Stosunki Międzynarodowe – International Relations
nr 1 (t. 56) 2020

ISSN 0209-0961
doi: 10.7366/020909611202005

Towards a Cybersecurity Zone in North America: Exploring the Creation of a Regional Cybersecurity Complex Under the USMCA

Marco Antonio Lopátegui Torres
Autonomous National University of Mexico

Cybersecurity has been an important developing subject for International Relations as a result of the ever-evolving world, much influenced by technological innovation. Since the end of the Cold War, security analysis has been regionalised and has examined cooperation among neighbours in order to address common problems. However, classic approaches to security within the discipline are deemed insufficient in the wake of new vulnerabilities from cyberspace. In order to put cybersecurity on the agenda for the region comprised by Mexico, the United States, and Canada – and in order to understand the possibilities of a cybersecurity zone in North America – this article uses the Regional Security Complex Theory to make a proposal for a North American Cybersecurity Complex. Based on the opportunities offered by the new United States–Mexico–Canada Agreement (USMCA), the means for such a complex are explained.

Keywords: cybersecurity, regional security complex, USMCA, North America.

Within the context of constant innovation and technological advances, the opportunity for analysis regarding international security that focuses on cyberspace becomes highly important. New information technologies raise threats that had not been contemplated before within International Relations (IR); they now require the cooperation of all actors in the international society. With tendencies towards regional analyses of security, and with the help of the political and juridical tools designed on this level, security becomes essential in regional agendas and, therefore, so does cybersecurity.

With all that in mind, different approaches to security analysis have been brought out in IR studies. Here I will take into consideration the Regional Security Complex Theory (RSCT), which is a theoretical tool for a comprehensive analysis of the conditions that exist in a region for creating security complexes that are composed of the actors involved and based on security agendas about important issues for the said region or

Marco Antonio Lopátegui Torrres, MA – Associate Professor, Faculty of Political and Social Sciences, Autonomous National University of Mexico (Universidad Nacional Autónoma de México, UNAM).

members of the said group. Cybersecurity, for example, could be seen as one of those topics on the agenda for the region comprising Canada, the United States, and Mexico.

With the objective of setting cybersecurity on the tri-national agenda, this article is guided by the question of what could be the necessary means to build a regime on the matter for North America under the current political context. In order to offer a reasonable answer, the presented hypothesis argues that cooperation guided by the integration process of the region – set out in the new United States–Mexico–Canada Agreement (USMCA), which entered into force in 2020 – can be the basis for an attempt to create a cybersecurity complex in the region. Based on the experience of each country and the will to make further efforts, as stated in the Agreement, this complex can be the future for securitisation in cyberspace.

Taking this into consideration, I believe that the RSCT is the most appropriate approach to address the opportunity of building a cybersecurity complex in North America. This theory makes it possible to take into account multiple actors and factors in the analysis of security of a certain region based on the will of the States within it and its processes towards integration. Hence, it allows for a full analysis of the current status and the opportunities for the future.

The Regional Security Complex Theory as an analytical tool for cybersecurity in North America

Ever since the end of the Cold War, the international security agenda has been regionalised. With the culmination of bipolar confrontation, numerous conflicts arose or became more visible worldwide as tensions between the superpowers were not totalising; multiple topics on the security agenda had important regional implications, without necessarily affecting the entire international system. Likewise, concerns ceased to be exclusively military and the agenda was no longer centred around nuclear weapons; rather, numerous issues emerged based on the threats and priorities in each region. Hence, it was necessary to use a theory that focused on regional and not only on worldwide security, as realism had, or one that focused on the global construction of the security agenda, such as constructivism.

Thus arose the RCST, which provides analytical tools to address the issue of cybersecurity from a regional stance based on the composition of security complexes and not from the viewpoint of international politics or either economic or technological development. This approach can include non-state actors, incorporate both local and interregional levels, and allow for particular circumstances of time and place to determine the preponderance of actors and factors.[1] Likewise, it recognises changes in the composition of the security agenda, allowing for an analysis of a variety

[1] Barry Buzan and Ole Weaver, *Regions and Powers: The Structure of International Security* (United Kingdom: Cambridge University Press, 2003), 12.

of non-traditional issues and actors within international security, such as military tactics, weapons, and politics.[2]

With all that said, it is necessary to define a Regional Security Complex (RSC) in order to fully understand the proposal of this research regarding the construction of a complex of this kind for North America, one which would focus on cybersecurity. The definition offered by Barry Buzan and Ole Weaver is: "[A] set of units whose major processes of securitisation, desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another". This axiom has evolved not to focus solely on the State and military policy,[3] but also to consider the possibility of different actors and various security sectors.[4]

This way, the RSCT has been chosen to address the issue of cybersecurity in North America, since "it offers the possibility of systematically linking the study of internal conditions, the relationships between the units in the region and the interaction of the regional dynamics with powers [and threats] that act globally".[5]

A holistic approach to cybersecurity based on the RSCT will make it possible to move away from the visions of the knowledge-based economy and technological innovation that are commonly used to study the phenomena of ICTs, as these analyse the problem from the point of view of the threats and risks that arise and develop in cyberspace. It does not see the development of ICTs merely as a part of the technological dynamic; rather, it focuses on the possibilities of damage to critical infrastructure, the penetration of military systems, or the theft of classified information as possible national and international security problems.[6] The RSCT is a reminder of the fact that we are not interested in development or interactions in cyberspace, but, rather, in addressing the risks and threats to security that occur in the virtual terrain so that we could tackle such problems.[7]

In this context, cyberspace can be seen as a new field of interaction for society. It is a social dimension whereby a lot of our activities as humans can take place through the Internet: from information exchange to shopping, working, and socialising. However, according to Luis Joyanes, due to its risks and threats, it should also be regarded as a possible battlefield.[8]

Also, for the present research, I will use the concept of securitisation[9] as the main theoretical tool to map regional variation. A theory based on securitisation makes it

[2] Buzer and Weaver, 17–18.

[3] Buzer and Weaver, 201.

[4] Buzer and Weaver, 44.

[5] Buzer and Weaver, 52.

[6] Buzer and Weaver, 76.

[7] Buzer and Weaver, 76.

[8] Luis Joyanes Aguilar, *El estado del arte de la ciberseguridad* (Madrid: Instituto de Estudios Estratégicos, 2011), 30.

[9] Securitisation should be understood as the process under which a topic that might pose a threat goes from being non-politicised (i.e. there are no political actions or policies that would face it) through being

possible to point out that security agendas are focused on different things in different regions; the actors differ and so does the relative importance of the different sectors.[10] In this case, I will seek to use North America as the focal point for the proposal towards the securitisation of cyberspace.

Authors such as Alejandro Chanona have previously used the RSCT to understand security in the region based on its dynamics for cooperation and its process towards integration.[11] Because of that, it must be kept in mind that regional integration between the US, Canada, and Mexico revolves around the free-trade area created by the North American Free Trade Agreement (NAFTA) in 1994 and sustained today by the USMCA.[12]

Talking about cybersecurity, Mark Raymond stresses the importance of both formal and informal institutions for cooperation.[13] On the formal side, legal documents are – as in any other regime, cooperation effort, or regional integration – fundamental to fully developing a cybersecurity regime. On the other hand, institutional cooperation is key to putting it into action from what could be seen as an informal stance. Thus, the main emphasis in this paper will be on the entry-into-force of the USMCA as the basis of a cybersecurity complex with the aim of inter-institutional cooperation across the borders of the three countries.

With all that in mind, and based on the parameters of the RSCT, I will undertake an analytical tour around the creation process, the operation, the current conditions, and the perspectives of a prospective regional cybersecurity complex among the three members of the USMCA by taking into consideration the following elements of practical analysis:

1) the background shared between the units in the CSR and how it conditions the main cybersecurity actors and the agenda they generate;
2) the main cybersecurity actors, problems, and reference objects that will define the CSR in cyberspace, and the nature of the processes that created it and sustain it as a formation process;
3) the essential structure of the region (anarchy or integration, distribution of power and patterns of friendship–enmity, securitisation–desecuritisation);

politicised (i.e. there are actions to tackle it, e.g. allocating resources), and even beyond all the way to being securitised (by presenting it as an existential threat with a need for immediate action). *See* Barry Buzan, Ole Weaver and Jaap de Wilde, *Security: A new Framework for Analysis* (London: Lynne Rienner Publishers, 1998), 42.

[10] Buzan and Weaver, *Regions and Powers*, 85–86.

[11] *See* Alejandro Chanona, "Regional Integration and Security: A Comparative Perspective of the European Union and North America," *Norteamérica* 1, no. 1 (2006), 100. Centro de Investigaciones sobre América del Norte–UNAM.

[12] Andrés Malamud, "Conceptos, teorías y debates sobre la integración regional," *Norteamérica* 6, no. 2 (2011): 236–237. Centro de Investigaciones sobre America del Norte–UNAM.

[13] Mark Raymond, "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot," *Strategic Studies Quarterly* 10, no. 4 (2016), 132. Air University Press.

4) the interregional and global dynamics that the North American cyberspace regional security complex will have;
5) the relative weights of the domestic, regional, interregional, and global levels, as well as that of the trends of securitisation of cyberspace;
6) the most likely scenarios for the future given the current condition and dynamics of the CSR in cyberspace.

Throughout the following sections, each of these points will be addressed with the aim of building a methodological proposal that will make it possible to determine the possibilities and the already existing opportunities for the construction of a cybersecurity complex.

The position of the USMCA members and their determining conditions in the region

The first aspect to consider is the immediate background and the general conditions of each member of the USMCA; only this will allow for determining if there is a possibility of building a regional cybersecurity complex between them. These are characteristics related to the telecommunications infrastructure as well as the access and use of cyberspace. This will be the first approach in identifying the main differences between the countries, which could condition the construction of a regional cybersecurity complex in North America.

It is pertinent to start with the most important actor in the region, namely the United States, which has a population of over 330 million people and Gross Domestic Product (GDP) of 21,428 trillion dollars (2019)[14], ranking as the world's leading economy. Since the beginning of the 20th century, it had emerged as a power of worldwide importance, but it was at the end of World War II that it took its place as a global superpower. After the attacks on the World Trade Center in 2001, it began to securitise the international agenda, with clashes in different areas of the Middle East and some political and economic disputes with actors such as Russia, China, and North Korea. Although it cannot be considered the only superpower, it is a hegemonic actor and a key player in global security. Corresponding with its importance and economic value, its telecommunications infrastructure occupies the fourth position.[15] It has more than 313 million people who access the Internet, reaching 94% of Internet penetration, which makes it the tenth country with the highest number of connected inhabitants in relation to its total population.[16]

[14] *GDP (current US$)*, The World Bank, last modified 2019, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?name_desc=false&view=chart.

[15] Soumitra Dutta, Thierry Geiger and Bruno Lanvin, cords, *The Global Information Technology Report 2015: ICTs for Inclusive Growth,* accessed August 25, 2020, http://www3.weforum.org/docs/WEF_GITR2015.pdf.

[16] *Internet Users and 2019 Population in North America,* Internet World Stats, last updated May 9, 2019, https://www.internetworldstats.com/stats14.htm.

Mexico is a country with more than 127 million inhabitants (2019). It is considered a developing economy with GDP of 1,258 trillion dollars (2019), which places it as 15th among economies globally.[17] Despite being an important economy, which is part of the G-20 and the Organisation for Economic Co-operation and Development (OECD), its position in telecommunications infrastructure worldwide is 81st out of 143 countries (2016). Its Internet penetration, although it has been growing, still has a significant percentage of the population lagging. Based on data from the Mexican National Institute for Statistics and Geography (INEGI) and the Mexican Internet Association, 44.3% of Mexican households have a computer (less than half),[18] while the total number of Internet users in Mexico has reached 82.7 million, which represents 71% of Internet penetration.[19]

Canada can be placed as the third country regarding population numbers in the region, with 37,589,000 inhabitants; however, with GDP of 1,736 trillion dollars (2019)[20], it ranks as the tenth global economy. Although its international performance has undergone various changes throughout history, traditionally Canada is not considered a military power and its foreign policy "... has been based on its moral and progressive reputation since it guards and promotes respect for international institutions; it has managed to overcome its alliances and differences with the governments of the United States and is considered a persuasive actor among the international community"[21]. Although its vast physical expanse could be seen as a problem (since it is the fourth largest country in the world), Canada is the sixth country with the largest telecommunications infrastructure (according to the World Economic Forum[22]) and has more than 35.5 million people with Internet access, which makes it the seventh country in the world, with more than 95% of Internet penetration.[23]

With this first approach, one can observe the current state of each of the countries that make up the USMCA in order to have a general picture of the economic conditions and access to the global network at the time of the entry-into-force of the said Treaty. Likewise, the basic data shows an uneven map of Mexico in relation to the United States and Canada. It is possible to observe a relationship between GDP and the

[17] *Mexico*, The World Bank, last updated 2019, https://data.worldbank.org/country/mexico?view=chart.

[18] *Disponibilidad y Uso de TIC,* Instituto Nacional de Estadística, Geografía e Informática [INEGI], last updated 2019, https://www.inegi.org.mx/temas/ticshogares/.

[19] *15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018: Movilidad en el Usuario de Internet Mexicano*, Asociación de Internet, July 31, 2019: 4, https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/15%2BEstudio%2Bsobre%2Blos%2BHa_bitos%2Bde%2Blos%2BUsuarios%2Bde%2BInternet%2Ben%2BMe_xico%2B2019%2Bversio_n%2Bpu_blica.pdf.

[20] *Canada*, The World Bank, last updated 2019, https://data.worldbank.org/country/canada?view=chart.

[21] Athanasios Hristoulas, "La política de seguridad canadiense: pasado, presente y futuro," in *Seguridad y defensa en América del Norte: Nuevos dilemas geopolíticos* (Washington, D.C & San Salvador: Woodrow Wilson International Center for Scholars & Fundación Dr. Guillermo Manuel Ungo, 2010), 103–151.

[22] Dutta, Geiger and Lanvin, *The Global Information Technology Report 2015*, 161.

[23] *Canada*, Internet World Stats, last updated May 12, 2018, https://www.internetworldstats.com/am/ca.htm.

telecommunications infrastructure that each country has with its level of Internet penetration; although the relationship is not direct, it is causal.

The heterogeneous composition of the region is evident since its members have very different conditions. Their economic, political, and military importance is uneven, as is their relevance to the international system. However, despite these differences, these countries have been able to generate significant cooperation schemes, such as the NAFTA and the USMCA. This is because each of these states has a defined role in the region and understands that there is interdependence as they share almost twelve thousand kilometres of borders.

The commercial and human capital exchange between these three actors is one of the most active in the world. The USA–Canada border is the longest one in the world at 8,891 kilometres in length and there is a commercial exchange of more than 615 billion dollars a year.[24] Moreover, the USA and Mexico share 3,100 kilometres of border and a daily exchange of more than 1.6 billion dollars in goods and services, which makes up about 590 million dollars annually. Also, migration between the two countries amounts to approximately 3 million people a year.[25] The United States is Mexico's first commercial partner and first migration destination. It is also Canada's first commercial partner and first migration destination. On the other hand, Canada and Mexico are, for the United States, the second and third trading partners respectively (surpassed only by China).

This data reveals a heavy interdependence between the three countries. It has prompted each actor to seek the strengthening of their relationships and improve cooperation schemes; especially on economic, political, and security issues. Although conditions are unequal, in the last 70 years the three countries have demonstrated a cordial relationship and in the last 30 years they have generated mutually beneficial co-responsibility agreements on issues of interest to each one of them.

Based on this background and data about what each member represents for its partners, a starting point can be established in order to consider that cooperation in the construction of a cybersecurity complex *is* possible as long as the said topic is on the political agendas of each of the States involved. The inclusion of the subject in one of the USMCA's sections reveals that it is not a matter outside of their agendas, but, rather, one which is of mutual interest. In the fourth section of this article, I will go deeper into the guidelines established in the USMCA on the subject of cybersecurity; however, before that, I will continue with the analysis of the region's structure, the role of each member for the region and the rest of the world, their dynamics, and how their integration schemes have evolved.

[24] Héctor Usla, "Canadá rebasa a México en comercio con EU," *El financiero*, July 3, 2020, https://www.elfinanciero.com.mx/economia/canada-desplaza-a-mexico-como-mayor-socio-comercial-de-eu.

[25] Gerardo Lissardy, "Frontera Estados Unidos-México: Por qué para Trump es (casi) imposible cerrar la frontera con México como hicieron otros presidentes de EE.UU," *BBC News Mundo*, New York. April 24, 2020, https://www.bbc.com/mundo/noticias-america-latina-48028600.

The regional structure and dynamics among the USMCA members

Given the general data, it is possible to analyse the second point and thus determine the general structure of the region and the dynamics between the members of the USMCA. I will focus on the position that each country has in the international arena and, in consequence, define the status of each country. With this, I will try to provide a sketch of the distribution of power, of some dynamics, and of how integration schemes have evolved within the region. Although some background references are to be made, such as the NAFTA, the main emphasis will be on the entry-into-force of the USMCA.

Based on the levels of differentiation established by Buzan and Weaver around the scope of the power of a State,[26] each member of the USMCA can be described as follows:

- The United States is a "superpower." It has a broad-spectrum influence throughout the international system as well as first-class military-political capabilities and an economy that supports these capabilities. It is also an active actor in the securitisation and desecuritisation processes in all (or almost all) the regions of the system, be it as a guarantor, a threat, an ally, or an intervening party.[27]
- Mexico is a "regional power", i.e. its capabilities are important only in its own region. Mexico is a relevant actor for North America, Latin America, and the entire continent within the OAS, but it does not have much influence on the global level. It influences the securitisation processes in its region, but its limited political, military, and economic capacities exclude it from being a systemically important actor.[28]
- Canada is a "great power" in the system. It has a less demanding status in terms of capacity and behaviour on the global level than superpowers do. It has great economic and political capacities, but not outstanding in all sectors, and it is not actively present in the securitisation processes of all areas of the international system, but it is a state taken into account by the superpowers for alliances and the distribution of global power.[29]

Understanding this composition on the individual level for each member makes it possible to reveal the essential regional structure, which is based on the leadership of the United States and a moderate counterweight achieved by Canada and Mexico, each in their own way. Therefore, together they compose a region with unequally distributed power, but with patterns of cooperation, mutual assistance, and securitisation backed by the military and technological resources of the United States.

Historically, the relationships between the members of the USMCA were rather rough. Each country took its neighbours into account in a strategic manner and tried

[26] Buzan and Weaver, *Regions and Powers*, 34.
[27] Buzan and Weaver, 34–35.
[28] Buzan and Weaver, 37.
[29] Buzan and Weaver, 35.

to make them allies in order to achieve its foreign policy objectives in the region[30] through relationships based solely on convenience regarding economic, political, social, security, and population topics, in addition to geographical proximity.[31] There were no attempts at integrating at the regional level, which is why relations between them developed bilaterally. It was not until 1990 – when the United States, Mexico, and Canada began the negotiations for the NATFA – that a leap towards the evolution of regional relations was made.

Among the determining factors for the integration of these three North American countries were the processes of economic globalisation and an increase of insecurity factors on the international level. "The importance of these two circumstances has been reflected in the creation of strategies and organisations that help improve the conditions and quality of life of the population of these three States, as well as the relations between them."[32] These factors intensified the international cooperation agenda in North America and aimed at increasing support and security in the region. The NAFTA entered into force on January 1, 1994.

After the terrorist attacks of September 11, 2001, the interests of the superpower turned towards the protection of its territory. In consequence, its relations in the region focused solely on border security, securitising the regional agenda, and leaving aside issues important to its neighbours, such as economics, immigration, the environment, or drug trafficking.[33]

The NAFTA was followed by several agreements – some even regarding topics of joint security – the most important of which included the Smart Borders programme in 2002 and the Alliance for Security and Prosperity of North America (ASPAN) in 2006. Both agreements had the intention of "building new spaces of cooperation to provide greater security, making companies more competitive and the economies more solid".[34] However, these pacts did not have the expected solidity in their execution, although the leaders of the three countries did realise that two developed economies and one developing economy had good conditions for strengthening each other through the cooperation.

The NAFTA was fulfilling its purpose, since between 1993 and 2015 trade amongst the three countries quadrupled, going from $297 billion to $1.14.[35] Factors such as the economic rise of China, the increase in organised crime, and the arrival of Donald

[30] However, they also came to have political and military conflicts for territorial and economic reasons, such as in the period of the expansion of the United States, when it had a confrontation with Mexico and annexed part of its territory.

[31] Elma del Carmen Trejo García, *Alianza para la Seguridad y la Prosperidad de América del Norte (ASPAN)* (Mexico: Servicio de Investigación y Análisis, Dirección General de Bibliotecas, Cámara de Diputados, 2006), 1, http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-02-06.pdf.

[32] Elma del Carmen, 2.

[33] Elma del Carmen, 5.

[34] Elma del Carmen, 2.

[35] "Del TLCAN al T-MEC: La historia del acuerdo comercial," *Milenio*, México City, June 30, 2020, https://www.milenio.com/negocios/del-tlcan-al-t-mec-la-historia-del-acuerdo-comercial_2.

Trump to the presidency of the United States were ones that prompted the renegotiation of the NAFTA.

As the Chinese economy began to displace Mexico and Canada as the main trading partners of the United States, the US economy required strengthening through economic agreements with its neighbours. By 2016, Donald Trump had won the candidacy for the presidency of the Republican Party and throughout the electoral process he attacked that agreement and claimed it was unfair to the US. Once installed in the White House, Trump threatened to remove the United States from the NAFTA if it did not modernise.[36]

In August 2017, the NAFTA renegotiations began in the city of Washington. Later, in September 2018, an agreement was reached between the three countries to update the NAFTA, but it had so many modifications that it was more efficient to replace it with a new pact, which they named the United States–Mexico–Canada Agreement (USMCA). On November 30 of that same year, Presidents Donald Trump, Enrique Peña Nieto, and Justin Trudeau signed the Agreement within the framework of the Group of 20 (G20) summit in Buenos Aires, Argentina.[37] The USMCA came into effect on July 1, 2020.

This brief review of the integration mechanisms in North America is directly related to the proposal of creating a cybersecurity complex in the region, since it shows the political will that the three countries in question have had to generate mutually beneficial agreements. Moreover, the active leadership of the United States can be noticed, but the firmness of its neighbours to negotiate and include issues of interest to them in the agenda could be seen, too. Also, the intention of the superpower in the region to push forward securitisation issues was emphatic, particularly after September 11, 2001.

At this point in the research, it is possible to propose the securitisation of cyberspace in North America, mainly due to the fact that it is an issue reflected in the USMCA, which implies that it is a matter of interest to the three countries. Therefore, in the next section I will present the current cybersecurity conditions in the USMCA member countries, which will provide guidelines for analysing the intentions of the Agreement and making proposals for the construction of a regional cybersecurity complex.

What are the current cybersecurity conditions in each USMCA member country?

As the third point, issues and reference objects regarding cybersecurity for the region will be addressed, as well as the strategic response of the USMCA members in the process of the securitisation of cyberspace will be elaborated. In order to understand the relevance of the topic, it is necessary to define what cybersecurity is and what its importance relies on. Later, I will review some incidents and problems that each of the USMCA countries have had in this area, as well as the strategies that each one has tried to develop in order to respond to threats to their cybersecurity.

[36] "Del TLCAN al T-MEC".

[37] "Del TLCAN al T-MEC".

For many analysts, there are four physical dimensions where there are conflicts, namely land, sea, air, and space. However, for three decades now, the dangers have reached the fifth domain: cyberspace.[38] As such, cyberspace can be seen as an environment for the interaction of international society. It is a non-physical space where battles are also fought, although consequences do not only remain in the virtual dimension but also affect the physical world in various ways and with significant magnitudes. Moreover, confrontations, risks, and threats that can occur to a country both internally and externally in the four physical environments can also be reproduced in cyberspace.

Starting from its immense capacity regarding access and information exchange with others, a cyber-threat can reach hundreds of millions of potential victims in a few seconds. Considering the amount of information on national and international security that is stored and exchanged online, cyber-liabilities can have devastating consequences. Based on this understanding, it is essential to maintain a secure cyberspace.

According to Gina Marie Hatheway, the director of the Microsoft Cybersecurity Solutions Group, "Cyberspace is the new battlefield, there is no discrimination in cybersecurity, everyone can be a victim of cyber threats, so challenges must be assumed to reduce the gaps in cybersecurity".[39] The issue of cybersecurity has been on the rise for a decade on the governmental level, too, especially within ministries of security, in international defence cooperation organisations such as the NATO, and other international institutions, both private and public, such as the ITU. With the growth of people accessing global networks and the possibility of attacks ranging from highly targeted ones against companies or sectors to attacks on entire countries and regions, cyberspace is becoming ever more important day by day.

Cybersecurity is emerging as a new vision for reducing the vulnerabilities derived from the use of cyberspace, which requires solutions that are consistent with its configuration and with the associated problems. Securing cyberspace is difficult, because this space is used by society for interaction and production, so it is its connectivity that is promoted, not its security. In order to face multiple threats, any cybersecurity strategy must involve protecting both data and people.

This approach strives to preserve the availability and integrity of networks and infrastructure, as well as the confidentiality of the information contained therein. Therefore, a whole "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 is required."[40]

[38] "Cyberwar: War in the Fifth Domain," *The Economist*, United Kingdom, June 1, 2020, http://www.economist.com/node/16478792.

[39] Stephanía Oliver, "La ciberseguridad no es prioridad en México," *El Universal,* January 26th, 2020, https://www.eluniversal.com.mx/techbit/la-ciberseguridad-no-es-prioridad-en-mexico.

[40] Gobierno de México, *Estrategia Nacional de Ciberseguridad* (México: Gobierno de México, 2017), 27, https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

Understanding the risks causes international actors to share an interest in staying safe from attacks within transnational networks and with regard to information structures that make up cyberspace, since “a small skirmish in cyberspace could be the precursor of a major cyber-conflict and unleash a regional escalation that would have international repercussions”.[41] As James Forsyth points out, each State faces its cybersecurity dilemma and, therefore, it must also cooperate with other States, since network vulnerabilities are created from within and from outside, and there can be both national and transnational threats. “Not for another reason than survival, States have no choice but to work together to modulate these vulnerabilities”.[42]

Given the difficulty of locating the origin of cyber-attacks and the wide scope they might have, there must be cooperation and coordination between public and private, national and transnational actors, even though each nation faces different cybersecurity problems. Likewise, it should be states that promote and lead such efforts. This is what should concern the member countries of the USMCA with regard to the issue of cybersecurity, namely the need to cooperate and strengthen each other in order to reduce vulnerabilities, face threats, and increase the resilience of cyberspace in the region.

So far, each member of the USMCA has acted separately, making its own efforts concerning cybersecurity. Each has individually gone through different paths that can be taken up again as a point of reference in order to understand the main instances and actions that can sustain a Regional Cybersecurity Complex in North America.

The United States is a country that is the target of the biggest number of cyber--attacks in the world annually.[43] Its importance globally, its technology companies, the size of its economy, and its Internet penetration all make the nation the main target for attackers. Suffice to consider some events, such as the classified documents that were revealed by Wikileaks, followed by the attacks of the Anonymous organisation against companies such as Amazon, ETECSA, and PayPal in 2010; as well as several attacks during the presidential election systems in 2016 in thirty-nine states, including intrusions into databases of voters, software systems, and e-mails from the Democratic Party.[44]

In response to these attacks, and being aware of the threats to national security, the US government has developed some cybersecurity strategies. The lines of action have been dictated by consecutive presidents and have evolved; they have been applied by the Department for Homeland Security. The most recent policy is from President

[41] John Bumgarner, *Jane’s Defence Weekly*, (September 29, 2010): 92, www.jdw.janes.com.

[42] James Forsyth and Maj. Billy E. Pope, “Structural Causes and Cyber Effects: Why International Order Is Inevitable in Cyberspace?,” *Strategic Studies Quarterly* (Winter 2014): 123, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-08_Issue-4/Forsyth.pdf.

[43] “Ransom ¿qué? El ciber secuestro de datos con el código malicioso Ransomware,” *Lockton International*, June 23, 2020, https://www.locktoninternational.com/mx/articles/ransom-que-el-ciber-secuestro-de-datos-con-el-codigo-malicioso-ransomware.

[44] Michael Riley and Jordan Robertson, “Ciberataque ruso en elecciones de EU es más grande de lo que se creía,” *El Financiero and Bloomberg*, June 13, 2017, http://www.elfinanciero.com.mx/mundo/ciberataque-ruso-en-elecciones-de-eu-es-mas-amplio-de-lo-que-se-creia.

Donald Trump and is outlined in the Cybersecurity and Infrastructure Security Agency Act of 2018. This legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within the Department of Homeland Security as well as creating the Cybersecurity and Infrastructure Security Agency (CISA), which develops the national capacity to prevent cyber-attacks and work with the federal government to provide cybersecurity tools, services for incidents, and capabilities of evaluation to safeguard networks.[45]

Moreover, the United States has its Cyber Incident Response System through the Department of Homeland Security (DHS), from which it assists potentially impacted entities, analyses the potential impact on critical infrastructure, and investigates those responsible for the attacks. In conjunction with law enforcement bodies, it coordinates the national response to cyber incidents. It collaborates with other agencies – federal and local – takes part in cybernetic complementary missions, and works with owners and operators of the sector to ensure greater unity in the efforts towards security and nationwide response to cyber-incidents.[46]

In the case of Mexico, the lack of awareness and culture of prevention is the greatest vulnerability that exists in terms of cybersecurity. A study called *User habits in cybersecurity in Mexico 2019*, published by the federal government, concluded that 27% of the study participants had suffered identity theft in digital media, while 21% were victims of financial fraud.[47] The Lockton insurance company reveals that crimes and threats of cyber-attacks increased by 215% in Mexico from 2017 to 2019, within which the sectors with the highest number of incidents were financial and insurance services, as well as mass media. One example of this was the 'WannaCry Virus' in 2017, which affected more than 200 thousand computers around the world, of which the most affected country in Latin America was Mexico, including a case registered in April 2018, when five Mexican banking entities were hacked through its SPEI platform, producing an approximate loss of 300 million pesos.[48]

To face these risks, Mexico's National Cybersecurity Strategy (ENC) was created at the end of 2017; it serves as a reference to create a regulatory framework that adds to the existing legislation, such as the Federal Personal Data Protection Law and regulations for public and private entities. However, no new programmes have been generated, nor has an executing mechanism for the strategy been created. Not even a budget has been allocated by the federal government, so the ENC seems to consist only of good intentions. Therefore, Mexico relies on other entities, such

[45] *Cybersecurity*, Homeland Security, accessed September 1, 2020, https://www.dhs.gov/topic/cyber-security.

[46] *Cyber Incident Response*, Homeland Security, last updated November 26, 2018, https://www.cisa.gov/cyber-incident-response.

[47] Oliver, "La ciberseguridad."

[48] NOTIMEX, "México, el tercer país con más ciberataques en el mundo: Estudio," *El Financiero*, January 9, 2019, https://www.elfinanciero.com.mx/tech/mexico-el-tercer-pais-con-mayores-ciberataques-el--mundo-estudio.

as the National Centre for Investigation and Security (CISEN), which oversees the generation of intelligence and tactics to face cyber-risks. It also has the Incident Response Center (CERT-MX), whose task is to respond to computer emergencies and run cybercrime investigations.[49]

Canada, even with its large infrastructure, is not immune to attacks, as it was also one of the countries most affected by the WannaCry attack. It has been a target for attacks on its companies and attempts at military interference, such as in 2018, when they had to respond to a threat that came from Eastern Europe. The Canadian government also came under fire on August 15, 2020, when approximately 11,000 online governmental service accounts were reported to have been the victims of hacking attempts.[50]

The Canadian Cyber Security Centre is the authority on the matter, seeking to coordinate cybersecurity advice, guidance, services, and support for the government, property owners, and critical infrastructure operations. They have also designed several national cybersecurity strategies, of which their latest edition is from 2018. It includes numerous initiatives, such as the consolidation of the Centre and the establishment of the National Cybercrime Coordination Unit within the Royal Canadian Mounted Police.[51]

The superpower conditions of the United States make it a target for cyber-attacks, but Canada and Mexico also have too many risks. All three countries have acted on their cybersecurity, but not on the same level of priority. On the one hand, the United States and Canada remain at the forefront, generating strategies in maximum periods of three years and assigning a specific agency to coordinate efforts, while Mexico carried out its first national strategy in 2017, and one which is not being executed in an optimal way. This explains why in the ITU Global Cybersecurity Index 2018 the United States is placed second in the ranking, with Canada not far behind, i.e. in the 9th position, while Mexico ranks only 63rd.[52]

By knowing the general conditions of cybersecurity in the USCMA members, reference objects can be established, from which the measures that will define the Regional Cybersecurity Complex can be proposed. Likewise, recognising the inequalities between the members, their ways of responding to risks, and the position that each has in the matter will allow for making balanced, viable, and prudent proposals that can be carried out in the course of the construction of the said complex.

[49] Rafael Fernández MacGregor B (cord), *Perspectiva de ciberseguridad en México*, (México: McKinsey&Company and COMEXI, 2018), 10, https://consejomexicano.org/multimedia/1528987628-817.pdf.

[50] Gabrielle Ladouceur Despins, *Cyber attacks: Several Canadian government services disrupted*, August 24, 2020, https://www.welivesecurity.com/2020/08/24/cyber-attacks-canada-revenue-agency-government/.

[51] *National Cyber Security Strategy*, Government of Canada, (Public Safety Canada: Canada, 2018), II–III, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

[52] *Global Cybersecurity Index 2018*, ITU (ITU Publications, 2018), 63–64, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

As already mentioned, regional securitisation in cybernetical matters is possible due to the fact that the three members of the USMCA have included the issue of cybersecurity in their political agendas, to the extent that they added it in the most important integration agreement in the history of North America. Therefore, it is necessary to review the guidelines established in the USMCA for this matter.

Cybersecurity in the USMCA and the foundations for building a regional cybersecurity complex in North America

The fourth point of my analysis focuses on the approach that the USMCA has towards cybersecurity as well as on the fundamental principles that should guide a regional cybersecurity complex for North America in terms of proposals focused on securitising cyberspace in the region. In this section, I directly review the way the USMCA addresses the issue of cybersecurity. Based on what the treaty itself indicates, I will explain to what extent the USMCA provisions provide the basis for a regional cybersecurity complex in North America.

The Agreement is the most important international treaty in the history of North America. As a substitute for the NAFTA, it entered into force on July 1st, 2020. The negotiations that took place between 2017 and 2018 to modernise the NAFTA made it possible to retain the key elements of the commercial relationship between the United States, Mexico, and Canada while incorporating new and updated provisions that aimed at responding to the challenges of the 21st century. "Strengthening the rules and procedures regarding trade and investment, this agreement has proven to be a solid basis for strengthening the already strong economic ties between the three nations".[53]

These are the most relevant points of the USMCA[54]:

- It promotes the growth of digital commerce and strengthens the protection of consumer data;
- It provides greater access to financial services and more opportunities for financial institutions in the markets of the region;
- It adapts the agreement to the continuous evolution of the telecommunications sector, optimising the infrastructure and free-market conditions necessary to encourage its future development;
- It incorporates mechanisms for dialogue and collaboration to promote the participation of Small and Medium Enterprises in regional trade;
- It strengthens and amplifies the protection of workers' rights;
- It establishes clear obligations to cooperate in the fight against corruption;

[53] "¿Qué es el T-MEC y por qué es importante para México?," *Forbes México*, July 1, 2020, https://www.forbes.com.mx/economia-que-es-el-t-mec-y-por-que-es-importante-para-mexico/.

[54] "T-MEC," *Forbes México.*

- It incorporates provisions that regulate the activity of the companies owned by the state in order to prevent distortions in trade and investment flows between the members.

In contrast to the NAFTA, the USMCA presents two important modifications:[55]

1) The NAFTA has 22 chapters, while the USMCA is made up of 34 chapters, where the additions and modifications to the chapters imply important changes in topics such as regional content, the fight against corruption, wages, environment, and digital commerce (where cybersecurity is included);
2) The Agreement will have a periodic evaluation; it will be valid for 16 years, but it will be reviewed every 6 years.

As said, among the most significant modernisations in the Agreement is Chapter 19, which refers to digital commerce. This topic is one of the most important additions, as during the elaboration of the NAFTA this issue was barely glimpsed. However, with the evolution of ICTs, digital commerce has become one of the main means for exchange and a very important value creator sector, whose development will reach incalculable levels of relevance in the world economy. Hence, the inclusion of a chapter on digital commerce "seeks to promote the growth of interactive computer services to promote the development of information platforms, the interaction between users, multimedia content, increased commercial activity, and business opportunities".[56]

With this in mind, the main benefits that this chapter of the USMCA aims to attain are as follows:[57]

- generating and promoting the innovation of high-quality digital content, products, and services, which will allow for transforming the way in which people and companies interact;
- strengthening and promoting the development of digital commerce through a legal scheme that encourages electronic operations and, at the same time, provides security for users of electronic media;
- promoting safe digital environment.

This last point is further explained in article 19.15: "Cybersecurity". In this section, the Agreement recognises that threats to cybersecurity undermine confidence in digital commerce, for which two intentions are raised in this matter:[58]

[55] *Agreement Between the United States of America, the United Mexican States, and Canada 12/13/19 Text*, Office of the United States Trade Representative, accessed on September 1, 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[56] César Buenrostro, *Retos y oportunidades del comercio digital ante el T-MEC*, (KPMG, August, 2020), https://www.delineandoestrategias.com.mx/blog-de/retos-y-oportunidades-del-comercio-digital--ante-el-t-mec?utm_campaign=Delineando%20Estrategias&utm_medium=email&_hsmi=93449194&_hsenc=p2ANqtz-9u1wocw5OyK5nCt_VbIRJ-NtXh0DEhQKuNK3SxAJBD4LymSUuYMri8IUWOV8lCM_CVugzRyyuXLUXmpWV1ZHs398sa0Q&utm_content=93448806&utm_source=hs_email.

[57] "T-MEC," *Forbes México.*

[58] "Chapter 19" in *Agreement Between the United States of America, the United Mexican States, and Canada 12/13/19 Text*, Office of the United States Trade Representative, accessed on September 1, 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

a) to build the capabilities of their respective national entities responsible for a cybersecurity incident response;
b) to strengthen the existing collaboration mechanisms for identifying and mitigating malicious intrusions or dissemination of malicious code that affect electronic networks, and using those mechanisms to swiftly address cybersecurity incidents as well as for sharing information for awareness and best practices.

These two points could be projected as the main objectives that should be worked on at the regional level in terms of cybersecurity. These would be the foundations for a whole joint strategy that allows for building a regional cybersecurity complex in North America.

Also, due to the changing nature of threats to cybersecurity, the USMCA members recognise that risk-based approaches can be more effective than prescriptive regulation in addressing those threats. Thus, the intent is set to employ – and encourage that companies also do so within their jurisdiction – risk-based approaches that rely on agreed standards and risk management practices in order to identify and prevent cybersecurity risks as well as to detect, respond, and recover from cybersecurity events.[59] This way, a main strategic line is set based on cooperation, the strengthening of response centres, multi-stakeholder collaboration, a consensus of the parties, and risk management; it is all focused on prevention, response, and cyber-resilience.

With these approaches – based on what the USMCA focally establishes for cybersecurity in the region – and the analytical part based on the Regional Security Complex Theory, it is possible to offer some proposals for a possible configuration of the securitisation of cyberspace in the North American region as well as the construction of a regional cybersecurity complex.

Proposals for the construction of a regional cybersecurity complex

In the section herein, proposals are made regarding the measures and schemes that must be applied to achieve the securitisation of cyberspace in North America, which are based on the USMCA and can be developed for their possible application on the domestic and regional levels.

In order to build a regional cybersecurity complex following the path outlined by the USMCA, it is necessary to retake and complement the intentions that the said treaty proposes. Therefore, this section will take the following elements into consideration:
1) what is cited in the USMCA;
2) the efforts that the Member States are already making in this regard;
3) a complementary proposal on the possible application of a regional cybersecurity complex.

[59] "Chapter 19" in *Agreement Between the United States of America, the United Mexican States, and Canada*.

I shall begin with the first point indicated in the USMCA: developing the capacities of the respective national entities responsible for responding to cybersecurity incidents. In this regard, each member of the USMCA has spent over a decade working with its own CERT (Computer Emergency Response Team), from which they have strengthened their national capacities to respond to cyber-threats.

The United States has the CERT-US administered by the Cybersecurity and Infrastructure Security Agency (CISA), which is the body that leads the national effort to protect and improve the resilience of the physical and cyber-infrastructure of the country. It is the CERT that provides help to stakeholders to leverage the cybersecurity framework and enhance their risk management capabilities. It also offers the Cybersecurity Framework that helps organisations improve cyber-resilience through the identification, protection, detection, response to, and recovery of systems and infrastructure, with the support of a whole series of academic resources, research, databases, training, and technical networks.[60]

In the case of Mexico, the CERT-MX is responsible for preventing and mitigating security threats that jeopardise the technological infrastructure and operation of the country. It is responsible for monitoring the Internet permanently in order to identify conducts that might constitute a criminal offence, and carrying out tasks for the reduction and risk mitigation of threats and cyber-attacks. Likewise, it implements scientific-and-technological-development programmes in cybernetic matters as well as exchanges information with technology companies, financial associations, and public institutions dedicated to training and awareness-raising tasks in different productive sectors.[61]

The Canadian Centre for Cyber Security is responsible for responding to cyber-incidents in Canada. It is a sophisticated institution that provides technical support, generates alerts, and guides the different stakeholders to prevent and mitigate risks as well as respond to cyber-attacks through the generation of information, training, and continuous innovation.[62]

As can be seen, the CERTs of the three countries have similar objectives and functions. All three are intended not only to respond to cybernetic threats, but also to strengthen the national capacity in multi-stakeholder collaboration. Hence, the objective of the USMCA with regard to its first point could be considered fulfilled. However, individual efforts on the national level can be limited in the light of coordinated transnational threats.

In the national cybersecurity strategies of each country, the importance of international cooperation to strengthen capacities and have an accurate and coordinated

[60] *US-CERT*, CISA, accessed September 2, 2020, https://us-cert.cisa.gov/.

[61] Policía Federal, *Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal*, May 17, 2018, https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es.

[62] *Canadian Centre for Cyber Security,* Government of Canada, accessed September 2, 2020, https://cyber.gc.ca/en/.

response stands out. For the United States, it is of strategic interest to foster the creation and maintenance of strong international alliances and partnerships in order to deter shared threats and increase the international security and stability.[63] Canadians consider cyber-threats as increasingly sophisticated and mostly external to the transnational scope.[64] However, none of the three countries has taken the initiative to create a body that coordinates responses and capacity-building efforts towards cybersecurity at the regional level.

Therefore, the first proposal for the construction of a cybersecurity complex for the region is the creation of the North American Computer Emergency Response Team (CERT – NA): an international body that could organise and implement a coordinated response to cyber-attacks. This response team would not imply the suppression of the national CERTs of each member of the USMCA, but, rather, it would translate into a coordinating agency that facilitates the flow of information and response to coordinated threats that come from outside of the region, or even from within, posing a potential transnational damage that could affect the entire region. Likewise, it would promote the compilation of information, the generation of innovation, the strengthening of capacities, and the evaluation of best practices among the CERTs in each country.

The second point to consider when pondering the USMCA regarding cybersecurity refers to strengthening the existing mechanisms of cooperation among the three countries in order to identify and mitigate malicious intrusions and the spreading of malicious code that could affect electronic networks; it should be followed by using those mechanisms to quickly deal with cybersecurity incidents as well as exchanging information for common knowledge and implementation of better practices. In this sense, the three members of the USMCA already propose international collaboration in their national strategies. For the United States, an essential strategic component is the creation and maintenance of international alliances and partnerships to deter shared threats and increase international security and stability.[65] Likewise, in Mexico, international cooperation with public and private actors is considered the main axis.[66] For Canada, it is important to partner internationally in order to advocate for an open and secure Internet, enhancing capabilities to combat cybercrime.[67] However, so far there has been no trilateral mechanism, scheme, agency, or instance that allows for achieving these purposes at the regional level.

In order to address this challenge, the second proposal towards a cybersecurity complex in North America is the creation of the Regional Cybersecurity Agency that would coordinate the efforts of the three countries as well as develop and facilitate

[63] *The Department of Defense Cyber Strategy,* US Department of Defense, April 2015, 7, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2015_Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[64] *National Cyber Security Strategy*, 17.

[65] *The Department of Defense Cyber Strategy*, 8.

[66] Gobierno de México, *Estrategia Nacional de Ciberseguridad*, 20.

[67] *National Cyber Security Strategy*, 36.

the implementation of multi-stakeholder collaboration. This agency would be composed of a committee with state officers from the three countries, specialising in cybersecurity; they would establish protocols and manuals to share information, generate alerts, strengthen capacities, seek technological collaboration, and encourage innovation processes for cyber-resilience and a response to attacks. This Agency should be multidisciplinary and promote the implementation of policies as well as the evaluation of the current mechanisms regarding cybersecurity. Moreover, it would be in permanent interaction with the CERT-NA about technology-strengthening issues.

The main task of the Agency would be to coordinate the regional cybersecurity complex and be an asset that enhances all actions related to the mitigation of malicious intrusions, the immediate response to cyber-attacks, and the exchange of information and the best practices. This way, the collaboration strategies that each country already has would be complemented, the objectives set by the USMCA on collaboration mechanisms would be fulfilled, and regional cybersecurity cooperation would be taken to the next level. It would be a great step towards securitising cyberspace in North America.

With these two points in mind, a viable proposal can be made that allows for the construction of a regional cybersecurity complex in North America. However, due to the changing nature of threats to cybersecurity, the USMCA members recognise that risk-based approaches can be more effective than prescriptive regulation in addressing those threats. Therefore, another recommendation can be made.

As said before, the USMCA proposes to employ and encourage companies to use risk-based approaches that rely on agreed standards and best risk-management practices in order to identify and prevent cybersecurity risks as well as to detect, respond to, and recover from cybersecurity events. In this regard, there already are enforcement measures in national cybersecurity strategies. The United States' Department of Defence has among its strategic objectives the mitigation of risks in cyberspace, which includes collaboration with companies, especially those dealing with technology, infrastructure, and telecommunications operators. For the Mexican government, it is a matter of national security to monitor conflicts in cyberspace, for which it is necessary to prevent risks and control threats in all sectors involved in cybersecurity. In Canada, moreover, it is a priority to help the business sector at all levels in order to make cybersecurity's capacity-building tools more accessible.

Taking this into consideration – and in order to further complement the regional cybersecurity complex – I suggest the creation of the Permanent Program of Cybersecurity Capacity Strengthening for all productive sectors, governmental agencies, and service providers that supply or supervise digital services. The idea is that both public and private sectors which are not immersed in the issue of cybersecurity yet – or those which could be weak links to cyber-threats – should stop lingering and begin their integration into the securitisation dynamics of cyberspace.

This permanent programme would work as a public policy destined to generate cybersecurity standards so that all the actors involved can have the most homogeneous capacity level possible. This programme would be implemented by the Regional Cybersecurity Agency, which would be responsible for prioritising training, creating best-practice standards, providing tools, and assessing the participants through the issuance of certificates.

It should be noted that the proposals regarding the establishment and construction of a regional cybersecurity complex are based on the assumption of its viability for general application. It is vital to begin the discussion with the theoretical point of view of the Regional Security Complex Theory and generate an analysis which would have the securitisation of the cyberspace on the regional level in its core, which can be achieved through integration schemes for the three countries.

Cybersecurity in the USMCA and the foundations for building a regional cybersecurity complex in North America

In this last section, some perspectives and conclusions will be raised with regard to the possible application of the proposals for building a regional cybersecurity complex. The feasibility and some final considerations on cyberspace securitisation opportunities in North America will be reviewed.

The proposals outlined in the previous section are based on three major foundations that were revised throughout this article:

- the principles of analysis and construction of the Regional Security Complex Theory, which I consider as the central concept for the securitisation of cyberspace on the regional level in North America;
- the regional dynamics that culminated in an integration scheme such as the USMCA, and the approaches established in the said agreement to strengthen cybersecurity among its three member countries;
- the existence of similar measures amongst the three countries, as already raised and executed by their national cybersecurity strategies, which gives feasibility to the ideas expressed in this research to build a complex of regional cybersecurity.

These three points reveal the feasibility of applying the said proposals. The historical and political development of regional relations – in addition to a theoretical approach that puts the debate for regional securitisation in its centre, specifically tackling the subject of cybersecurity – makes it possible for the proposed ideas to mobilise a solid analytical support.

The revision of the intentions embodied in the USMCA for collaboration towards cybersecurity among its members – and the cybersecurity strategies that each country in the region is already applying – both provide a real empirical possibility for the complex. The fact that there already are similar measures among the three countries that are being carried out at the individual level as well as the possibility of resuming them in order to make new proposals at the regional level bestows viability and meaning on the ideas presented in this research.

On the one hand, the three countries consider international cooperation in cybersecurity as a fundamental axis for achieving their objectives. However, they do not propose a specific mechanism to fulfil their purposes at the regional level. There is no clear reflection on the creation or construction of mechanisms, agencies, programmes, or institutions that could integrate the transnational cybersecurity efforts of the three countries. This endows the proposals of this research with a certain empirical value.

On the other hand, it is a curious fact that each country has strategies where they recognise cybersecurity as an important and multidimensional problem, but at the USMCA level cybersecurity is considered only within the sphere of digital commerce. This is related to the essentially commercial nature of the said treaty, although the reference to cybersecurity within the most important agreement in the history of the region is brief. Despite proposing solid principles of action in cybersecurity, the Agreement does not explain or propose any scheme for improving conditions in this matter among the three countries. This reveals the importance of analytical exercises, such as this article, which generate innovative proposals based on already consolidated theoretical frameworks while at the same time adapting them to subjects that are only developing, such as cybersecurity.

However, the proposals would have their own structural and application problems, mainly due to the unequal conditions and unequal technical and institutional development that exists between the three countries. Especially in the case of Mexico, there are greater institutional, technological, and economic liabilities for the application and contribution of value to a regional cybersecurity mechanism or agency. Despite this, cooperation could be encouraged in order to generate more equality on the matter amongst the three countries.

Although the interest that has been given in the region to the issue of cybersecurity and its inclusion in the USMCA is worth mentioning, it must be recognised that it has not been a priority, even though possible risks to national, regional, and global security can be presented with regard to cyberspace. The efforts must not remain in the sphere of generating awareness, nor in the mere words of a treaty, but, rather, specific actions are necessary to create integral efforts to securitise cyberspace in the North American region.

A reflection on the future of the North American Cybersecurity Complex

The USMCA provides a legal framework for building a cybersecurity complex in North America, since it outlines the intentions of each country in the region to start working on it. Moreover, similar national attempts have been seen in Mexico, Canada, and the United States, which is why there is common ground to further cooperate in creating tri-national institutions, as proposed in this paper.

The Regional Security Complex Theory offers an integral approach to the securitisation of a non-physical space based on physical attempts towards the regional integration of a security regime (despite being originally focused on trade). Since it takes into consideration intentions, cooperation, and common problems from a multifocal perspective, it allows for the translation of security matters into cyberspace while at the same time recognising the pre-existing conditions and interactions. Hence, from instruments such as the USMCA, the RSCT identifies common ground to work for cybersecurity in the region.

It is possible to conclude that a North American regional security complex can be achieved; however, a lot of work is yet to be done. Commitment between the three partners is imperative and, in this regard, the next four years will be crucial. The agenda for the future must involve strong bonds amongst the neighbours.

Since most of the facts in this research are the product of the foreign policy of Presidents Donald Trump and Enrique Peña Nieto with Prime Minister Trudeau, changes on the agenda are possible with different governments. Since 2018, President Andrés Manuel López Obrador has walked a similar path on the matter as his predecessor in México had. However, in 2020, the US presidential elections will determine the possible re-election of Donald Trump, who has shown a fluctuating attitude towards the southern neighbour. Although the President might want to continue with the compromises set in the regional agreement, tensions with Mexico in other matters might not allow it.

To conclude, stressing the importance of advancing towards cybersecurity – both theoretically in the discipline of International Relations and in practice in the trinational agenda – is of primary concern. Several regions in the world are working towards exchanging experience and good practices for the regional securitisation of cyberspace, e.g. the European Union and the Association of Southeast Asian Nations. North America must also do this in order to address security in an integral manner. Moreover, doing so makes it possible for other regions to implement actions that one day might culminate in a secure global-scale cyberspace.