equally objects of the study.

In just a few years, digital technologies became framed in terms of peace and war, arms control and politico-military affairs. Accordingly, national cybersecurity strategies became ordinary measures for addressing "extraordinary" political and technical circumstances.[2]

The first generation of cybersecurity strategies led some analysts to observe differences in understanding what cybersecurity is about, unclear relationships between the strategies and other information technology policies as well as a lack of a dynamic approach to cyberspace threats and challenges. National approaches also lacked explicit methodology and criteria addressing tactical and operational plans.[3] Indeed, cybersecurity has been defined and approached differently throughout national strategies, as depicted by a sample of earlier and contemporary documents in Table 1 of the Annex.[4] However, regardless of their definition or framing of cybersecurity, all strategies signify a clear shift toward security as the leading consideration of digital development.

Most national cybersecurity strategies have inherited the pre-cyber era's focus on basic information security and network protections. Over time, as dependence on ICTs has increased, strategies have come to offer insights into immediate national defence concerns and priorities. Acknowledging that such imperatives cannot be supported by solely public means, strategies contain complex administrative, economic, operational and normative ambitions and mechanisms.

Some governments have, in addition to national positions, taken explicit stands on international cybersecurity, including cross-border cooperation, capacity building and global normative processes. Each of these instruments depicts a variant of international cybersecurity governance, similar in name but very different in details and implementation. These strategies are introduced in Table 2 of the Annex.

Over the past dozen years, 106 states have adopted national cybersecurity or information security strategies. More than half of the members of the international community of states have spoken about their concerns and solutions when it comes to the question of ICTs and security. The main interest of the authors lies in evaluating normative aspirations and instructions in national strategies. Approximately half of the national strategies were issued before 2015. These countries, many of them

---

[2] Strategy can be understood as a pattern or method of thinking, an administrative process or a manifestation of policy in the form of an issued instrumental document. Strategic thinking refers to calculation between ends, ways and means; balancing between desired objectives and available resources, writ large. Strategy as an administrative process constitutes organised work to define objectives and design overarching and long-term policies and action plans as well as implement, steer and improve such policies and plans. The purpose of issuing strategy is to inform and educate domestic and foreign audiences; provide political guidance by articulating objectives, choosing priorities and allocating resources; and legitimise the direction and content of taken policy. On strategy and strategies see Colin S. Gray, *The Future of Strategy* (Cambridge: Polity, 2015), pp. 23-42; Lawrence Freedman, *Strategy* (Oxford: Oxford University Press, 2014), especially page xii on strategy as "the central political art" and "the art of creating power"; and John Lewis Gaddis, *On Grand Strategy* (New York: Allen Lane, 2018).

[3] Eric Luiijf, Kim Besseling, Maartje Spoelstra & Patrick de Graaf, "Ten National Cyber Security Strategies: a Comparison", *CRITIS 2011 - 6th International Conference on Critical Information Infrastructures Security*, September 2011, also Eric Luiijf, Kim Besseling and Patrick de Graaf, 'Nineteen national cyber security strategies', *International Journal of Critical Infrastructure Protection*, Vol. 9, No. 1/2 (2013), pp. 3-31. The website *CIPedia* that follows developments in critical infrastructure development and resilience and which also maintains a registry of national cybersecurity strategies (https://publicwiki01.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy). The Global Forum on Cyber Expertise report "Global Agenda for Capacity-Building" discusses the role of national strategies (November 2017; p.6).

[4] It is essential to notice the difference between the notions and the use of the notions of *cybersecurity* and *information security*. In the West, in general, cybersecurity is seen as a broader concept encompassing also information security. Information security is then operationalised as the preservation of confidentiality, integrity and availability (C-I-A) of information. For many countries, information security functions as the umbrella concept also including questions regarding the content of information and, for example, the notion of *media sphere*. Some national policies named information security doctrines or strategies take the C-I-A approach, some the more inclusive approach.

obviously rather advanced, need to renew and update their policies in the coming years.[5] At the same time, many developing countries are working to formulate their first consolidated positions on cybersecurity and information security. National policy formulation and renewal, being a constantly ongoing process, invites countries and regional organisations to find cooperative resilience, capacity building and capability development solutions.

2. Normative relevance of national cybersecurity strategies

Normative trends and directions in national cybersecurity strategies have not received wide attention.[6] Some states have made reference to their national cybersecurity strategies in submissions to the First Committee. They have not been discussed at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). This is regrettable as national strategies point out distinctions between proper and improper behaviour, the alleged focus of the international cybersecurity dialogue.

Although only a few strategies make explicit reference to international law or norms processes, all strategies express accepted or expected standards of behaviour. Applying a normative reading[7] to these documents allows identifying principles and norms, promises and pleas of certainty, predictability and transparency of societal and international relations in their area of regulation. At times when the meaning, and even the existence, of legally binding norms or guides of behaviour in this domain is contested, these leads reveal ways to eliminate prejudice in international cyber affairs. Thus, national cybersecurity strategies offer a reading of norms that complements, verifies and perhaps even corrects the focus of the international cybernorms dialogue. In this context, exchange of information regarding national policies, doctrines and legislation plays an important role in normative processes and is a confidence-building measure.[8]

“

Although only a few strategies make explicit reference to international law or norms processes, all strategies express accepted or expected standards of behaviour.

Seen through the lens of national strategies, cybersecurity is a normalizing activity that does not call for a global convention, new norms or *a priori* debates of the applicability of international law. The politico-societal anchorage of national cybersecurity strategies indicates that cybersecurity, despite the cognitive, technical and performance challenges associated with it, has become a mainstream function

[5] As a rule of thumb, we recommend countries review their strategies four years after implementation and issue an updated strategy every six years. These milestones allow time to implement but enforce assessment, review and renewal. National administrative and political realities obviously trump this observation.

[6] A notable exception is Väljataga's analysis of the national strategies of seven significant cyber powers (Ann Väljataga, Tracing opinio juris in National Cyber Security Strategy Documents (Tallinn: CCDCOE, 2018). A comparative, albeit not legal, analysis of the EU and NATO member-state strategies was conducted by Štilitis, Pakutinskas and Malinauskaite in 2016 (Darius Štilitis, Paulius Pakutinskas and Inga Malinauskaite, "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis", Security Journal Vol. 30, 4 (2016), pp. 1151-1168.

[7] In our reading, the notion of *objectives and issues* refers to key areas, concerns and objectives a government has stated in the analysed document. *Principles* refers to general, antecedent and foundational assumptions of the state of affairs or their organising mode; and *norms* 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. That some expressions do appear in two or even three categories (objectives and issues; principles; norms) follows from the contextual reading of how governments have used these expressions and what they mean by certain words. For example, 'transparency' may be an objective; an sought-after state of affairs; or a norm, depending on the actual circumstances of usage.

[8] We owe this observation to Patryk Pawlak.

of national action. The strategies adopted so far represent a collection of functional activities and instruments containing political, societal and financial consequences as any other political and administrative activity or instrument. They introduce a collage of challenges that requires attention and action by all stakeholders. In their uniformity, strategies argue "why" and dictate "how" cybersecurity is to be harnessed.

The evolution and proliferation of national cybersecurity strategies has several normative implications. Normative pointers in national strategies indicate (a) where states are accumulating normative efforts at the national level and, consequently, where burden-sharing can be considered between national and international level regulation; (b) where states strive for additional normative clarity and certainty that should be achieved and supported by both national and international regulatory mechanisms; and (c) how the normative guidance of regional and international organisations could be, and is, implemented.

National cybersecurity strategies introduce a range of normative goals and means that can be compared to those promoted in the international cybersecurity dialogue of norms, rules and principles of responsible state behaviour. For example, cooperation, first in the line-up of recommendations of the 2014-2015 UNGGE[9], is normally regarded as essential in national cyber strategies. Even a superficial reading of strategies informs the reader about the main modalities of required cooperation (international, regional, interagency and public-private). Cooperation and coordination are expected and ordered at the national and international levels, regionally and in communities of interest. There is hardly a strategy or policy instrument that does not make reference to the need for cooperation and offer guidance and direction for joint efforts. This is essential as it counterbalances the otherwise dominant claims of a lack of shared views and common understanding. Emphasis on cooperation underscores the ideal of ICTs as tools of normal communication as opposed to adversarial and bipolar relations.

"

The politico-societal anchorage of national cybersecurity strategies indicates that cybersecurity [...] has become a mainstream function of national action.

The majority of national cybersecurity strategies explicitly express and factually subscribe to the rule of law. This practice signifies the normative aspect of a national strategy in two senses: as a political ideal vision and objective and, perhaps most importantly, as a penetrating regulatory foundation. There is also an important implication in this shared wording of a rather uniform expectation of increased certainty and predictability in international cyber affairs, something that the UNGGE has so far not been able to offer. References to the rule of law put pressure on the upcoming UNGGE and open-ended working group, as well as other venues, to come up with substantive proposals aimed at resolving political tensions and differences among strategic contestants.

The normative terrain of national cybersecurity strategies is far from flat. Several countries, many of them in Africa, the Caribbean and Central and South America, in their formative phase of cybersecurity policy development, are only starting to design their legal and institutional frameworks. Meanwhile, countries in the European Union and, more generally, technologically more advanced states, are in very advanced stages of applying legal and policy instruments in the service of advanced and nuanced national goals and ambitions. Regardless of the exact stage of development, such work requires thorough politico-normative discussions within governments and debate within societies. Governments are also looking for practical guidance, which global and regional initiatives and their state or private partners could provide. However, this does not prevent governments from coming up with the same objectives and premises of national cybersecurity, such as centralised coordination, accountability or reference to human rights and liberties. These handles can be found in the strategies of small and big

[9] Paragraph 13 (a) of A/70/174.

states, in those that are technologically advanced and least-developed, in the North and the South, and in all time zones.

Occasionally, normative directions are contradictory. For example, countries *in verbatim* subscribe to constitutional guarantees of civil liberties, as well as international law. Many of these governments are nevertheless conducting cyber operations, implementing security practices and supporting principles that undermine those constitutional and even universal guarantees. In line with the chosen securitisation argument, deviations are claimed to be of necessity, as if there weren't any other options.[10] Undermining of agreed-upon international obligations and constitutional commitments takes place on all continents.

To respond to those states that remain sceptical about the trend of securitisation, it is worth pointing out the recent activities of the UN Secretary-General. Mr Guterrez has pointed out that the scale and pervasiveness of cyber insecurity and actors adopting offensive postures could "weaken the delicate balance and system of reciprocity that underpins much of the contemporary international security architecture". In particular, the Secretary-General wants to deepen understanding of how new technologies can be used "to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws".[11]

The UNGGE reports have addressed numerous issues overlapping with those addressed in national strategies, e.g. attribution, exchange of incident information, international political and technical cooperation, human rights, vulnerabilities, supply chain security and the culture of cybersecurity. As the UNGGE reports seek to provide guidance on the applicability of international law and recommendations of responsible state behaviour, connecting these efforts with national strategies, practices and lessons would create much-needed connections between international- and national-level efforts to secure the ICT environment. Currently, no national strategy or doctrine explicitly defines or guides how any of the UNGGE recommendations should or could be implemented, which indicates a disconnect between national and international efforts.[12] Some countries have endorsed the 2015 UNGGE report and the recommendations in bilateral or group statements, including Australia, China, the US and the G7.

For many nations, the more acute issues than the international normative vacuum are national (in)security and capability development. This underscores the direct relevance, for national development, stability and security, of the recommendations agreed upon in the UNGGE. It is also an opportunity for the next UNGGE or the open-ended working group to invite governments to make explicit reference or links to the work done in the UN and create mutual consideration and trust between the UN and national efforts. The same gauntlet can be thrown to other organisations and regional champions - as Table 3[13] indicates, states are looking to regional organisations for guidance and coordination.

To sum up, national strategies identify and offer further food for the broader discussion of norms, principles and responsible state behaviour. Statements of normative significance and representations of moral and normative value positions serve as potential input factors indicating dedicated adherence to national or universal values and principles. Investigating national policy documents reveals both contingent national and common global preferences.

[10] Personal observations.

[11] United Nations, *UN Secretary-General's Strategy on New Technologies* (September 2018).

[12] UNGA, Developments in the field of information and telecommunications in the context of international security (A/70/174 (22 July 2015)). Australia's International Cyber Engagement Strategy (2017) does mention the 2015 recommendations (Annex B) but without the explicit guidance expected from a strategy.

[13] See Annex.

3. Recurring normative pointers

Figure 1 summarises the most commonly sought-after, and promoted, principles and norms contemporary national cybersecurity strategies build on and advance[14]. These and other norms and principles can be argued to constitute normative foundations of responsible state behaviour and may help to further outline criteria of and boundaries for what is tolerable and intolerable. A more thorough analysis of similarities and differences between national conceptions is not provided in this paper.

Compiling this baseline list was not without methodological challenge - "accountability", for instance, also includes more nuanced references to enforcement and responsibility. The latter, depending on national priorities and focus, can be individual or collective, and point to the government or to the private sector. "Cooperation" is grouped with "collaboration" and, at the same time, does not distinguish between various (and sometimes separately emphasised) levels of preferred cooperation (international, regional, interagency and occasionally also between the government and the private sector, thus marginally overlapping with public-private partnerships). "Harmonization" covers references to holistic and unified agendas, and occasionally also integration of national, international and regional efforts and instruments with national goals and ambitions as well as strategies themselves. "Centralization" can refer to concentration of not just management but also response, capabilities, planning, coordination, implementation or leadership.

"

However, no national strategy can exist and be read or interpreted in a vacuum. Successful cybersecurity requires governments and societies take a comprehensive approach.

What stands out in national strategies is heavy emphasis on privacy and confidentiality - the topics currently outside the mandate and focus of the international cybersecurity dialogue. As national strategies indicate, there seems to be a strong and strict connection between cybersecurity (at least at the national level) and privacy, and, consequently, a shared concern about espionage and surveillance practices of both states and non-state entities. National strategies also draw a very clear link between cybersecurity and human rights, another topic so far addressed in the UNGGE only by reference. Some national strategies also address the rights of certain minority groups. These connections deserve additional analysis and attention in future work on norms, rules and principles.

Although normative emphasis on, for instance, transparency, trust, accountability or autonomy is less frequent, several strategies provide insights into how states understand and apply relevant standards of behaviour. In addition, national strategies quite often refer to general guidelines and lines of action - such as situational awareness, forensic capability development and workforce education - that can further guide the implementation of various norms, rules and principles.[15]

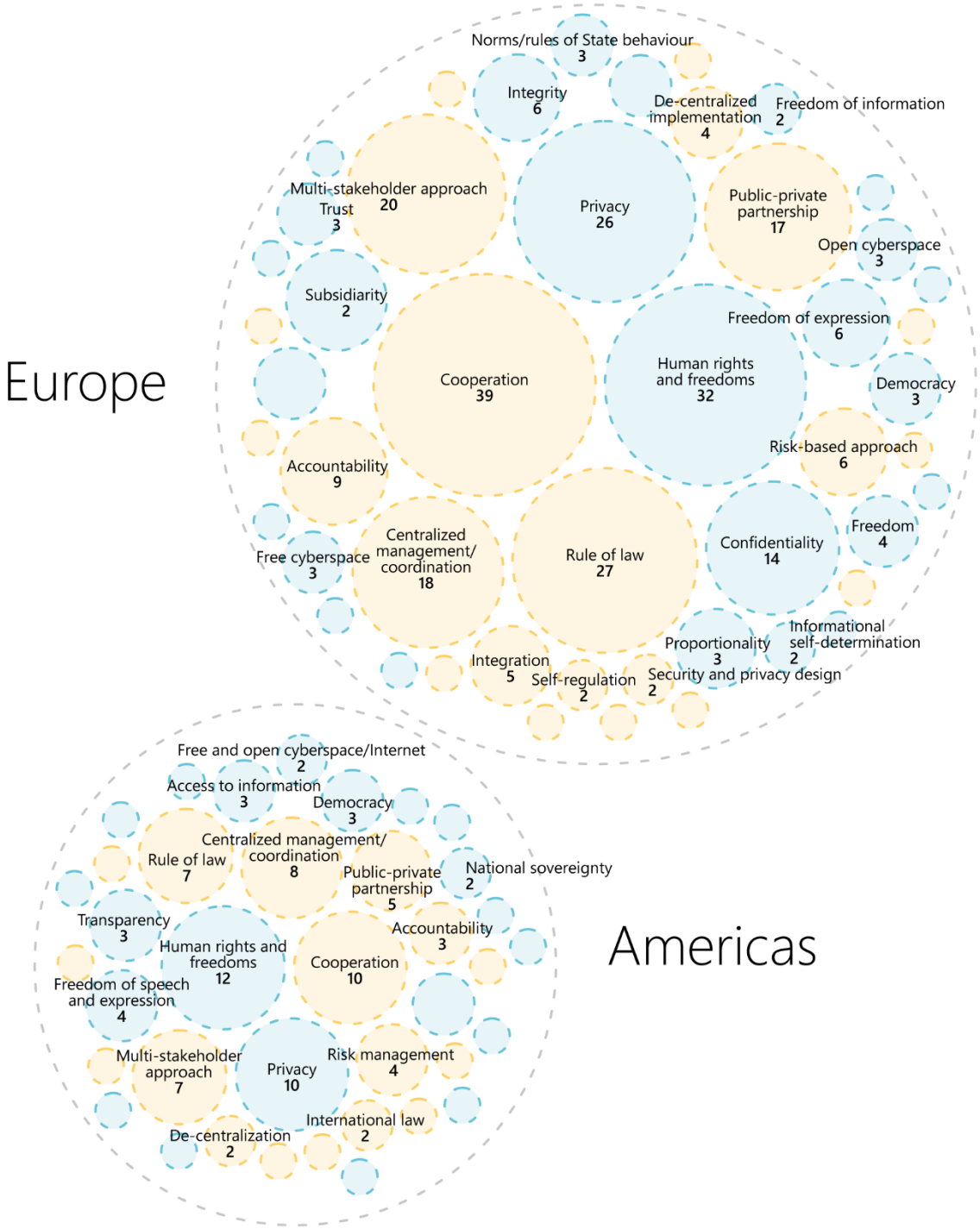
By way of critique, normative pleas in cybersecurity policies hardly speak to the level and quality, let alone sincerity of following, those norms and principles. Neither is there any uniform understanding of the concepts. For example, the principle of multi-stakeholder approach can be understood either as harnessing the private sector and academia to support governmental activities or as the private sector, academia and civil society equally participating in policy planning and implementation.

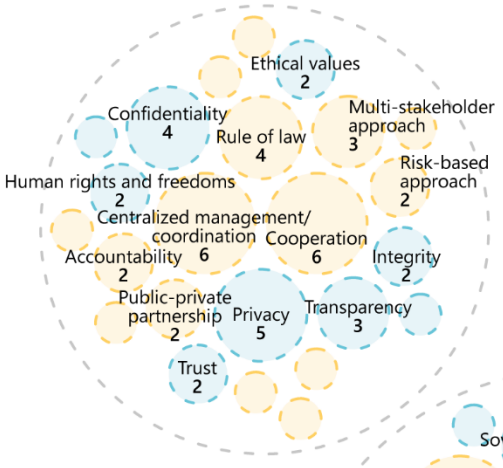
[14] For more information, please see Table 4, Annex.

[15] Similarly, the Commonwealth Telecommunications Organisation lists four guiding principles that represent recommended lines of action: *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015), pp. 5-9 and Table 1.

PRINCIPLES AND NORMS

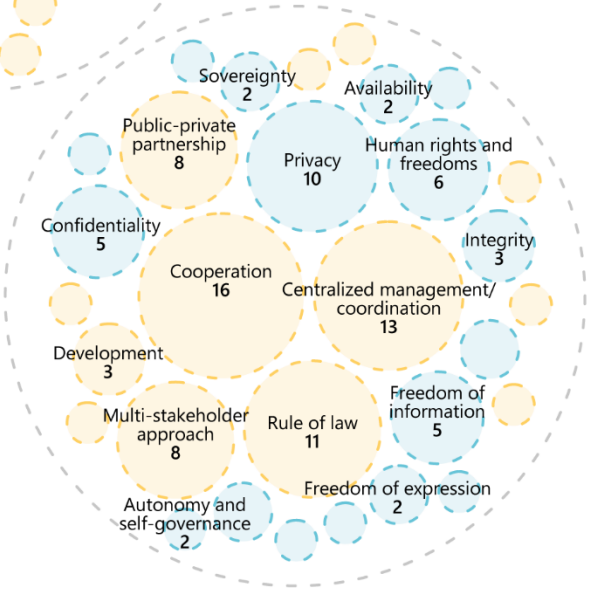
AS EXPRESSED IN NATIONAL CYBER AND INFORMATION SECURITY STRATEGIES AND POLICIES



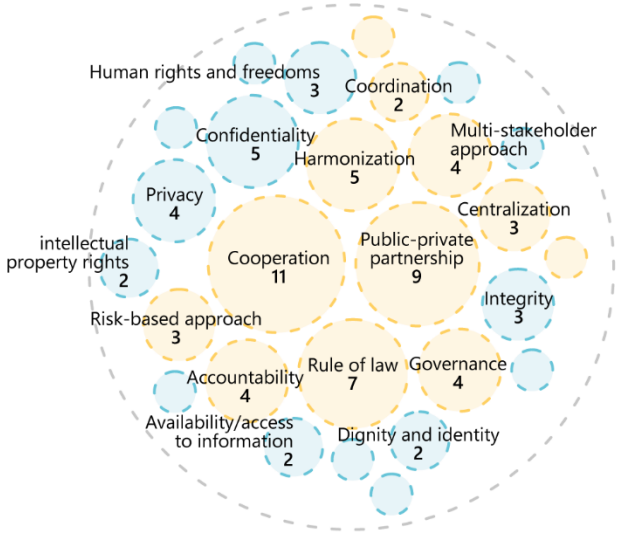


Middle East and the Gulf

Asia and Pacific



Africa



Similarly, the ideal balance between privacy, freedom of information and national security, often simultaneously emphasised, remains unspecified. Neither has the notion of rule of law been operationalised.[16] However, no national strategy can exist and be read or interpreted in a vacuum. Successful cybersecurity requires governments and societies take a comprehensive approach. In addition to explicit regulations and standards, such an approach will often involve other strategies - such as the development of information technology, information society or e-commerce - and supporting legislation on, for example, data protection, network monitoring and intelligence and cybercrime. Governmental policies and national legislation across the field must remain balanced. Fundamental rights and civil liberties online cannot be stronger than they are offline, yet they cannot lag behind either. Any imbalance between online and offline rights would create double standards and loopholes, undermine public trust and damage the credibility - even legitimacy - of the State.

4. Strategy as a norm

National cybersecurity strategies have a normative value on their own. A national cybersecurity strategy can be regarded as one of the most thorough normative moves a nation and government can take in the context of cybersecurity. Countries having a properly drafted, thoroughly discussed and orderly adopted and implemented strategy could itself be regarded a norm, a justified expectation of state responsibility and transparency. The requirement of a national strategy has been acknowledged in the African Union and the European Union. The African Union Convention on Cyber Security and Personal Data Protection requires parties to develop a national cybersecurity policy and adopt strategies to implement it.[17] Likewise, the NIS Directive of the EU states that "to achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented"[18] - an objective that the European countries have successfully achieved. The Directive defines national strategy on the security of network and information systems as a starting framework providing strategic objectives and priorities regarding the security of network and information systems at national level.[19]

The fact that 106 governments have issued an explicit national cybersecurity strategy should not overshadow the fact that close to 90 states still have not formulated or published explicit cybersecurity or information security policies. It should be noted that many governments have issued information technology, digital development and e-government and e-commerce policies and programs wherein cybersecurity and information security have briefly been touched upon. The fact that many countries have not formulated a cybersecurity strategy leads to the critical question of why their governments have been unable or unwilling to make such a comprehensive, transparent and explicitly transforming move. As there is no one model or level of strategy, the claim of impotence does not seem credible. A variety of strategies - covering information security or international peace and security, empowering key governmental agencies or all of society - have been issued by the strongest of nations and the smallest of countries. That the governments have deliberately avoided issuing a strategy would, on the other hand, suggest a paradoxical claim that the very normative character of cybersecurity strategies inhibits their adoption. For the advocates of rule-based and transparent political and legal orders, such

[16] The Swedish governmental inquiry for proposal on cybersecurity provides a thorough example of the comprehensiveness and level of detail a national cyber security strategy process can entail when the principle of rule of law is taken seriously (Sweden 2015), p. 23. Obviously a 338-page-long inquiry can express much more than much shorter strategies, but the point here is that to be able to eventually write a concise strategy, one has to master both the whole and the details.

[17] African Union Convention on Cyber Security and Personal Data Protection (EX.CL/846 (XXV)), Article 25.

[18] NIS, Recital 29.

[19] NIS, Article 4 (3).

political reluctance is nevertheless alarming. It supports and prolongs low levels of cybersecurity, ineffective administrative performance and opportunistic politics.

States have a variety of reasons to defer from issuing national cybersecurity strategies.[20] First, a rather commonly heard argument is that a government does not possess the necessary intellectual, financial and technical resources to issue and, most importantly, implement a strategy. For some, survival or providing electricity for the majority of the population are more urgent national goals. Second, perhaps surprisingly often national experts are skeptical of the narrative surrounding cyber threats, and claim that "cybersecurity is being pushed upon" them. Third, there are also different levels of tolerance of sub-security: some states are willing to accept higher levels of risk than others. Admittedly, despite cyberspace being shared and common, countries face very specific problems, challenges and threats. Fourth, some countries have created very advanced levels of security by adopting sector-by-sector security measures, without sensing a need to establish a unified national and published policy. These countries are typically more advanced when it comes to general and advanced levels of education, as well as research and development, thus reducing the need to have an all-encompassing policy. We have observed that many governments, having maintained this approach, now have started to issue national strategies. Fifth, some governments hesitate to commit to a comprehensive and penetrating policy that would likely change some domestic power structures, reveal bad governance and corruption and expose national practices to external observers. What is truly alarming is that, in some cases, governments have received inappropriate ''international" guidance pushing for overly ambitious or premature measures. These countries now have a model cybersecurity strategy that they can't implement. Domestic disputes can lead to political impasses and indecision, blocking significant national advancement in cybersecurity. Finally, perhaps most controversially, we have noticed political calculations in which governments wait for, or even expect, other stakeholders, international partners or international agreements to solve their national cyber issues. On the other hand, international outreach may decrease cyber threats originating from nations to which the international outreach is made.

National cybersecurity strategies have a normative value on their own. A national cybersecurity strategy can be regarded as one of the most thorough normative moves a nation and government can take in the context of cybersecurity.

In this context, it is also essential to share how we know what we do of the existence of national strategies. When conducting this study, we initially used three renowned resources that track national cybersecurity strategies and policies: NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) library, the United Nations Disarmament Research Institute (UNIDIR) *Cyber Policy Portal*, and the CIPedia national strategy database.[21] The databases did not explain their methodologies in detail and ended up offering very different accounts of national strategies. (The number of identified strategies varied from 64 to 124.) Eventually, we expanded our own, also imperfect, collection of research and observations into an database containing not only national cybersecurity strategies but also information technology, information and communication technology, e-society and military strategies, doctrines, action plans and manuals.

[20] This analysis is based on our observations of strategy processes and discussions with national, regional or thematic experts. We defer from naming their names in this section.

[21] CCDCOE library available at https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies; UNIDIR *Cyber Policy Portal* available at: https://cyberpolicyportal.org/en; and CIPedia database available at https://publicwiki-01.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy.

5. Conclusion

Norm-based international order and norm-based state behaviour in cyberspace provide a better guarantee of a peaceful, secure and open Internet and cyber domain than any other conceptual alternatives: hegemony, "Balkanisation" or lawlessness.[22] Anchoring national cybersecurity strategies to norms and principles such as rule of law, privacy, cooperation and confidentiality, to name but a few, is an important first national step toward establishing better predictability and certainty in international cyber affairs.

Following Krasner,[23] Katzenstein[24] and Finnemore and Hollis,[25] norms can be defined as expectations of certain behaviour in a group with a shared identity. This understanding stems from social theory and the liberal-institutional school of thought.[26] It operates with ideational ontology, concepts and factors, and assumes and builds on shared identities, mainly economic interdependency and international cooperation. This cultural anchorage underlies particular, nationally and regionally based approaches. Therefore, while reading and interpreting national cybersecurity and information security strategies it is important to keep in mind the local context and values which have driven their development.

Domestic political and administrative communities have sufficiently shared, homogenous or functional norms to initiate change and set expectations of agent behaviour. On the other hand, the international system is often governed by self-interest and coercion and autonomous and materialistic state behaviour is common.[27] Yet, sufficient foundational basis to recognise principles and norms of responsible state behaviour can be found or established in regional, sub-regional and national approaches. Normative moves in national strategies do matter.

Organisations such as the Organization for Security and Cooperation in Europe (OSCE), the Organization for American States (OAS), the African Union (AU), the Economic Community of West African States (ECOWAS), the Association of Southeast Asian Nations (ASEAN), the Shanghai Cooperation Organization (SCO), the North Atlantic Treaty Organization (NATO) and the European Union (EU) have taken or are taking determined and nuanced political, administrative and normative approaches to regional and international cybersecurity. Five United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security have studied and provided politico-normative guidance on issues such as the applicability of international law, confidence-building measures and recommendations for norms, rules and principles

[22] Hegemony refers here to a single state or otherwise unitary actor occupying a dominant position with power to determine the direction and development of cyberspace, Balkanisation to cyberspace being split into separate nationally or block-regulated spaces, and lawlessness to a condition where cyberspace and state behaviour in cyberspace are not bound by any binding laws or rules. These scenarios are often used as political tools and warning signs rather than as foundationally sound arguments.

[23] Stephen D. Krasner, "Structural causes and regime consequences: regimes as intervening variables", *International Organization* 36:2 (Spring 1982).

[24] Peter J. Katzenstein (ed.), *The Culture of National Security. Norms and Identity in World Politics* (New York, NY: Columbia University Press, 1996).

[25] Martha Finnemore and Duncan Hollis, "Constructing Norms for Global Cybersecurity", *American Journal of International Law* 100:3 (2016)*; Temple University Legal Studies Research Paper* No. 2016-52, https://ssrn.com/abstract=2843913. See also Martha Finnemore and Kathryn Sikkink, "International norm dynamics and political change", *International Organization* 52:4 (1998), pp. 887-917.

[26] In addition to Katzenstein (1996) *op.cit.,* normative landmark works on regimes and norms include e.g. Robert Keohane and Joseph S. Nye, *Power and Interdependence* (Boston, MA: Little, Brown, 1977) and Martha Finnemore and Kathryn Sikkink, "International norm dynamics and political change", *International Organization* 52 (Autumn 1998), pp. 887-917. On the epistemic assumptions on norms see Roland. L. Jepperson, Alexander Wendt and Peter J. Katzenstein, "Norms, identity, and culture in national security", in Katzenstein (1996), pp. 33-75.

[27] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), p. 2.

of responsible state behaviour in cyberspace.[28] All these processes can be informed, and fortified, by references to relevant national approaches.

As evidenced by this paper, countries are actively seeking to stabilise their activities and functions in cyberspace and increase certainty and predictability in both national and international cyber affairs. Globally, the current goal is adoption of voluntary non-binding norms of responsible state behaviour and states have been requested to implement the normative recommendations of the UNGGE. Whether the UNGGE has captured all normative leads, or whether states will accept all proposals made, remains to be seen. Meanwhile, the need to understand the normative foundations and direction of national policies in this field cannot be overstated.

This paper opens further avenues for studying particular national views on issues like international cooperation; desirability and applicability of international law; and individual, corporate and state responsibility and accountability. Analysis of national positions and policies can inform the implementation of the 2015 GGE recommendations and the work of the established UNGGE 2019-2021 and the UN open-ended working group. Such an analysis will also be beneficial for regional initiatives taking place, including those in the ASEAN region and West Africa.

Ultimately, the questions surrounding national cybersecurity and information security policies are not whether institutional, legal and regulatory frameworks are needed, or whether cybercrime must be combatted, or even whether it is most essential to protect the cyber part of critical infrastructure. As we approach the end of the 2010s, those questions have been answered. The question of today is how. The key strategic differences lie in the principles of implementation. When analysing individual policies, instead of considering the strategies *en masse*, we should start asking questions such as where states fall on the delicate balance between privacy, national security, and the freedom of information. Who sets the agenda: the state, the private sector or the individual? Is the system based on centralised leadership, centralised coordination or the principle of subsidiarity? And do we prefer global justice, international law or a national sense of justice being served? Accordingly, national approaches to cybersecurity thus can be modelled into two ideal types: liberal and conservative. The liberal approach emphasises the individual and favours decentralised implementation where the state has a facilitating and supporting rather than ruling role. In a conservative model state control and coordination is valued over the individual and the private sector. This division is visible in the strategies. The divide has manifested in the GGE negotiations and will dominate the discussions in the UN open-ended working group. By the end of the day, technical has turned strategic, and strategic political.

[28] See for example the 2015 and the latest UNGGE report, United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174 (22 July 2015). For a comprehensive analysis of the UNGGE process, see Eneken Tikk and Mika Kerttunen, "Parabasis: International Cybersecurity in a Stalemate?", Norwegian Institute for International Affairs (October 2018).

Annex

Table 1. Selected national approaches to cyber security. *Authors' compilation*.

Orientation	Key goals or lines of action
Australia[29]	
> Cyber security is a fundamental element of growth and prosperity in a global economy and vital for national security. It requires partnership involving governments, the private sector and the community as well as cooperation with regional and global partners.	> A national cyber partnership among major stakeholders; > Strong cyber defence to detect, deter and respond to threats; > International cooperation to secure open, free and safe Internet and in law enforcement; > Growth and innovation through supporting businesses and research and development; > Development of professional skills and competences and public awareness.
Czech Republic[30]	
> A sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace and by enhancing confidentiality, integrity, and availability of data, information systems and other elements of information and communication infrastructure.	> Enhancement of structures, processes, and cooperation; > International cooperation; > Critical information infrastructure and important information systems; > Cooperation with private sector; > Research and development/Consumer trust; > Education, awareness and information society development; > Cybercrime investigation and prosecution > Legislative framework and international regulations.
Denmark[31]	
> Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the internet.	> Regulatory frameworks > Technological preparedness > Situational awareness > Protection of critical governmental ICT systems and vital [societal] sectors > Combatting cybercrime > Public awareness

[29] *Australia's Cyber Security Strategy* (2016).
[30] *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020* (2015).
[31] *Danish Cyber and Information Security Strategy (2018).*

Orientation	Key goals or lines of action
Estonia[32]	
> Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation.	> Ensuring vital [societal] services; > Combating cybercrime; > Advancing national defence capabilities.
Kenya[33]	
> The processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction.	> Enhancing cybersecurity posture in a manner that facilitates growth, safety, and prosperity; > Raising cybersecurity awareness and developing cybersecurity workforce; > Fostering information sharing and collaboration among stakeholders; > Leadership by defining the national cybersecurity vision, goals, and objectives and coordinating initiatives at the national level.
The Philippines[34]	
> The protection of information systems (hardware and software including associated and support infrastructure), the data within these systems, and the services that are provided by these systems from any unauthorized access, harm or misuse, whether it included intentional or accidental, or from natural disasters.	> Systematically and methodologically harden the Critical Information Infrastructure for resiliency; > Prepare and secure government Infostructure; > Raise awareness in the business sector on cyber risk and use of security measures to prevent and protect, respond and recover from attacks; > Raise awareness of individuals on cyber risks, as they need to adopt the right norms in cybersecurity.
The Russian Federation[35]	
> The state of the protection of Russia's national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state.	> The constitutional rights and freedoms of man and the citizen to receive and use information, the spiritual renewal of Russia, and the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country; > Information support for the state policy; > Promoting modern information technologies, boosting the national information industry domestically and globally;

[32] *National Cyber Security Strategy 2014-2017* (2014).
[33] *National Cybersecurity Strategy* (2014).
[34] *National Cybersecurity Plan 2022* (2017).
[35] *The Information Security Doctrine of the Russian Federation* (2000).

Orientation	Key goals or lines of action
	> Protection of information resources against unsanctioned access, and securing the information and telecommunication systems.
Singapore[36]	
A resilient and trusted cyber environment that will enable to realize the benefits of information and communication technology and so secure a better future.	> Resilient infrastructure; > Safer cyberspace; > Vibrant cybersecurity ecosystem > Strong international partnerships.
The United States[37]	
> Network stability a cornerstone of global prosperity, and securing and maintaining their trustworthiness those networks is not only a technical matter but requires economic, political and social measures.	> Promoting international standards and open markets; > Protecting networks through security, reliability, and resiliency > Law enforcement; > Military response options; > Internet Governance; > International Development; > Freedoms and privacy on-line.
> Organizational actions that provide assurance of legal and reliable use of cyberspace, from hardware and software systems to operations and information (data), so that it is protected and usable in the manner expected by its originators and recipients.	> Countering cybercrime, combatting theft of intellectual property and promoting attribution and prosecution; > International consensus on rules, and continuation of multilateral negotiations and bilateral discussions; > Situational awareness through information sharing, expanding education and capacity-building; > Public-private partnerships to provide policy and operational and technical expertise.

[36] *Singapore's Cybersecurity Strategy* (2016).
[37] The White House, *International Strategy for Cyberspace* (2011), and the Department of State, "Report on A Framework for International Cyber Stability" (2014).

Table 2. International cyber policies issued by states. *Authors' compilation.*

Key goals or lines of action	Normative stands
Australia, *International Cyber Engagement Strategy* (2017)	
> Digital trade > Cybercrime > International security > Governance > Human rights and democracy > Capacity building	> Responsible state behaviour > Human rights and democratic principles online; > Stable and peaceful online environment; > Sustainable development
China, *International Strategy on Cooperation in Cyberspace* (2017)	
> International order > Security and stability > Digital divide > General international rules	> Peaceful settlement of disputes > Non-use of force > Privacy > Freedom and order
Netherlands, "Digitaal bruggen slaan" Internationale Cyberstrategie *naar een geïntegreerd internationaal cyberbeleid* (2017),	
> Public international order > Cybercrime > Malicious state activities and cyber attacks > Economic espionage > Robust response capacity > Capacity building	> Fundamental rights and freedom > International peace, security and stability > Transparency > Responsible state behaviour
Norway, *Internasjonal cyberstrategi for Norge* (2017)	
> Innovations and international trade > Public international order > Cybercrime > Capacity building	> International security and stability > Freedoms, democracy, universal rights and sustainable development
Russia, Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020 (2013)[38]	
> Technological parity with major world powers > Strategic stability > International legal regime, including international legal regime of non-proliferation of information weapons > International information security system > National and international regulatory institutions > Crime, terrorism, extremist purposes and interference into the internal affairs	> Rights of the individual, society and State > Sovereignty and territorial integrity of states > International peace, security and strategic stability

[38] *Osnovy gosudarstvennoy politiki Rossiyskoy Federatsiyi v oblasti mezhdunarodnoy infor- matsionnoy bezopasnosti na period do 2020 goda* (July 24,2013).

Key goals or lines of action	Normative stands
United States, *International strategy for cyberspace* (2011)	
> Innovative markets > Rule of law > Stability > Cybercrime > Dissuasion and deterrence > Diplomacy > Capacity building	> Freedom of expression and association, privacy and free flow of information, Internet freedom > Norms of responsible state behaviour > Right of self-defence > Cybersecurity due diligence

Table 3. Selection of normative standpoints as expressed in previous and contemporary national documents. *Authors' compilation.*

Normative positions	International venues and mechanisms
Chile, *National Cybersecurity Policy 2017*	
> 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. > 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. (p. 20)	> Multilateral and global arena supporting regional, sub-regional and multilateral consultations in this field, especially in Latin America, and actively involving stakeholders in this debate.
Germany, *Cyber Security Strategy for Germany 2015*	
> …strengthening cyber security also requires the enforcement of international rules of conduct, standards and norms. Only a mix of domestic and external policy measures will be appropriate for the dimension of the problem. Cyber security can be improved by enhancing the framework conditions for drawing up common minimum standards (code of conduct) with allies and partners. (p. 4)	> The United Nations, the EU, the Council of Europe, NATO, the G8, the OSCE, the OECD and other multinational organizations
France, Strategic review of cyber defence 2018	
> …the failure of the 2016-2017 GGE ..must not end the efforts of France and the international community to propmote standards of behaviour and confidence-building measures for ensuring the international stability and security of cyberspace (p. 4) > France must in particular work towards reaching an agreement at international level on the obligations of a State whose infrastructures could be used for malicious purposes. (p. 9)	> The European Union ('Europe'), G20. > International enegagement in creating norms of responsible state behaviour and to increase stability, joint crisis management, communication and de-escalation. > Strategic bilateral relations.

Japan, *Cybersecurity Strategy 2015*	
> Japan is committed to ensure the rights and safety of the people, and to strive for the socio-economic development of the nation as well the development of international order. (p. 5) > In particular, Japan firmly believes that recognizing the diversity of values, respecting autonomy and securing people's freedom of speech and corporate activities in cyberspace based on the rule of law will bring peace and stability to the international community, thereby ushering in prosperity for all. (p. 35)	> Bilateral and regional cooperation, outreach and awareness activities as well as research and development with ASEAN and other countries. > Active engagement in the discussions on the applicability and application of international law, development of rules and norms, Internet governance and confidence-building measures in various for a, e.g. the UN, OECD, ASEAN, APEC and Global Conference on Cyberspace and bilaterally.
The Netherlands, *National Cyber Security Strategy 2 2013*	
> Together with its international partners, the Netherlands is part of a progressive coalition that seeks to protect fundamental rights and values in the digital domain. (p. 8)	> The Netherlands is promoting international standards at the United Nations, during international cyberspace conferences, in other multi-stakeholder settings like the Internet Governance Forum, by promoting the principles of cyber security as published by the World Economic Forum, and in developing trust-inspiring measures between states, like the OSCE.
New Zealand, *New Zealand's Cyber Security Strategy 2015*	
> The openness of the Internet is part of its unique value – allowing for unrestricted participation and the free flow of information. > Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. > Human rights apply online as they do 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. (p. 7)	> International engagement on norms of State behaviour in cyberspace (e.g. London agenda). > International engagement on Internet Governance (e.g. ICANN). > Capacity-building in the Asia-Pacific region.
Nigeria, *National Cybersecurity Policy 2014*	
> To promote emergence of an appropriate legislative environment with respect to freedom of access to	> Collaboration within the regional and international community, bilateral and multi-lateral

information, intellectual property, data protection and privacy rights. (# 4.3.2 vi)	institutions, multi-national corporations, and global cyberspace governing bodies. The policy recognizes various contributions of international discourse on Internet governance, policies and management of cyberspace critical resources and contributions of global institutions.

Table 4. Number of principles and norms as expressed in national cyber and information security strategies and policies. ***Authors' compilation.***

	Principle		Norm
16	**Africa**		
11	Cooperation	**5**	Confidentiality
9	Public-private partnership	**4**	Privacy
7	Rule of law	**3**	Integrity
5	Harmonization	**3**	Human rights and freedoms
4	Accountability	**2**	Availability/access to information
4	Multi-stakeholder approach	**2**	Dignity and identity
4	Governance	**2**	intellectual property rights
3	Risk-based approach	**1**	Right to communication
3	Centralization	**1**	Freedom of expression
2	Coordination	**1**	Social justice
1	Protection of vulnerable groups	**1**	Universal access to cyberspace
1	Assurance and monitoring mechanisms	**1**	Patriotism
		1	Genre equality
		1	Good governance
		1	Transparency
14	**Americas**		
10	Cooperation	**12**	Human rights and freedoms
8	Centralized management/coordination	**10**	Privacy
7	Rule of law	**4**	Freedom of speech and expression
7	Multi-stakeholder approach	**3**	Access to information
5	Public-private partnership	**3**	Transparency
4	Risk management	**3**	Democracy
3	Accountability	**2**	Free and open cyberspace/Internet
2	International law	**2**	National sovereignty
2	De-centralization	**1**	Protection of private life
2	Proportionality	**1**	Protection of personal property
1	Integration	**1**	Confidentiality
1	Coordination	**1**	Cultural diversity
1	Multi-disciplinary collaboration	**1**	Proportionality
1	Sustainable development	**1**	Internet neutrality
1	Governance	**1**	Conflict prevention
1	Deterrence	**1**	Peaceful solution of disputes
1	Consequences	**1**	Commitment to cooperate
1	Transparency	**1**	Social justice
1	Norms of responsible state behaviour	**1**	Inviolability of communication
		1	Human dignity and integrity
		1	Protection of personal data
24	**Asia and the Pacific**		
16	Cooperation	**10**	Privacy
13	Centralized management/coordination	**6**	Human rights and freedoms
11	Rule of law	**5**	Freedom of information

8	Public-private partnership	**5**	Confidentiality
8	Multi-stakeholder approach	**3**	Integrity
3	Development	**2**	Sovereignty
1	Risk-based approach	**2**	Availability
1	Crisis consciousness	**2**	Autonomy and self-governance
1	Peace	**2**	Freedom of expression
1	Stability	**1**	Peace
1	Deterrence	**1**	Freedom of speech
1	Standardization	**1**	Independence
1	Mobilization of social resources	**1**	Internal and external security
1	Whole-of-society collectivism	**1**	Democracy
		1	Diversity
		1	Open cyberspace
		1	Collective responsibility
42	**Europe**		
39	Cooperation	**32**	Human rights and freedoms
27	Rule of law	**26**	Privacy
20	Multi-stakeholder approach	**14**	Confidentiality
18	Centralized management/coordination	**6**	Freedom of expression
17	Public-private partnership	**6**	Integrity
9	Accountability	**4**	Freedom
6	Subsidiarity	**3**	Democracy
6	Risk-based approach	**3**	Free cyberspace
5	Integration	**3**	Open cyberspace
4	De-centralized implementation	**3**	Trust
3	International law	**3**	Proportionality
2	Self-regulation	**3**	Norms/rules of State behaviour
2	Proportionality	**2**	Informational self-determination
2	Transparency	**2**	Freedom of information
2	Security and privacy design	**2**	Subsidiarity
1	Governmental assistance	**1**	Personal responsibility
1	Similarity	**1**	Tolerance
1	Precaution	**1**	Collective engagement
1	Democracy	**1**	Peaceful cyberspace
1	International influence	**1**	Transparency
1	Multi-disciplinary approach	**1**	Self-defence
1	Comprehensive approach	**1**	International law
1	Complementarity	**1**	Equality
1	Enhanced military capacity	**1**	Sovereignty
1	Balance between freedom of information and national security	**1**	Political and social stability
1	Democratic control	**1**	Moral and spiritual values
1	Adherence to EU and NATO standards		
10	**Middle East and the Gulf**		
6	Cooperation	**5**	Privacy
6	Centralized management/coordination	**4**	Confidentiality

4	Rule of law	**3**	Transparency
3	Multi-stakeholder approach	**2**	Human rights and freedoms
2	Public-private partnership	**2**	Integrity
2	Risk-based approach	**2**	Ethical values
2	Accountability	**2**	Trust
1	Holistic approach	**1**	Availability
1	National capacity	**1**	International rules and norms
1	Exclusion of designated â€œespecial bodiesâ€		
1	Continuity of operations		
1	Free flow of information		
1	Integration		
1	Public order		
1	Consensus of the top leadership		

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.