National Cyber Security Strategies: Commitment to Development

Mika Kerttunen & Eneken Tikk*

Introduction

As human and societal dependence on high technologies and information is only increasing, governments face justifiable demands for security, freedom and economic prosperity, but also expectations to contribute to international cybersecurity and even support military cyber operations. Hence, cyber security becomes an agenda encompassing various goals and ambitions related to the development and proliferation of information and communication technologies (ICTs).

Visionary, realistic and sustainable cyber and information security strategies help countries pursue the positive and deter the negative effects of technological development. As of February 2019, 106 countries had issued a cyber or information security strategy, doctrine, master plan or an equivalent government-level policy instrument.[1] The positive statistics of adopting national strategies adopted also offers important evidence of their absence: half of the states are still to formulate and implement their first explicit cyber security strategies We can also ask of the normative direction of the strategies.

Cyber security strategies have become means of political and technical continuity as well as crisis management. Having a cyber strategy can be considered a requirement of responsible state behaviour.[2] Major regional organizations such as the Organization for Security and Cooperation in Europe (OSCE), the Organization for American States (OAS), the African Union (AU), and the Association of Southeast Asian Nations (ASEAN), the Shanghai Cooperation Organization (SCO), North Atlantic Treaty Organization (NATO) and the European Union (EU) all have taken determined and nuanced approaches to cyber security.

---

* D.Soc.Sc. Mika Kerttunen and Dr.Iur. Eneken Tikk are founders of the Cyber Policy Institute, and Senior Research Scientists at the Tallinn University of Technology, Department of Software Science,

[1] This number is based on the CPI analyses of 193 UN member states and three other countries or authorities and their ICT, IT and cyber or information security documents.

[2] See in particular, the African Union *Convention on Cyberspace Security* and the European Union directive on network and information systems security ('NIS Directive') (2016/1148) stressing the need of their Member-States adopting a strategy.

We can expect the trend of national cyber security strategy development continue. In their efforts, especially developing countries are offered capacity-building support as well as various guides and indices to support national efforts.

This paper promotes an engaging, development-first approach to national cyber security strategy development. We design a "commitment to development" approach that recognizes and respects the contingent and political nature of national ICT, cyber and cyber/information security strategy processes. By doing this, the analysis calls for societalizing cybersecurity, a move that runs counter to the process of securitization, but without undermining or underlining the security imperative.

The development and use of ICTs and other high technologies influences our attitudes, habits, behaviour and processes. Accordingly, national strategies, both as a process and as products, require continuous review and updates. This analysis advocates attention to the ambition, direction and content of national cyber security strategies. It calls for reliable methodologies to evaluate the impact of policies. The authors call for sustainable and development-oriented capacity building in this field.

National Cyber Security Strategy

Strategy can be understood as a pattern or method of thinking, an administrative process or a manifestation of policy in form of an issued instrumental document. Strategic thinking is a balanced calculation between ends, ways and means, or in other words between objectives and resources. Moreover, strategy and strategic decision-making, by choosing between contesting but legitimate alternatives, takes – and needs to take – deliberate risks.[3]

Strategy as an administrative process requires organized work to define objectives, design overarching and long-term policies and action plans as well as to implement, steer, and improve such policies and plans. As a prerequisite to effective implementation, strategies as manifestation of policies and plans need to be communicated.[4]

The purpose of formulating and issuing a strategy is to form and provide political guidance, choose between policy options, prioritize objectives, allocate resources, legitimize the direction and content of taken policy as well as to inform domestic constituencies and foreign audiences.

[3] Colin S. Gray, *The Future of Strategy* (Cambridge: Polity, 2015), p. 23-42; John Lewis Gaddis; *On Grand Strategy* (New York: Allen Lane, 2018). See also Lawrence Freedman, *Strategy* (Oxford: Oxford University Press, 2014), especially page xii on strategy as "the central political art" and "the art of creating power."

[4] Often the notions of *strategy* and *doctrine* can be used interchangeably or in hierarchical order: strategy – doctrine or doctrine - strategy. Strategies can accordingly be characterized as doctrinal policy papers.

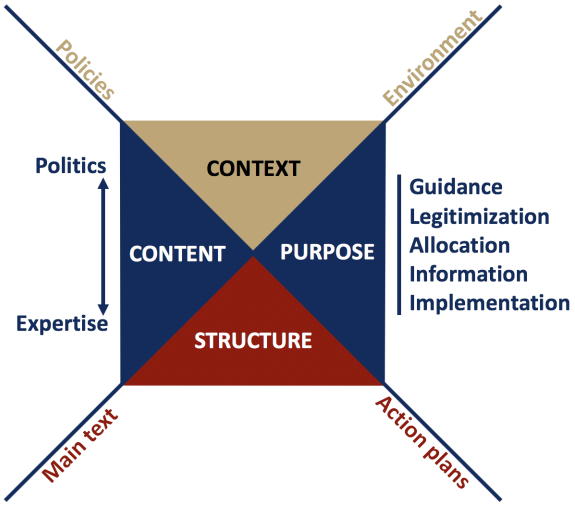

Illustration 1. National cyber security strategy conceptualized. Authors' illustration.

Issued, ambitious but realistic, strategies are also needed to create deterring effects many countries as pursuing against malicious and hostile acts in and through cyberspace. In fact, a lack of explicit strategy (or policy) can lead to the question of the efficacy and legitimacy of governmental and official activities.

National political and administrative cultures differ. Thus, instruments such as issued legislation, adopted proposals, government decisions, and development plans can fulfil the purpose of a strategy document (proper).[5] More important than the purity of the process and structure of documents is determined and successful implementation of the chosen policy: issuing a strategy does not end but starts the work of improving national cyber security situation.

Strategies need to be tailored to the political, operational, financial and technological realities and stages of development of the actor and its environment. Standardization of national approaches goes against the very nature of strategy being contingent, tailored and qualitative edge providing an instrument. The art of strategy is not of adopting proven and universally coherent and acceptable measures but to design and apply particular, different and still feasible approaches that will match with national ambitions, concerns and resources.

Thus, there cannot be any uniform ambition, direction or content to be followed or be evaluated by.

[5] Of countries not having issued explicit cyber or information strategies Israel is the most notable example. Hardly anyone can question the cyber or information and communication technological prowess of that nation. The Israeli Government nine pages long Resolution 3611 "Advancing National Cyberspace Capabilities" (2011) outlines Israeli cyber policy, http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf. The US published its first national cyber security strategy in 2003, but the next equivalent ones were issued fifteen years later by the Trump administration, namely the Department of Homeland Department *Cybersecurity Strategy*, and the White House *National Cyber Strategy of the United States of America* (note that the latter not named as cybersecurity, but cyber strategy.

A functional national security strategy:

- Defines and prioritizes national, strategic objectives;
- Remains focused on the clearly identified core issues;
- Maintains a long rather than short-term perspective;
- Aligns, and is harmonized, with other policies and strategies;
- Clearly allocates resources and responsibilities;
- Implements international best practices and lessons learned;
- Considers international cyber security trends and currents; and
- Frequently reviews the process as well as the objectives, methods and means chosen.

Strategy answers to three fundamental questions:

Where are we?
Where do want to go?
How do we get there?

To locate the starting point and the 'ground-zero' state of performance requires analysis of the current situation of cyber prowess and cyber security as well as 'real' and anticipated threats and risks in question. The difficulty is not only of cognitive nature but also of political correctness: national planners and decision-makers need to admit acute shortcomings and acknowledge domestically sensitive issues, including sub-competent administration or under-resourced agencies, state or private telecom and internet service provider monopolies, money laundering, or the surveillance of political dissidents and insurgents.

Defining the direction requires strategic vision. The importance of IT and ICTs are often recognized only from a narrow, single sector or tactical-technical perspective. Strategic choices before any government require considering national values, societal development, national security, and geopolitical gaming in the context of ICT development and dependence. Deciding on the ways and means seems easy – at least in the sense that there are both guidance and lucrative services and products available promising to fill the gaps between the present and the flickering future.

The mastery of strategy does not lie in maximal pursuit of any or every relevant objective. It derives from the ability to allocate and use resources optimally: doing less is as good as doing more.

The need of national cybersecurity policy is usually argued as set of consolidated measures *against* threats. The commonly-prioritized objectives of the contemporary national cyber and information security strategies thus consist the following, interlinked, categories, priorities or key areas of focus: legal and institutional frameworks; information assurance and basic network security; critical infrastructure protection; combatting cybercrime; national security, including military cyber defence; workforce development; public awareness; and international cooperation.

As long as there is no systemic understanding and technical competence, cyber policy is inevitably driven by technical and security-first considerations. Without holistic understanding and vision of the potential and consequences of the use of ICTs national and intergovernmental policies easily become, or remain, incremental. Comprehensive and detailed analysis and planning therefore in and of itself indicates maturity and high level of strategic preparedness. Many governments still lack a developed culture, confidence and competence of coordinated cyber policy planning and implementation.

Can there be too much security?

In the aftermath of the 2007 cyber-attacks against Estonia, technologically and economically advanced countries have driven a security-centric approach to national cyber strategies. The first wave of national strategies in the early 2000's led some analysts to observe differences in understanding of the very term *cyber security*, the unclear relationship of cyber security strategies with other national and international policies as well as the lack of a dynamic approach to cyberspace-specific (technological) threats and challenges. Early national approaches also lacked explicit methodology and criteria as to tactical and operational plans [action plans].[6]

Many countries have since updated their strategies by increasing/furthering their political, operational and technical ambitions, expanding their focus for example to include offensive military capacity, and developing measures and mechanisms of implementation. Contemporary national strategies contain references to deterrence and counter-measures and initiatives to develop cyber military capabilities, including cyber commands and offensive capabilities. Countries with cyber military ambitions include the obvious military powers such as France, the Russian Federation, the United Kingdom, and the United States but also e.g. Columbia, Estonia, Finland, Monaco, Moldova, the Netherlands, North-Macedonia, Poland, Serbia, and Senegal, many of them labelled as small states.

Strategy formulation is a process that transforms the administration. Implementing a strategy transforms the society, the object of those action. An obsession with security turns ICTs from the tools of peace and development into tools of suspicion and surveillance, and the open societies into fearful societies. To avoid the negative consequences of securitization and to maintain the promise of ICTs, cybersecurity needs to be societalized. Societal and developmental objectives and fundamental rights and freedoms of the individual need to be the starting point and the end-game of cybersecurity, and the ultimate criteria of validity and relevance of the action to be taken. Cybersecurity is yet but means to an end, engaging rather than an isolating process.

National cyber security strategies are building blocks for international peace and security. Strategies allow countries to address issues of perceived insecurity and promote issues of stability. Of the latter national commitment to international law and confidence building measures are of particular and practical importance. Strategies being politically approved documents can mandate and task agencies and organizations to implement for example transparency measures, participate in regional cooperative initiatives, and exercise restraint in their otherwise more offensive activities. Similarly, strategies can communicate government ambitions to develop international regulatory instruments for the cause of peaceful use of ICTs and cyberspace. In fact, issuing cyber or information strategies can itself be regarded as a norm: expected and constructive conduct by a government that takes an active stand on the nation's future and development and for the stability of international relations. The proliferation of national strategies is not inflating or inflammatory but progressive behaviour, a sign of emerging global cyber culture.

Security-first advocates find deliberate risk taking and the acceptance of some threats, an inevitable condition of strategy making, difficult. Furthermore security-heavy cyber and information security

---

[6] 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), p. 3–31.

strategies are unable to anticipate and deal with the upgrades of services, software and infrastructure, changing social and economic behaviour as well as emerging threats. That leads to their early retirement. The instability and the economic and societal progress projected by technological development need to be constructively balanced to create of the desired and necessary national and international effects.

Frameworks, Measures, and Indices

In the wake of emerging national information technology, information and communication technologies and cyber and information security strategies several national, international and commercial assessment tools and maturity models have emerged. Nations are ranked by various ICT, *e-*, cyber and cyber security postures and profiles. The simplest of assessments pay attention to technical and other measurable indicators such as telephone connections, Internet penetration, financial expenditure, and manpower. More sophisticated analyses pay attention to a wider range of capability factors or elements such as legal and political frameworks, organizational measures, technical measures and levels, and national and international cooperation. Measures and rankings pledge tangible benchmarks to promote development of national ICT and cyber policies and strategies as well as advanced culture of cyber security.

These models depart from defining factors, dimensions or key performance indicators which existence and level of implementation are assessed. The most metrical of assessments break findings into weighed factors to produce individual scores and international rankings. Some frameworks remain more principal and take distance from prescriptive checklist typologies.

The objectives and methodologies (typologies, methods, and criteria) of the recently developed and employed assessment models are summarized in the annexed table. The table includes the [UN] International Telecommunication Union (ITU) *Global Cybersecurity Index and Cyberwellness Profile* (GCI)*;* the Commonwealth Telecommunication Organization (CTO) *Commonwealth Approach for Developing National Cybersecurity Strategies*; European Union Agency for Network and Information Security (ENISA) [An] *evaluation framework for National Cyber Security Strategies*; University of Oxford, *Cyber Security Capability Maturity Model* (CMM); Melissa Hathaway and Potomac Institute for Policy Studies, *Cyber Readiness Index* (CRI)*;* and Australian Strategic Policy Institute (ASPI) International Cyber Policy Centre *Cyber Maturity in Asia-Pacific Region*, the Estonian e-Governance Academy (eGA) *National Cyber Security Index* (NCSI) and the World Economic Forum (WEF) *Networked Readiness Index* (NRI).[7]

---

[7]The [UN] International Telecommunication Union, *Global Cybersecurity Index and Cyberwellness Profile,* https://www.itu.int/pub/D-STR-SECU-2015; the Commonwealth Telecommunication Organization, *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015), http://www.cto.int/media/foth/cybsec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf; University of Oxford, *Cyber Security Capability Maturity Model,* v. 1.2 (15 December 2014), https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf; European Union Agency for Network and Information Security, *An evaluation framework for cyber security strategies* (2014), https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1; Melissa Hathaway, *Cyber Readiness Index 2.0.* Potomac Institute for Policy Studies (November 2015), http://www.potomacinstitute.org/academic-centers/cyber-readiness-index; Australian Strategic Policy Institute International Cyber Policy Centre (ASPI), *Cyber Maturity in Asia-Pacific Region 2017,* https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017; e-Governance Academy (eGA), *National Cyber Security Index* (NCSI), https://ncsi.ega.ee/; and World Economic Forum (WEF), *Networked Readiness Index,* https://widgets.weforum.org/gitr2016/.In addition, the ITU as well as NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have published handbooks that discuss in detail strategy development as a process (Frederick Wamala, *ITU National Cybersecurity Strategy Guide* (Geneva: ITU, 2011); Alexander Klimburg (ed.), *National Cyber Security Framework* (Tallinn: CCDCOE, 2012).

The benefits of evaluation as summarized by the ENISA *Evaluation framework* are:

- Evaluation can inform about policy changes and the framing of issues in the long term; allow learning from past experience;
- Evidence of effectiveness or learning can support the accountability of political action;
- Evidence base can give credibility towards general public and international partners;
- Evaluation can support outreach and enhance public image as transparent organization;
- Having facts on what works can help gain traction in policy process;
- Evaluation makes it necessary to compile data sources on policy and its implications for long-term planning; and
- Catalyses discussion with stakeholders.

Accordingly, ENISA lists the challenges of:

- Evaluation needs investment of resources;
- Exposing flaws in policy can undermine political priorities even when the priorities themselves are supported;
- Good practices can be of limited use due to differences in national evaluation cultures;
- Outcomes are often challenging to define and measure; and
- Attributing changes to the strategy itself can be difficult.[8]

Using these tools, one has to recognize that standardized approaches can remain blind to other theoretically as 'real' or nationally preferred aspects of cyber or information security. For example, military cyber capability development, a fact deductible from empirical analysis of national security strategies, is absent in the most assessment tools. Similarly, national needs and ambitions to develop legislative framework and law enforcement measures differ from country to country – even in cyberspace. A strategy planner or developer must therefore cautiously select the dimensions of various models and factors that need to be assessed for their country's purposes, or undergo a more holistic approach to consider and accommodate all relevant aspects.

Ranking nations for the purposes of strategy development is potentially counterproductive. Indexing and ranking implicitly promotes relative country positions and reward political and administrative attention over implementation and performance. Most importantly, indexing and ranking does not pay attention to the impacts, outcome, of efficiency of the chosen policy. Invalid measurement taxonomies, uncritical selection of criteria and the lack of interest in evidence produce results that many cyber policy and security professionals at best find amusing. This impotence of assessments is dangerous if politicians and public truly start to believe in these propagated national strengths or weaknesses. One can also critically ask how many international rankings and measures are enough?

The debility of the indices and measurement tools does not lie in their taxonomies or specific methods, which can be fine-tuned *ad infinitum,* but on the very reductionist logic of the models. Firstly, measuring models are built on a number of implicit and questionable assumptions on their validity, and secondly, they are at one and the same time a-historical, a-political and a-strategic.

In general, the assessment models assume that:

[8] European Union Agency for Network and Information Security, *An evaluation framework for cyber security strategies*, p. 7, drawing from the evaluation policy research of J.E. Furobo, Christoph Knill, and Carol Weiss, yet with a slightly more positive view of the impact of evaluations.

- All nations face similar threats and risks and thus same similar political, operational and technical ambitions;
- The total fulfilment of the measured [selected] criteria equals perfection and certainty of cyber prowess;
- The total fulfilment of the criteria is in the best interest of all nations;
- All nations need, want and are able to fulfil the recommended measures.

The existing models thus expect uniform, maximalist and pre-determined behaviour in admittedly interlinked but still diversified field of national policy-making where national priorities differ, authoritative allocation of values is challenging and where intellectual, financial and material resources are scarce. By promoting paradigmatic views of cyber security strategy any indexing and measurement model contradicts the very notion of strategy and strategic thought.

Many models explicitly promote Western and technologically advanced countries' values such as market economy and growth, democracy and transparency, and technological solutions to social and political issues. One does not need to contest the inherently good of these values to observe that many nations and in particular governments, including some Western democracies, do not wholeheartedly share or follow these values.

The metrics and ranking of different indexes tend to reflect the assumptions and values of their patrons, also, predominantly Western liberal democracies. One should therefore be critical to the methods and assumptions that lead to numbers and positions.

To conclude, models can be fully correct but, without being internalized, would still remain irrelevant. For example, the notion of harm is not universally shared: for some regimes digitalization, the proliferation of ICT services represents harmful development; similarly, the development of cyber military capabilities or robust response policies can be considered harmful – or stabilizing. While recognizing the traps of overgeneralization, patronizing or colonial attitude or the so-called Balkanization of the cyberspace local emphasis need to be acknowledged in the well-meaning capacity enhancing initiatives.

As stated above, a strategy process, by definition, is contingent and calculative. The practice of strategy can be understood as the use of tactical measures for broader purposes,[9] but strategic thinking and strategic decision-making cannot be reduced to prefixed lists of tactical and technical activities. Improving the models and tools by adding, removing or fine-tuning the dimensions, elements or factors or changing their metrics will not remove the fundamental problem of reductionism.

Imported models and tools neglect the contingent, political nature of strategy-making by marginalizing explicit recognition and acknowledgment of alternative directions and solutions. After all, a strategy must balance between contesting views, each of which can be justifiable. Balancing of opposing views and approaches takes place in democracies as well as in totalitarian regimes. Policy-making stems from national political, societal, cultural and organizational realities.[10]

[9] Following Clausewitz's approach to strategy as "the use of engagement for the purposes of war."

[10] Strategy-making is by default decision-making of who gets, what, when and how to paraphrase Harold Lasswell's maxim (and the name of his 1936 book on politics). See also ITU *Guide*, p. 5 and 35-39.

The critique above does not deny the value of indices or maturity models. Empirical research points out that evaluations and assessment have less impact to strategy and policy formulation but can have more influence on the implementation of the on-going policies. Whereas the former is explained by the dominant role of values and ideology in fundamental policy questions as well as the influence of competing pressures and objectives, the latter builds on the instrumental match between implementation as problem and evaluation as answer.[11] Surveys, interviews and workshops with baseline analysis can promote self-awareness, and with the help of incentives and feasible benefits the measuring models get national authorities to meet, talk and work together.

Guidance and measurements, which take national ambitions and political and material realities better into account, would support governments to answer to the essential and difficult questions of strategy. They would also help to build endogenous capacity that is needed when becoming strategic developer and employer of IC technologies and services. Without abandoning technical and political security requirements national cyber security strategies can become positive tools of societal development and instruments of international peace and regional stability.

Commitment to Development (C2D)

Being able to formulate an implementable strategy requires thorough negotiations among domestic stakeholders. These strategy talks have to follow the purpose and direction of the chosen national and societal development policies and plans. They have to be cognizant of the domestic resources available. These discussions then lead to a national agreement, even social contract, between competing views and entities. To formulate a national cyber security strategy requires commitment: strategy without implementation remains an empty promise.

By developing national cyber security strategies and respective capabilities, governments commit to responsible, comprehensive, forward-looking policies that increase their developmental capacity and help achieve national ambitions. Effective implementation of strategies will narrow capability and performance gaps, reduce perceived insecurity and foster international cooperation. Strategies, in sum, help determine and analyze shared expectations to responsible State behaviour and guide international cyber diplomacy and policy-making.

Commitment to Development (C2D) is an approach that promotes cybersecurity as a societal and economic enabler. C2D methodology weaves values, development goals and societal realities into the fabric of cybersecurity policy. It enables nations to identify needs and capabilities, threats and risks as well as areas of potential domestic and cross-border cooperation. The framework supports experts, policy planners and decision-makers in understanding and explaining the field and its respective ambitions, opportunities, requirements and consequences in a broader governmental, national and international context. By doing this, the approach promotes interagency and cross-disciplinary dialogue and attention to the interrelationship of priorities, ambitions and resources. Most importantly, such horizontal and vertical dialogues help to grasp and consider 2nd and 3rd order consequences and requirements that otherwise could be missing in action. These may include legal and resource requirements, interagency coordination, international normative restrictions and cooperative opportunities. This also enables to

[11] Jan-Eric Furubo, "The Role of Evaluations in Political and Administrative Learning and the Role of Learning in Evaluation Praxis", *OECD Journal on Budgeting*, 3(3) (2003), p. 67-86; Furobo concludes that "[T]he information acquired from evaluations does not seem to be a major explanation for significant policy changes" (p. 72); Carol Hirschon Weiss, "The interface between evaluation and public policy", *Evaluation*, 5(4) (1999), p. 468-486.

conduct more fruitful discussion with the private sector and civil society as governments are empowered to communicate their visions and cyber security profiles. Societal stakeholders can support the government to identify, for example, economic and industrial opportunities as well as private or corporate issues of concern. The framework of such an approach consists of three interlinked and value-free elements: Direction, Strategic Capacity, and Policy Analysis.

Direction

Threat assessment is not the point of departure for cybersecurity. Instead, cybersecurity thinking should be driven by societal values and political ambitions. The formulators of national cyber security policy have to look backwards to the fundamental base values to recognize the purpose and potential of security.

Cybersecurity, among other positive features, guarantees functionality of systems and services and the confidentiality, integrity and availability of information of which all public and private processes and functions depend. These systems and service have been established to safeguard organized, prosperous and peaceful life and desired and sustainable lifestyle for citizens. A heuristic and strategically attuned engagement can support governments to design national vision, provide political direction and develop sustainable long-term policies, strategies and action plans. Without vision national cyber security strategies can be rich in detail but yet remain misdirected. Moreover, assessing technological change "within a lesser context of than the ultimate cultural aims undermines the very existence of the culture".[12] As the World Economic Forum points out, the use of ICTs should not be an end in itself, either: what ultimately matters is the "impact that ICTs actually have on the economy and society".[13]

The role of technology is important for the ultimate ends, values and choices of human life and our societies, and therefore, must be taken seriously. Cybersecurity is to serve that positive impact and the afore-mentioned objectives by being more an active security-to enabler than a reactive and inevitably outsmarted security-from disabler, the relic from the age the thick security manuals and firewalls.

All governments have to establish, continuously develop and maintain technical-organizational information security and network protection capacities. National authorities also need to establish the subsequent supportive capabilities such as institutional and legislative frameworks and workforce development. These rather technical and technocratic lines of action come with number of competing values and choices; indeed, they set the normative direction and content of cybersecurity policy. It is therefore essential that information and cybersecurity policy becomes fully aligned with broader national policies and initiatives, in particular national development policy, IT and digital strategies and the Sustainable Development Goals.[14]

Cybersecurity otherwise starts to live a life of its own, departing from national politics becoming an enclave of extra-ordinary beyond scrutiny and accountability. Finding a balance between security and development, controls and freedoms, centralization and decentralization, and the State and the Individual, must be determined in the strategy process, discussions between the stakeholder and in

---

[12] Arne Næss, *Ecology, community and lifestyle* (Cambridge: Cambridge University Press, 2001), p. 33.

[13] World Economic Forum (WEF), *Networked Readiness Index* (2016), p. 33.

[14] Commonwealth Telecommunication Organization, *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015), p. 5-9 and table 1. The listed principles represent more lines of action deriving from moral and normative value positions than such positions. On value-based approach see also Wamala, *ITU National Cybersecurity Strategy Guide*, p. 42-45.

political and societal debates.[15] Given the omnipresence of smart and connected technologies in all sectors of societal life, from agriculture and fishing to nuclear energy and speed trains, cybersecurity is but an essential enabling element. Security by default, an ambition known from industry, is a feasible to be achieved in national policies.

Breaking apart, operationalizing, the key capability areas into more detailed lists of specific factors, and keeping in mind the desired levels of ambitions, allows outlining a comprehensive view of potential directions and alternative lines of action. The aim of such empirical accounting and typology is not to offer exhaustive to-do lists but to provide an encompassing overview of the alternative ambitions and actions. Contextualizing and grouping the detected elements, factors and criteria as optional and parallel lines of policy constitutes the crucial and unique element of the *Commitment to Development* approach. Without direction any action would be blind.

Strategic capacity

The common threat-centric thinking way of organizing national cybersecurity endeavor can, and should, be replaced. An alternative that departs from the needs of organized, prosperous and peaceful life, desired and sustainable lifestyle, begins with the values and only then proceeds to strategic capacity. Strategic capacity is a set of aspects that create national prowess that surpasses contingent concerns and provides sustainable, by-default security. Strategic capacity can be operationalized into individual and organizational skills and competences, resilience and recovery, leadership and governance, and international cognizance.

CONTEXT	OBJECTVES	STRUCTURE
Where are we? **An assessment of domestic, regional and global operating environment that the strategy will depart from, and build on.**	**Where do we want to go?** **Definition of ambitions and objectives that the strategy is intended to help to achieve.**	**How do we get there?** **Components and elements that the strategy will have to define, articulate, align and set in motion, together with a verification system.**
National • **Development policy** • **IT/ICT/digital strategies** • **Threat assessment** • **Defence/security strategy and doctrine** **Regional** • **Cooperation mechanisms** • **Agreements and agendas** • **Experience and expertise** **International** • **Goals and agendas** • **Conventions and policies** • **Standards**	**Economic benefits** **Social prosperity** **Cost reduction** **Resilient and safe ICT environment** **National security** **International lead and influence**	**Vision and mission** **Areas of focus/activity** • **Legal and institutional frameworks** • **Information assurance/cyber defence** • **Combating cybercrime** • **Critical infrastructure protection** • **Workforce development** • **Public awareness** • **International cooperation** **Implementation** • **Operationalization of objectives** • **Allocation of responsibilities and resources** • **Division of labour** • **Monitoring and measurement of process** • **Reporting, reviews and renewal**

Table 1. National cyber security strategy framework.

Building durable cyber capacity takes time. Elementary human skills and competences are created at basic and advanced education; some basic capabilities can even be purchased. It is advisable for governments to ask for external, domestic or international, support. Sustainable security, however, requires in-house

[15] Hathaway and Klimburg speak of "five dilemmas of national cyber security" representing competing directions of cyber security strategies: stimulation the economy vs. improving national security; modernizing infrastructure vs. protection of critical infrastructure; private sector vs. public sector; data protection vs. Information sharing; and freedom of expression vs. political stability (Melissa Hathaway & Alexander Klimburg, "Preliminary Considerations: On National Cyber Security" in Klimburg (ed.), *National Cyber Strategy Framework Manual*, p. 34-43.)

leadership, workforce and steady flow of resources. To effectively enhance visionary, political and strategic capacity requires long-term and progressive engagement between national authorities and their advisors and potential sponsors.[16]

Initial steps of such engagement should include strategy-formulation and issue-specific courses for national authorities: legislators, diplomats, administrators and regulators as well as intelligence, legal, law enforcement and military officers. The most generic of courses and workshop dealing with strategy alternatives and requirements, the nexus of ICTs and economic and social development as well as respective administrative, technical and financial methodologies can be, if needed, organized regionally. Such preparatory engagements also inform which policy directions are acceptable. In addition to general knowledge, specific skills and competences can build on targeted and tailored courses and workshops. If desired national sessions and consultations can follow to e.g. discuss and develop policy options, alternative strategies and draft legislation or to conduct table top exercises. Many nations would appreciate assistance in developing national IT and digital policies, cyber security strategy, legislative frameworks and legal competences, creating professional and academic work force and weaving smart and connected technologies into societal and economic processes.

It is essential to emphasize national responsibility and domestic considerations over theoretical knowledge. Obviously, the more detailed the process becomes the more necessary it is to bring on-board subject-matter experts. However, the national authorities in question and the external experts ought to maintain strategic mindset and the desired ambitions and directions.

Exercises are an effective way to train and test leaders, experts and organizations. Too often, exercises are built around heavy, complicated and expensive machinery and instructions stealing valuable time and effort from learning. Many available standardized exercises also tend to focus on incident management with predominantly escalatory scenarios. Instead, exercises should be used to develop individual and organizational competences and processes but also, and hopefully increasingly, to develop and test legislation, policies, action plans or particular elements thereof, for example financing or ethical considerations. They should also teach, train and test non-escalatory practises. Often, the most instructive national and policy exercise tasks operate with alternative input factors, asking 'what if B or C instead of A', calling for advanced thinking rather than rapid response.

Reliable policy analysis and assessment

A linear approach to the strategy process provides a framework of action but does not guarantee the outcome. National policies and strategies, their objectives, inputs, outputs and outcomes need to be assessed. This requires, in essence, policy analysis where its distinct methodologies can be employed. Issued policies, conducted exercises, acquired technologies, designed websites, and established programs are not outcomes; at best they are outputs, in some cases, mere input factors.

A proper assessment entails analysis of not only the content and direction or implementation of governmental policies and programmes, but in particular the impact-effect of these policies, that is the achieved level and status of actual ICT developmental prowess and cyber security. Conceptual and

[16] See the 2015 UN Group of Governmental Experts report emphasizing the importance of and providing recommendation for capacity-building (UNGA, Developments in the field of information and telecommunications in the context of international security (A/70/174 (22 July 2015), #21).

methodological support for analysis of outcomes instead of accounting the input factors can be found for example in health care, education, and energy sectors.[17]

A simple, yet demanding mechanism that should be included into strategies is defined measurable metrics and subsequent criteria of desired impact. At simplest, a policy metrics tool, a table, can combine verbs of action, for example 'established', 'recruited', 'adopted', 'harmonized', 'reduced', or 'increased' with responsible actors, ambitious but realistic numerical criteria of progress and the expected due-dates.

Analysis feeding forward into the strategy process, both reviewing mechanisms and the implementation (of action plans), strengthens national ownership and responsibility, the primacy of national decision-making. Thorough policy analysis also helps to satisfy the supervision and accountability criteria national parliaments and international financing institutes have on governmental policies and programmes.

Conclusion

The story of cybersecurity is often a story of the lack of security, a state of sub-security and a sense of insecurity. Threats, and urgency to act, are used to justify extraordinary, extrajudicial and extra-political measures. International pressure, popular literature and cybersecurity industry are amplifying the message of doom and destruction.

Technological development and dependency are not slowing. The benefits of 5G networks, artificial intelligence, nanotechnology or quantum computing will not be automatically employed or equally distributed. The functionality and stability of national ICT environments and infrastructure is a question of technical and political security but increasingly an essential element and dimension of development. Ineffective and unstable cyber infrastructure leads to the inefficient use of national resources and discourages international investments and other positive engagements.[18]

When measuring and ranking national cyber security strategies, indices assume that 'more' is better, setting ICT penetration, information society and other maximalist criteria as the ultimate goals of development. Doing so, they dismiss countries with lesser ambitions and capacities, or, more importantly, countries that are not yet convinced of benefits brought by ICTs. As a result, the existing indices and rankings fail to point the strategic objectives and the key priority areas of engagement. By over-prioritizing security, Western indices marginalize societal and economic development, an aspect more in-line with the core values and ICT related objectives of the West. Concluding that no country is cyber ready undermines the international capacity building agenda by suggesting that even those who seek to support others may not be up to the challenge. The enemies of open, free and pluralist societies, in turn, can exploit this attitude.

There is no pre-determined way or model or strategy to embracing ICTs in national development: countries and governments need to prioritize among competing but legitimate objectives, allocate scarce resources, and take calculated risks based on their own assessments and realities. Strategy, by default, is contingent and calculative. National priorities and resources order the depth and scope of activities.

[17] Cyber affairs in general are plagued by ill-researched and uncritical literature of cyber pulp fiction and politically, commercially motivated agitation and even undergraduate papers. ICTs as tools of peace and development deserve more serious and professional attention.

[18] International Institute for Strategic Studies, *The Evolution of Cyber Domain* (ed. Eneken Tikk-Ringas), (London: IISS, 2015).

States' approaches to cyber affairs are, and must be, shaped by their distinct national and political culture, particularly in the development, use and oversight of ICT capabilities. Countries, although facing similar-appearing problems and utilizing same foundational technologies, have very different political, operational, financial and cultural premises to build to and from. Strategic thinking can arguably be regarded universal and even a-historical but strategies cannot be not pre-ordered, exported or imported. A more ambitious and advanced strategy would not function in an operating environment where baseline technical and administrative requirements are not met. The equation is also correct the other way.

Societal and developmental objectives are the starting points of crafting national information or cyber security strategy. Security-first approaches will be outsmarted, and security-alone approaches will become obsolete. Starting from, and supporting, wider national ambitions the Commitment for Development is all about developing sustainable and by-default cybersecurity.