**Beirut International Conference on National Cybersecurity Strategy:**

**A Must for National Security**

**February 26, 2014**

Comprehensive national cybersecurity strategies: what is needed, and what other nations have done

*Henning Wegener*

Lately, elaborating and adopting a national cybersecurity strategy has almost become a fashion among nation States. The movement has increased in speed, 2012 and 2013 bringing in the richest harvest. As the table reproduced here shows, there are now some 30 countries that have endowed themselves with such an instrument, and if one counts in those countries that have announced the imminent publication of their strategy, one easily arrives at 35 or even 40. There is also the common cybersecurity strategy of the European Union of February 2013 so that the 28 countries making up that group can be considered covered, even though they have, or may not yet have, adopted a complementary individual national document of their own on the subject. The EU countries also have the advantage that they have a common cybersecurity agency, ENISA, which helps in implementing national strategies..

As the number of strategies grows, one can observe a learning process. From a perusal of the documents it becomes quite obvious that later strategies have taken cues from their predecessors, and have readily worked in some of their elements. It would thus seem logical that an analytical look at the most recent strategies yields the most insights, and I will for that reason give an added emphasis to the three most recent, and in each case excellent, documents from Turkey, India and Spain. The Spanish strategy was adopted as recently as December 2013. Yet, independent of the development over time, the US “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”, based on earlier National Cybersecurity Strategy Documents, of May 2011, and the UK strategy of 2009, because of its impressive attention to detail, also deserve to remain in our focus.

For a country seeking to join the crowd and endow itself with a National Strategy, a comparative analysis would, obviously, be a precious tool, and I am sure that our host, the Center of Research and Strategic Studies of the Ministry of Defense, has already proceeded to undertake such analysis.

I have no intention to emulate or duplicate them, which would be a futile attempt also in terms of the time available here. Also, some basic comparisons are already available in the literature, as in an ENISA document of 2012.[[1]](#footnote-1)

Yet I would like to make a brief structural analysis to demonstrate how most of the extant strategies are built (“common points”), make a list of objectives and contents most frequently included, and end with some personal recommendations, timidly offered, that might fertilize the current Lebanese government thought.

Most strategies start with a brief reminder of the perils of the digital age and the compelling rational for elaborating a national strategy (“threat assessment”) that seeks to involve all digital stakeholders in a common endeavor. There is no limit how detailed one can be on this, truisms included. Most strategies stress the all-permeating nature of digital technologies, the universal interconnectivity, and the security and national security dimension. Like in the introductory paper to this Conference, many strategies dwell on the necessity of cooperation, nationally, regionally and internationally. This is all essential and good. Language for such introductory chapter is available in many strategy documents, and the selection and length of discourse is a personal choice. I would counsel conciseness, as the basic technological facts, interdependencies as well as vulnerabilities and risks, are well known and universally perceived, essentially in the same manner.

Most strategy documents then proceed to state the objectives of the exercise and the principles on which they are based. In large measure, these texts have the same thrust; they stress the necessity to prevent and persecute cyber attacks, to protect essential infrastructures, to secure civil and military Government systems and networks, the need for partnering across society and internationally, all this to foment security and confidence. The objectives spelled out in the introductory document for this session very much reflect this approach.

Nevertheless, the way the various national strategy documents posit these objectives differs considerably. The Indian Strategy is particularly elaborate, mentioning 14 national goals - although the objective of international cooperation is hardly mentioned - , while others are more general. The most recent document, the Spanish, articulates one overriding goal – “to guarantee the secure use of information networks and systems through strengthening our capacity to prevent, detect, and respond to, cyber attacks” – with six sub-goals.

The strategy documents then spell out the various aspects and activities envisaged. ENISA has attempted to provide a synthesis, and has found that the main points covered by a typical NCSS are the following:

* To define a governance framework for cyber security.
* To define an appropriate mechanism (often a public private partnership) that allows all relevant public and private stakeholders to discuss and agree on different policy and regulatory cybersecurity issues.
* To outline and define necessary policy and regulatory measures and clearly defined roles, responsibilities and rights of the private and public sector (e.g. new legal framework for fighting cybercrime, mandatory reporting of incidents, minimum security measures and guidelines, new procurement rules).
* To set the goals and means to develop national capabilities and the necessary legal framework to engage in the international efforts of diminishing the effects of cybercrime. In several strategies
* There is a particular focus on cybercrime and the need to intensify

investigation and prosecution including the strengthening of current

legislation and international judicial cooperation.

* To identiíy critica1 information infrastructures (Clls) including key assets, services and interdependencies.
* To develop or improve preparedness, response and recovery plans and measures for protecting such Clls (e.g. national contingency plans, cyber exercises, and situation awareness).
* The documents stress the necvessity to establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation, based on integrated organizational structures that develop, implement and test preparedness, response and recovery plans and measures. This may also mean an integration of existing structures (e.g. national/governmentaI CERTs).
* To define a systematic and integrated approach to national risk management (e.g. trusted information sharing and national registries of risks).
* To define and set the goals for awareness raising campaigns that instill changes in the behavior and working patterns of users.
* To define the needs for new curricula with emphasis on cyber security for IT and security professionals and specialists; and also training programs that allow the improvement of skills of users. For example, the UK strategy aims to improve training and education for information security specialists to create a strong cyber security profession.
* International co-operation with EU and non EU Member States (e.g. adoption of international conventions).
* Comprehensive research and development programs that focus on emerging security and resilience issues of current as well future systems and services.

This is certainly not a full reflection of what the various strategies announce as political purposes and plans – and sounds very abstract in this condensed form – but at least shows the spread of problems that require an integrated strategic approach.

The manner and sequence in which these problems are discussed and solutions being sought, differs in length and structure.

The most recent strategy, the Spanish one, captures the required action in eight “Lines of Action”, with the following titles:

1. Capacity of prevention, detection, response, and post-attack recuperation, including cyber defense by the Armed Forces
2. Securing the ICT systems that are essential for the functioning of public administration
3. Securing the ICT systems that support critical national infrastructures
4. Capacity of investigation and law enforcement relating to cyber crime, but also cyber terrorism
5. Security and resilience of ICT in the private sector
6. Enhancing knowledge and competence, R&D
7. Fomenting a culture of cybersecurity
8. International coordination (harmonization of norms, international information exchange, treaty-making)

After this brief overview covering the already existing national strategies, I would now like to focus on a few points which I deem to be of crucial importance, especially if one looks at the strategic environment of Lebanon.

In the first place, I would argue that beyond uniting the whole range of stakeholders in a common national endeavor, it is imperative to assign a major place to international and trans-frontier cooperation. Prof. Mona Al-Achkar has eloquently presented the rational for this priority at the annual conference of our group in Erice in August 2013: “Cyber threats represent a transnational global criminal phenomenon which cannot be dealt with according to the traditional distinction between jurisdictions defined by State sovereignty and borders. An attack launched, from one country against another may affect many others. A single jurisdictional approach is not enough, a coherent and global approach is needed. Hence, cyber deterrence cannot be undertaken by one government alone, in the absence of cooperation. Cooperation is a must“. Among other tasks she stressed the following: „Avoiding emergence of safe havens through multilateral international and regional conventions, and through homogenization of legislations and regulations dealing with cyber crime, and cross-border cooperation. Establishing a regional consensus around common problems of cultural and national sensitivities, that may be particular to a region“. There is particular cogency in these arguments when they come from a country the size of Lebanon, while the Indian cybersecurity strategy, as we have seen, gives international cooperation only passing emphasis, given the size and high degree of self-sufficieny of the country.

There is perhaps no better guide to articulating such a transnational cybersecurity policy than the International Strategy for Cyberspace of the United States (2011) which I mentioned earlier. It offers an excellent strategic blueprint, „a roadmap allowing the United States Government’s departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek”

You will share my view that it is particularly significant that this call for international partnership has come from the United States, and that the whole spirit of their strategic document reflects an emphasis on cyberdefense and peaceful purposes.

In the context of international cooperation and especially the need to harmonize cybercrime laws world-wide it is as evident as it is important that laws on cybercrime and its prosecution are harmonized. Here the Budapest Convention on Cybercrime of 2001 has been the seminal event. As of now, 41 countries have signed and ratified it, and 11 ratifications are pending. It is regrettable that Lebanon is not yet among the signers. If the underlying thought of this passive stance is that the Convention is considered a European text, made for Europeans, that is certainly not true. Countries as distant and different as the United States and Ukraine are full members of the Convention. And it is not only the material penal norms on cyber delinquency and the successful systematization of cybercrimes that are being harmonized, and “safe havens” for criminals eliminated - as Prof. Al-Achkar finds very important – but the Convention also internationalizes law enforcement and international information-sharing, 24/7 observation, early warning, transnational cooperation by CERTs, etc. in a multilateral contractual framework. The US International Strategy, in advocating broad accession to the Treaty, has the following to say: “The United States and our allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facili­tates evidence-sharing, extradition, and other types of coordination. The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases”. What is true from a US viewpoint would certainly also be true from the perspective of smaller countries.

My third observation concerns the organizational prerequisites of a functioning cybersecurity strategy. From the beginning, mechanisms for coordination and supervision of implementation must be built into the cybsersecurity strategies. More than half of the existing strategies provide for that need. Most of them have established a National Cybersecurity Council as a government organ with political composition, and, in addition a National Cybersecurity Center with the necessary technical qualifications to monitor threats, coordinate responses centrally vis-avis public and private stakeholders, be the focal point for contacts with national and international CERTs, run the 24/7 contact agency, and direct public cybersecurity education. An organization of this kind would also be the place to enact “Best Practices” that tend to undergo change (The Turkish Cybersecurity Strategy deals at length with Best Practices; I would prefer to see them handled in a National Cybersecurity Center). The new Spanish model has a triple structure: a National Council at political level whose meetings are far apart, a Special Commission for Cybersecurity which meets often and can react on issues of principle and, for instance, Best Practives, and a Special Situation Commission which takes action when threats become manifest or incidents occur. In some countries, military cybersecurity/cyberdefense has organs of its own, in other countries, like Germany, the National for Cybersecurity, part of the Ministry of the Interior, deals inclusively with all threats. Surely there is no “one fits all” solution, and the criteria must be efficiency and transparency in the administration of the strategy.

One important in the administration of a strategy, perhaps too often overlooked in conceptual planning, is financing. It is a sad experience that coordination without the possibility of allotting funds for execution rarely functions. Yet, in the vast majority of cases reviewed, no or only minimum budget provision has been made for implementation, the US of course being the exception (and NATO which has funded its two cyberdefense centers quite adequately). In the other cases, the strategies do not even mention finances, quietly assuming that the various stakeholders, ministries and all, will provide the necessary when urgency looms.

Let me conclude my remarks with the hope that I have not only dwelt on facts and developments long known in this erudite professional assembly, thus carrying, using the famous proverb, too many “owls to Athens”.

1. “National Cyber Security Strategies. Setting the course fo national efforts to strengthen security in cyberspace”. There is also a table, “National Cyber Security Strategies in the World” dated 7 February 2013, which directly accessible links to the texts of all available strategies. [↑](#footnote-ref-1)