LATIN AMERICAN AND CARIBBEAN ECONOMIC SYSTEM

EIIS EUROPEAN INSTITUTE OF INTERNATIONAL STUDIES

Second Specialization Courses on Cyberdiplomacy and Techplomacy

Final Report

SOCIAL DEVELOPMENT

Second Specialization Courses on Cyberdiplomacy and Techplomacy
Caracas
21 to 24 March 2022
SP/2da. Edición CCT/ IF-22

C O N T E N T S

I. RAPPORTEUR'S REPORT

Within the framework of the construction of negotiating capacities in cyberspace governance for the public sector in Latin America and the Caribbean, the Latin American and Caribbean Economic System (SELA) and the European Institute for International Studies (IEEI), in collaboration with the Pontifical University of Salamanca, held from 21 to 24 March 2022 the Second Specialization Courses on Cyberdiplomacy and Techplomacy for the training of future negotiators in this area in the region

A total of 298 public officials from the region participated, mostly diplomatic representatives, officials from regional organisations such as the Andean Community (CAN) and CAF-development bank of Latin America, and university professors. Each specialisation module consisted of eight academic hours. The sessions on Cyberdiplomacy were held on 21 and 22 March, while the second workshop on Techplomacy took place on 23 and 24 March 2022. The facilitators were Professors Mario Torres Jarrin from the Pontifical University of Salamanca, and Shaun Riordan from the IEEI.

The virtual training activity was aimed at building negotiating capacities for a better understanding of the application of diplomacy in political and geopolitical problems arising in cyberspace, as well as of the technological development at the international level to promote the region's interests in the digital era. It also provided the necessary tools to develop skills of future negotiators in their relationship with technological actors with a view to building an agreement on norms of behaviour in cyberspace, both in terms of Internet governance and cybersecurity.

The activity was opened by Ambassador Clarems Endara, Permanent Secretary of SELA, and Ambassador Antonio Núñez García-Saúco, Director of the IEEI. During his speech, the former explained the importance of the digital strategy within the framework of international policy and the interaction of actors in a digital scenario, driven by the coronavirus pandemic. Ambassador Endara also stressed that cyberspace is an area of growing relevance on the international agenda due to its instantaneous nature, real-time interaction and transparency, where cyberdiplomacy is gaining weight in the foreign strategies of countries that apply this tool.

In this context, the Permanent Secretary of SELA stressed the importance of taking advantage of the digital world in diplomatic functions and structures. He also emphasized that the reconfiguration of the digital world demands the action of governments through diplomacy on issues such as security, Internet governance and regulation in the areas of data protection or consumer protection. Hence the importance of emphasising that the use of cyberdiplomacy goes beyond the expansion of diplomatic networks at the digital level and must be addressed as a state policy involving all actors that interact in international relations, in which the objectives and short and long-term actions are defined and the message boosters, the main stakeholders and the type of messages to be transmitted are identified, in order to project the country image that is desired.

For his part, Ambassador Núñez García y Saúco stressed the importance of this training in the current digital scenario, highlighting the challenges that Internet governance and cybersecurity pose to cyber diplomacy. Likewise, he highlighted the need to link these issues with techplomacy in the search for solutions to the problems generated in this virtual reality.

II. CONCLUSIONS

The following conclusions can be drawn from the speeches by Professors Shaun Riordan and Mario Torres:

- The need to conceptualize cyberdiplomacy and its application in geopolitics. Cyberspace has no geography. It is a virtual and borderless space, where governments are less and less relevant and citizens can communicate directly through virtual networks. However, governments have not disappeared and pursue their geopolitical rivalries over cyberspace.
- Both state and non-state actors launch cyber-attacks for political and criminal reasons. In this confrontation, cyberspace has become a collateral casualty on the battlefield of international conflicts.
- Cyberspace consists of four levels, namely: the physical, the logical, the data and the social levels. The physical level describes both the continental and oceanic cables through which data flows, data stores and switching stations. The logical level describes the rules and protocols that allow the Internet to function. The data level refers to the contents of the communications that pass over the networks, the data in our emails and the contents of our web pages. These three levels constitute the Internet. The fourth level, which is the social level, turns the Internet into cyberspace. It is the level at which we communicate with each other.
- Within the layered structure, there are two distinct aspects: i) cyberspace does not exist only in the clouds; ii) cyberspace is strongly embedded in the physical world. In addition, both political and geopolitical controversies take place at all four levels of cyberspace.
- It should be borne in mind that many conflicts nowadays take place in cyberspace (virtual world). To illustrate this, according to the data on "Cybersecurity in the European Union," the European Council indicates that, between 2019 and 2020, the Union faced 5 (five) major cyber-threats: i) malware: 71% of companies and organisations were victims; ii) web-based attacks; iii) phishing; iv) attacks on web applications: Introduction into vulnerable servers and mobile applications of malicious files to obtain sensitive information undetected; and v) spam.
- Diplomacy in cyberspace is important, aiming to: i) build an international community of "cyber-diplomats;" ii) rely on "multi-stakeholder" diplomacy (acting with non-state actors); iii) build diplomacy based on interests rather than values or ideologies; and, iv) negotiate norms from the bottom up, including the role of blockchain technology.
- Global governance is made up of various actors: Nation States; international, transnational and multinational companies (trade in goods, trade in services such as banking, insurance, energy, etc.); international organisations; regional integration bodies; non-governmental organisations (NGOs) and international foundations or think tanks; technology companies such as Big tech companies or Industry 4.0 (a concept outlined in developed countries as an industrial policy response to the revolution in information and communication technologies).
- There is no clear definition of who governs cyberspace. There is no conceptual, physical or spatial delimitation. Areas such as Internet governance, economic and trade regulation, cybercrime and cybersecurity suffer from a lack of international norms governing their behaviour.

- Artificial intelligence, machine learning, robotics, the Internet of Things, virtual reality, 3D printing and 5G technology are consolidating technology companies as new international players whose actions have geopolitical implications.
- The regulation of cyberspace in the hands of technology corporations such as ICANN and to some extent the military has not been successful. For this reason, facilitators Riordan and Torres argue that techplomacy reconfigures the conception of international relations, modifying the international system by representing a paradigm shift in global governance.
- So far, the digital era is led and governed by Industries 4.0, whose economic might and external action have geopolitical implications. Both factors (economic and geopolitical) make Big Tech Industries the new de facto global players.
- Industry 4.0 or Big Tech Industries such as Apple, Alphabet, Microsoft, Amazon, Facebook and PayPal are among the top ten companies in the world in terms of revenue. These companies have a large part of the control over the infrastructure of cyberspace and know how to make full use of the Internet's potential compared to governments.
- Denmark became the first country in the world to raise technology and digitalisation to a cross-cutting foreign and security policy priority and to develop the concepts of Techplomacy, Tech Ambassador and Techembassies. In this context, cyberdiplomacy is considered a tool to solve problems generated in cyberspace with the support of Techplomacy. Other countries such as France, Germany, Switzerland and Estonia have appointed Ambassadors for digital issues.
- Techplomacy aims to address three interrelated trends in foreign policy:

  i) Social changes driven by technological disruption: artificial intelligence, the automation of work, the protection of personal information related to big data, social media on democratic dialogue and electoral processes, cybersecurity on the Internet of Things, digital business models on tax systems; and cryptocurrencies in the global financial architecture.

  ii) The influence of multinational technology companies due to the political and economic power they possess, overtaking traditional partners, nation states.

  iii) The transformative nature of emerging technologies, combined with the emergence of powerful non-state actors (Industry 4.0 companies), which is generating new forms of foreign policy and geopolitics.
- The Tech Ambassador's mission is to: gather information on new technological developments in the Tech-Industry sector; gather information on the future plans of these companies in terms of operations and investments; meet and discuss with technology companies on issues such as data protection and privacy, the functioning of cyberspace and Internet governance, among others.
- The mission of a Tech Ambassador is towards the executive branch of a Nation State, regional integration body or international organisation. His/her global mandate and mission is towards the executive power of large companies in the Big Tech Industries sector. He/she should have a physical presence in the capitals of the tech-industry cities.
- Techembassies would be the “tech-industry cities” or technology centres. They are set to become the new political capitals of the world, as they are the decision-making centres for trade in goods and services in the new digital era. The external action of these Big Tech Industries has a geopolitical repercussion at the global level given their economic capacity.
- The first capital of these technology centres is Silicon Valley (America), but there are others such as Shenzhen (Chinese Silicon Valley), Skolkovo Technopark District (in Russia) or

Dubai Silicon Oasis (United Arab Emirates), and more are being created in other regions of the world.

- Participants concluded that in the governance of cyberspace, the main actor needs to be identified. In this scenario, States need to establish and develop relations and reach agreements with big tech companies by fostering debate among stakeholders (public, private, academic and civil society actors). It would be a great step forward if countries agreed to develop a common foreign policy for the digital era where Techplomacy could serve as an instrument in the relationship with technological actors. One framework for action could be the convening of a five-sided international conference: Big Tech Industry 4.0, governments, academia, civil society and citizens. There, the interests of all parties could be brought together, agreeing on clear rules that allow for peaceful coexistence in cyberspace
- In this regard, the need for an international regulator was outlined. Without international regulation, there is a risk of an unbalanced international system and a constantly endangered peace due to a lack of security. The lack of regulation, regulators and enforcement bodies means that cyberspace remains a no man's land, a space for hybrid warfare. Cyber-attacks target businesses as well as government institutions. It is therefore a reality that cannot be denied.

Finally, the participants made some remarks, establishing that the level of capacities in the countries of the region is still uncertain and that the possibilities of taking advantage of the development of giants in Silicon Valley, reproduced in China and Russia, are very limited. This situation should lead to reflection on the national strategies adopted in successful countries in building the information society, such as China and Singapore, which less than 30 years ago were countries with high levels of poverty and today are leaders in e-government and in offering virtual services to their citizens in all areas. Therefore, long-term state policies that include the aforementioned issues are needed so that Latin America and the Caribbean are in a position to make credible proposals and not just witness the great events of cybertechnology.

•