Approaches to Cybersecurity from Mexico.[1]

Brief considerations on cyberspace and cybersecurity

There is no single definition for the term cybersecurity, much less a harmonized one. Even the use of the term "cyber" as a form of combination or as an adjective, is used to exemplify different issues. In this sense, the first step to know about the norms, values and culture of cybersecurity is to understand what cybersecurity is and from there lay the necessary foundations in order to be able to protect the networks of the present and future.

Cyberspace is an electronic world, a global common space where people are united to exchange ideas, services and even friendship[2]. It constitutes a nervous system, which controls the countries and the critical infrastructure that sustains them. Its healthy functioning is essential for the economy and national security[3]. It is a global digital environment consisting of computer networks and telecommunications, in which people communicate and interact, allowing the exercise of their rights and freedoms, in the same way they do in the physical world[4].

And, what is cybersecurity? Cybersecurity is going to deal with the security of this cyberspace. In accordance with the definitions of the paragraph above, cybersecurity will be understood to protect that conception of cyberspace. In the case of Mexico, cybersecurity constitutes a: "set of policies, controls, procedures, risk management methods and standards associated with the protection of society, government, economy and national security in cyberspace and public telecommunication networks"[5].

As a consequence of the importance of cyberspace, governments in many countries have begun to develop strategies to protect themselves against cyber threats, to manage risks and to know their vulnerabilities, while trying to promote the benefits of a hyper connected and cyber-enabled world. In several countries, the development of national cybersecurity strategies (NCSS) has become a national policy priority[6]. For the OECD[7], national cybersecurity strategies should have two objectives: to promote economic and social prosperity, as well as to protect societies that depend on cyberspace against cyber threats, which should be done while preserving the openness of the Internet as a platform for innovation and new sources of growth.

In this situation, the Cybersecurity Strategies or National Cybersecurity Strategies[8] involve plans and actions taken to facilitate the achievement of national competitive advantage around cybersecurity. They´re designed to improve the security and resilience of national infrastructures and services. These documents articulate an approach to cybersecurity adapted to a specific national or legal context. In this sense, the implementation of the strategies must be accompanied

[1] Anahiby Becerril

[2] Government of Canada, *Canada´s Cybersecurity Strategy. For a stronger and more prosperous Canada*, 2010: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx

[3] United States Government, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

[4] Gobierno de México, Estrategia Nacional de Ciberseguridad, México, 2017: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[5] Ibídem.

[6] OECD, *Cybersecurity policy making at a turning point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD, 2012, p. 9.

[7] OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines").

[8] *National Cyber Security Strategies* (NCSS)

by a planning in the development of technology, as well as the development of skills and human capital.

Just as there is no single definition for the terms cyberspace and cybersecurity, there is no single strategy that can be follow, given the characteristics of each country. However, within them we can identify common themes, which in the end do not make us so different. These include cooperation (international and national); Human Rights protection; as well as risk management.

The National Cybersecurity Strategy (ENCS) of Mexico.

In the case of Mexico, in April 2017 and with the accompaniment of the Organization of American States (OAS), we began work on the creation of what would be the National Cybersecurity Strategy (ENCS). This effort was done through a multistakeholder approach. In this way, we were able to identify strengths, but more importantly, needs and vulnerabilities of the various sectors.

The National Cybersecurity Strategy (*Estrategia Nacional de Ciberseguridad*, ENCS) was published on November 13, 2017. It´s vision is to make Mexico a resilient nation in the face of risks and threats in cyberspace, taking advantage of the potential of ICT in a responsible way, for sustainable development in a reliable environment for all.

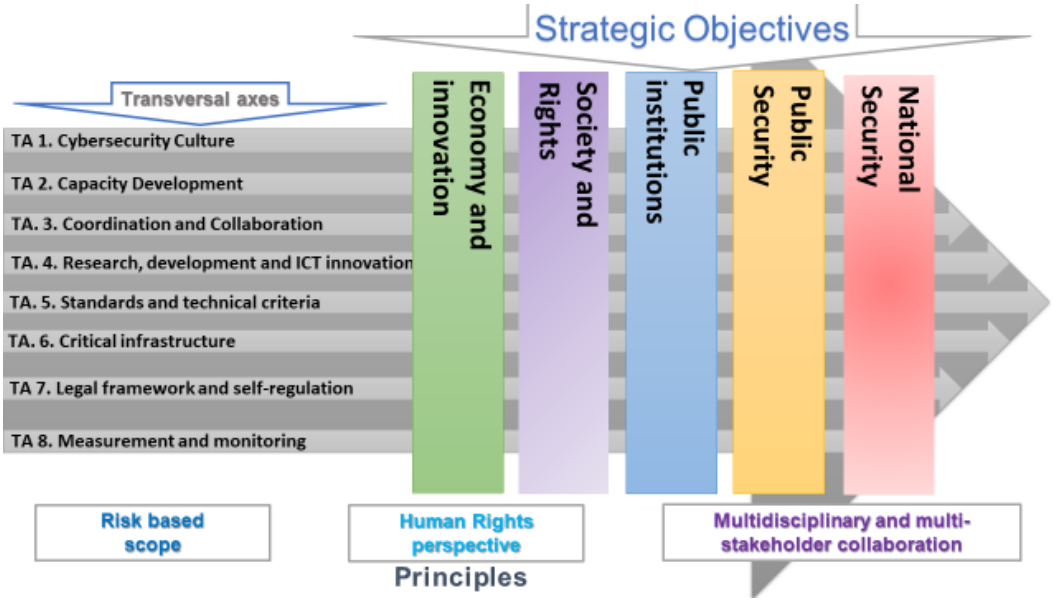

Figure 1. Structure of the National Cybersecurity Strategy

Although the ENCS was published last year, this does not mean that there were no applicable laws, norms and technical standards in the matter. However, this effort set the tone for the coordination and collaboration of the various stakeholders. In this sense, what we want to highlight from the Strategy are its guiding principles:

(a) Human Rights perspective: Contemplate in the different actions in cybersecurity the promotion, respect and fulfilment of human rights; among others, freedom of expression, access to information, respect for privacy, protection of personal data, health, education and work;

(b) Approach based on risk management: Have the ability to handle scenarios of uncertainty through preventive and corrective approaches, with the intention of minimizing the impact of the changing threats and risks of cyberspace;

(c) *Multidisciplinary and multi-stakeholder collaboration: Approach based on the multidisciplinary collaboration of the different parties (actors and sectors): with an Internet governance focus on cybersecurity, which allows the integral, transversal and holistic development of the Strategy and facilitates the open and transparent participation of them*

This last principle has been replicated in other countries of the region that have developed or are making efforts to shape their strategies. In this sense, we can consider that this principle sets the standard for a good practice within the cybersecurity issue, that is, that the thematic can be approached from a multidisciplinary and multistakeholder collaboration. Being able to work under this model allowed meeting the stakeholders, and knowing their roles and responsibilities within the ecosystem of cybersecurity. This is useful if we also consider that, the norms apply to multiple actors and that cybersecurity norms are as heterogeneous as the actors and issues.

The success of the norm rests largely on those who accept it, adding the where, how and how they do it. In this sense, the ENCS applied the path of how cyber-standards are constructed; it will configure the content and the nature of the rules that arise.

One of the transversal axes of the Strategy constitutes the creation of a cybersecurity culture. At this point, we consider the importance of awareness and sensitization. Some stakeholders, such as Federal Police, @prendeMX, INAI, as well as in academic areas, have made efforts to carry out an education and awareness of the users. However, there is still much work to be done, especially if we consider that in Mexico there are Internet users from 6 years old[9].

Cybersecurity law and norms.

As we have already mentioned, most of the countries are developing their laws on cybersecurity and we are not the exception. However, this does not mean that we did not have progress in this regard.

Recognized as a fundamental right, the protection of personal data is recognize in articles 6 and 16 of the Constitution. From there derives a Federal Law[10] and its Regulation, which bound private parties who deal with personal data and a General Law[11] that must be accomplished by the so-called "obliged subjects", who mostly correspond to the government sector. Recently[12] the country acceded to the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[13] (Convention 108), of the Council of Europe and its Additional Protocol. This is consider the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.

---

[9] Data obtained from the *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares* (ENDUTIH), 2017: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf

[10] *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[11] *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, https://www.colmex.mx/assets/pdfs/10-LGPDPPSO_57.pdf

[12] Decreto publicado en el Diario Oficial de la Federación el 12 de junio de 2018: http://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018

13 Details of Treaty No.108: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

*Criminalisation of certain cyberactivity.*Although there are provisions in the Federal Criminal Code, there are some as well as in the 32 State Codes and some Federal Laws. However, there is no uniformity at the national level in these laws. The necessary discussion on the need for a legal framework that adequately incorporates the criminal types in the matter is under development.

Code written by the technical community has created new spaces and sites where we develop our daily activities. In the same way that the codes shape possibilities for human action, they prohibit others. In this sense, we consider that they are not so different from the law and the norms.

Norms cannot be simply writing shared beliefs. I do not think we should not leave the Law out. Law can serve as a basis for formulating norms, just as law can codify norms. The creation of a law and regulatory cybersecurity framework should not fragment the Internet or have any harmful consequences for its technical operation.

While we are in the work of developing laws, standards and a culture of cybersecurity, the efforts that are made should aim not at the creation of a complex regime, but a coherent one.We know that constructing new norms is difficult. We believe that regulatory and regulatory efforts should focus on how standards will work and be applied, rather than on what they are going to say.

Anahiby Becerril