Blanquerna
RAMON LLULL UNIVERSITY

School of Communication and International Relations

Mainstreaming Disaster Risk Management into Cyber Risks:

Proposing a Policy Brief to the Barcelona City Council

Final Degree Project

May 2021

Author: Alicia Amorós Fuster-Fabra

NIU: 756555

Supervisor: Enrique Schonberg-Schwarz Letzen

Degree: International Relations

Specialization track: Foreign Policy & EU

Type of Project: Applied Research

Executive Summary

Cyber risks and incidents have augmented in the past decade with the increasing usage and development of internet services. Consequently, national and regional cybersecurity agencies have been set to protect us. But, let's take a step forward.

Cyber risks have been traditionally tackled by a security and law enforcement perspective. Thus, leaving aside meaningful tools that adopt a whole-of-society approach when tackling risks. This is the case of **disaster risk management**, that, for example makes sure that prevention is better than cure and looks after the interconnection of different stakeholders.

For that reason, this Final Degree Project provides an exercise to bridge together an efficient tool (disaster risk management) with an emerging risk (cyber risks).

Cities are having an impact internationally and are marking a new trajectory for a lively global future. Many global initiatives have provided cities with a voice and a space to network and collaborate for action; which in this case has been **working towards resilience**.

As many experts would agree, Barcelona has been recognized as an example of a resilient city. As a city committed to the promotion and implementation of the Agenda 2030 for Sustainable Development and the Sendai Framework of Disaster Risk Reduction, there would not be any more accurate place to exemplify the intention of this project.

Key Words: cyber risks; disaster risk management; disaster risk reduction; resilience; cyber resilience; Barcelona

Table of Contents

List of Figures and Tables

List of Abbreviations

DRM	Disaster risk management
DRR	Disaster risk reduction
FAO	Food and Agriculture Organization
FDP	Final Degree Project
GAR	Global Assessment Report
IMI	*Institut Municipal d'Informática* (Municipal Informatics Institute)
IT	Information Technologies
NUA	New Urban Agenda
PESTLE	Political, Economic, Social, Technological, Legal, Environmental
SDG	Sustainable Development Goals
SME	Small and Medium Enterprises
SWOT	Strengths, Weaknesses, Opportunities, Threats
UN	United Nations
UNDRR	United Nations Office for Disaster Risk Reduction

Acknowledgements

The completion of this FDP would not have been possible without the help of all the experts that collaborated with their knowledge and recommendations; as well as the support of my family and friends.

I am extremely grateful for the support of Mr. Luis Miguel Laguna for his valuable guidance and deep and long conversations. His altruistic contribution has been key to make up my mind in the midst of a quite complex topic. He has taught me about disaster risk management principles and encouraged me to continue developing the topic.

I would also like to express my gratitude to Mr. Costis Toregas, one of the only authors that have addressed this topic thoroughly. Being able to replicate his study in Barcelona and have his feedback is beyond appreciated. I am very lucky to have counted on experts with high motivation for my topic and with time to discuss it.

My special appreciation also goes to Enrique Schonberg-Schwarz, for his guidance, patience, and open mind for understanding and supervising this project.

Last but not least, I would also thank Ecuador's Ambassador to the UN, Emilio Izquierdo, and Mr. Ricardo Mena, for having me showed and taught about disaster risk management, its importance, and the relevance to have an international relations' perspective in order to tackle risks. I am very pleased to have finally developed what it was started to be discussed in a meeting.

1. Introduction

1.1. Motivation of the topic and relevance to the field of international relations

How many hours a day did we spend on our devices during lockdown? Who has access to our data? And, how reliable is the media we consume? These are some of the questions that came to me in March 2020 when the COVID-19 outbreak was declared a pandemic and thus Spain implemented a nationwide lockdown and social distancing norms. The fact that "internet services have seen rises in usage from 40 % to 100 %, compared to pre-lockdown levels" (Brascombe B. 2020) made me realize two general trends. On the one hand, the possibility to keep in touch with our relatives and loved ones, as well as continue with our academic and professional responsibilities. However, on the other hand, it also made me realize how this increasing usage could make us more vulnerable to a cyber threat or attack.

In the meantime, I had the opportunity to do an internship in Geneva, where I worked for the Permanent Mission of Ecuador to the UN. Ecuador is a country with a high risk of earthquakes, volcanic eruptions, and tsunamis due to its location in an area of high seismic activities (Instituto Geofísico). For these reasons, they work closely with the United Nations Office for Disaster Risk Reduction (UNDRR) and even hold the Presidency of the UNDRR Support Group. There is where I personally came across the Disaster Risk Reduction field. "UNDRR works at the intersection between understanding risk and risk impact: reducing disaster loss and preventing the emergence of new risk" (Mizutori, M. 2019). Nevertheless, currently, the risks assessed by the UNDRR do not tackle explicitly cyber risks, and this feature made me wonder about the following reflection. In a global and smart city like Barcelona, which is less likely to be affected neither by a natural hazard nor a man-made hazard (considered by UNDRR), what other type of risk could affect it? So there I remembered what I thought during lockdown: cyber risks. Why would an office of the United Nations dedicated specifically to risks not tackle cyber risks?

From those reflections, the experience acquired during the internship, and the additional personal interest for international and local politics, I thought that a future study with an applied outcome could be relevant to the field of international relations. Cyber risks, threats, or cybersecurity are commonly studied through Security Studies, a

subfield of International Relations. If we make a quick search about who has the competencies to approach cyber risks, it would show that security, or law enforcement authorities do so. And the same happens internationally (within the UN framework), the United Nations Office for Drugs and Crime or the International Telecommunications Union are the bodies that tackle cyber risks. And, consequently, natural hazards such as floods, earthquakes, or man-made hazards, such as transport accidents, are tackled through the UNDRR.

Since the purpose is to mainstream disaster risk management (DRM), which is the tool for disaster risk reduction (DRR), into cyber risks (an increasing global risk), an exercise of understanding international standards, legislation, even power has to be made. If this Project would work, in the long-term it could be a model for other cities and even countries to follow, as well as for the UNDRR to consider. It is also relevant to the international relations field because I will study both a tool and a threat that has a global effect and impact, but with a local approach. Moving from any International Relations theory that looks after a state-level behavior in the international arena and opting for a local lense, was thought to be an insightful exercise. The intention is to approach cyber risks with a more integrative tool, addressing resilience, and making sure that prevention is better than cure.

1.2. General and Specific Objectives

1.2.1. Can disaster risk management be used to study and address cyber risks?

It all started with that question. As a curiosity, and as mentioned above, I found myself wondering how DRM could benefit the study and assessment of cyber risks. However, even if the question will serve to give a storyline to the theoretical part, the nature of this Project is applied. This means the data collected will not be sufficient to provide a forceful answer. Yet, the development of the Project will be based on the accomplishment of the following objectives.

The general objective of the Project will be to learn how to provide the Barcelona City Council with recommendations for addressing cyber risks with DRM. In this sense, the aim is to move from the traditional perspective of mainly including natural and man-made hazards (excluding cyber risks) in the use of DRM. While, at the same time, shift from a security and law enforcement response to cyber risks. “Risk management is a

systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues" (Berg H.P. 2010) and the United Nations provides, through the Sustainable Development Goals and the Agenda 2030; the Sendai Framework for Disaster Risk Reduction 2015–2030 from UNDRR; and the United Nations Global Assessment Report on Disaster Risk Reduction (GAR) very accurate tools to achieve it at national and local levels.

In order to achieve the general objective, there have also been established some specific ones.

(1) Analyze the current situation of Barcelona in regards to cyber risks and DRM in order to study the accuracy of the Project.
(2) Adapt cyber risks into the DRM language. In order to do so, an analysis of the existing literature will be essential, as well as interviews with both experts of cyber and disaster risk management and reduction.

1.3. Methodology

The methodology will be based on a theoretical and applied research process. As a first step, the research will be structured through a literature review and data collection, which will support and provide a basis to the applied part. In this sense, the second part of the Project will be devoted to the "field study" and design of the policy recommendations for the Barcelona City Council through a proposed policy brief (found in Annex 6).

The theoretical block will include a more specialized contextualization of the key words of the Project, mainly: risks; cyber risks; disaster risk management; disaster risk reduction; resilience; cyber resilience; and Barcelona. In order to do so, scholarly sources will be used and some interviews will be conducted. As regarding the interviews, their transcription, as well as a brief biography of the interviewees will be found in Annex 5 Moreover, data collection will be a key feature for the accuracy of the project. A proper data collection, for example, of the possible relation that public sectors have with Information Technologies (IT), or the political will that the Barcelona City Council may have to consider cyber risks as a priority, could make the project more credible, and the further conclusions more solid.

For the applied part, the methodology will be more specific to the Barcelona case. With the help of analytical tools like PESTLE, SWOT, and Canvas I will study how the

strategy could be implemented in Barcelona through the City Council authorities. It will also serve as to demonstrate its possible feasibility and draw the conclusions of the project. In addition, it has to be noted that all the translations from either datasets, interviews, or literature have been self-made.

1.4. Literature Review

This Final Degree Project's work will be based on research of different scholarly sources, official data, and self-obtained data through quantitative and qualitative methods. As previously stated, a literature background that supports the final document is needed. So, in this sense, the research will be sustained by three main pillars, though a wide range of different sources will diverge from them. It should be noted that these pillars have been decided following the accuracy of the general topic and its relation to the international relations field. Having said that, the pillars are (1) the Sustainable Development Goals and the Agenda 2030 of the United Nations; (2) the Sendai Framework for Disaster Risk Reduction 2015–2030 from the United Nations Disaster Risk Reduction; and (3) the United Nations Global Assessment Report on Disaster Risk Reduction (GAR) as a link between the previous two.

Starting from the first pillar, the Sustainable Development Goals (SDGs) were adopted in 2015 as a continuation and expansion of the previous Millennium Goals (2000-2015). Though there are 17 different objectives, this FDP will sustain its theoretical framework on the SDG 11 - "Make cities and human settlements inclusive, safe, resilient and sustainable". Within this objective, and quoting the UN, "cities must plan their development in a sustainable and participatory way […]. In addition, they must […] prepare comprehensive, resilient solutions for the risks stemming from climate change and other possible disasters". Since cities are now taking part more actively in the international arena, it was found accurate that the applied part of the project would be a policy brief to the local authorities.

Furthermore, within SDG 11 (Target 11.b) the UN also established some indicators that should help countries, or in this case, local government and authorities, to share, implement recommendations, and achieve this goal. The Indicator that will be used in this Project will be Indicator 11.b.2: "Proportion of local governments that adopt and implement local disaster risk reduction strategies in line with national disaster risk reduction strategies" (UN 2015). This in part would seem to overlap with the literature

from the Sendai Framework Targets, but this should not be a problem because the Target we will specify on is already in line with the SDGs. So far, it could be perceived that the scope is still too broad, but this is only to set some frames for the further specification of the project. Then, the aim is to work on the interconnection of different definitions and aspects.

The second pillar is the Sendai Framework for Disaster Risk Reduction 2015–2030 from the United Nations Disaster Risk Reduction. It was adopted the same year as the SDGs and its "predecessor" was the Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters. Within the preamble, we see that states also reiterated their commitment to "address disaster risk reduction and the building of resilience to disasters with a renewed sense of urgency within the context of sustainable development" (UNDRR 2015). Additionally, it advocates for the integration of DRR and resilience in policies and programs at all levels, which goes in line with the purpose of this FDP. The concept of resilience will be essential when addressing the specific case of Barcelona.

As a first glimpse to the Sendai Framework, the two most relevant aspects to mention are its four priorities and its seven targets. On the one hand, the priorities are:

(i) Understanding disaster risk;

(ii) Strengthening disaster risk governance to manage disaster risk;

(iii) Investing in disaster reduction for resilience and;

(iv) Enhancing disaster preparedness for effective response, and to "Build Back Better" in recovery, rehabilitation and reconstruction.

The proposed policy brief which is going to be designed for the Barcelona City Council will include the four priorities adapted to the specific topic of cyber risks. On the other hand, a meaningful target of the Framework is Target e: "**substantially increase the number of countries with national and local disaster risk reduction strategies by 2020**" (UNDRR 2015, 9). However, as it can be noted, this target has a different "expiration date". It should have been achieved by 2020, so, in this sense, it will be an opportunity to study the performance, participation, and interaction of our local government with the Framework.

Finally, the last pillar is the Global Assessment Report (GAR) on Disaster Risk Reduction of 2019, also produced by the UNDRR. This report has been chosen as pillar because it provides a comprehensive approach combining both the Sendai Framework and the SDGs, and it gives updated data. This pillar is fundamental because it

acknowledges that "new risks and correlations are emerging in ways that had not been anticipated" (GAR 2019, 4). This assumption gives space for interpreting that new risks could be cyber risks and thus a new approach could be adapted to these new circumstances.

Additionally, it also states that a "fundamental re-examination and redesign of how to deal with risk is essential" and that "existing approaches to understanding risk are often based on the largest and most historically obvious and tractable risks for humans, rather than on the full topography of risks" (Idem). This would argue in favor of renovating the traditional definitions and conceptions of DRM mainly focused on natural and man-made hazards, usually excluding technological risks like cyber risks. This report also calls on the interaction of different disciplines, integrated, multisectoral research engaging non-traditional counterparts, risk assessment and decision-making connected through collective action and the representation of different sectors that will develop strategies and address the different risks. Finally, this report is essential because every new edition makes a call for case studies. This means that successful papers could be published in the next GAR and consequently become an object of study and replication.

Up until this part, the bibliography that has been introduced can be considered of an agreed language. Those are official documents, standards, frameworks, or guidelines that have been published by the UN, and from there, we can start to introduce more academic sources that either support or argue about them. Personally, I found that it would be more appropriate to start by a wide basis for the theoretical framework, and, from that standpoint, continue with more specific academic discussions and the research *per se*. This order would follow the Guidelines' criteria: going from general to specific; and in this case, having in every stage an international relations' reference.

To support the pillars, there are different initiatives coming from the UN, philanthropic organizations, or led by other private sectors. One of them is the New Urban Agenda, "a shared vision for a better and more sustainable future, where urbanization can be a powerful tool for sustainable development for both developing and developed countries" (NUA 2016). This was adopted in 2016 in Quito, Ecuador, and it has a strong approach to disaster risk reduction and resilience. For example, in its paragraph 78 its commitment towards a risk-based, all-hazards of all-of-society approaches is clear. In addition, it also calls for the building of resilience and the need to provide local responses to address the necessities of people affected by disasters. Finally, it promotes the awareness of news risks and the integration of resilience building in future

plannings (NUA 2016). This urban perspective is very insightful because cities are having an international impact and setting a new trajectory for a vibrant global future (DiMSUR 2020). This means that strong networks of cities can be determinant to our collective future.

In the case of Barcelona, as a preliminary overview, the urban resilience model rests on three pillars corresponding to the three stages that make up the continuous improvement cycle for building resilience, which are very similar to those presented in the Sendai Framework:

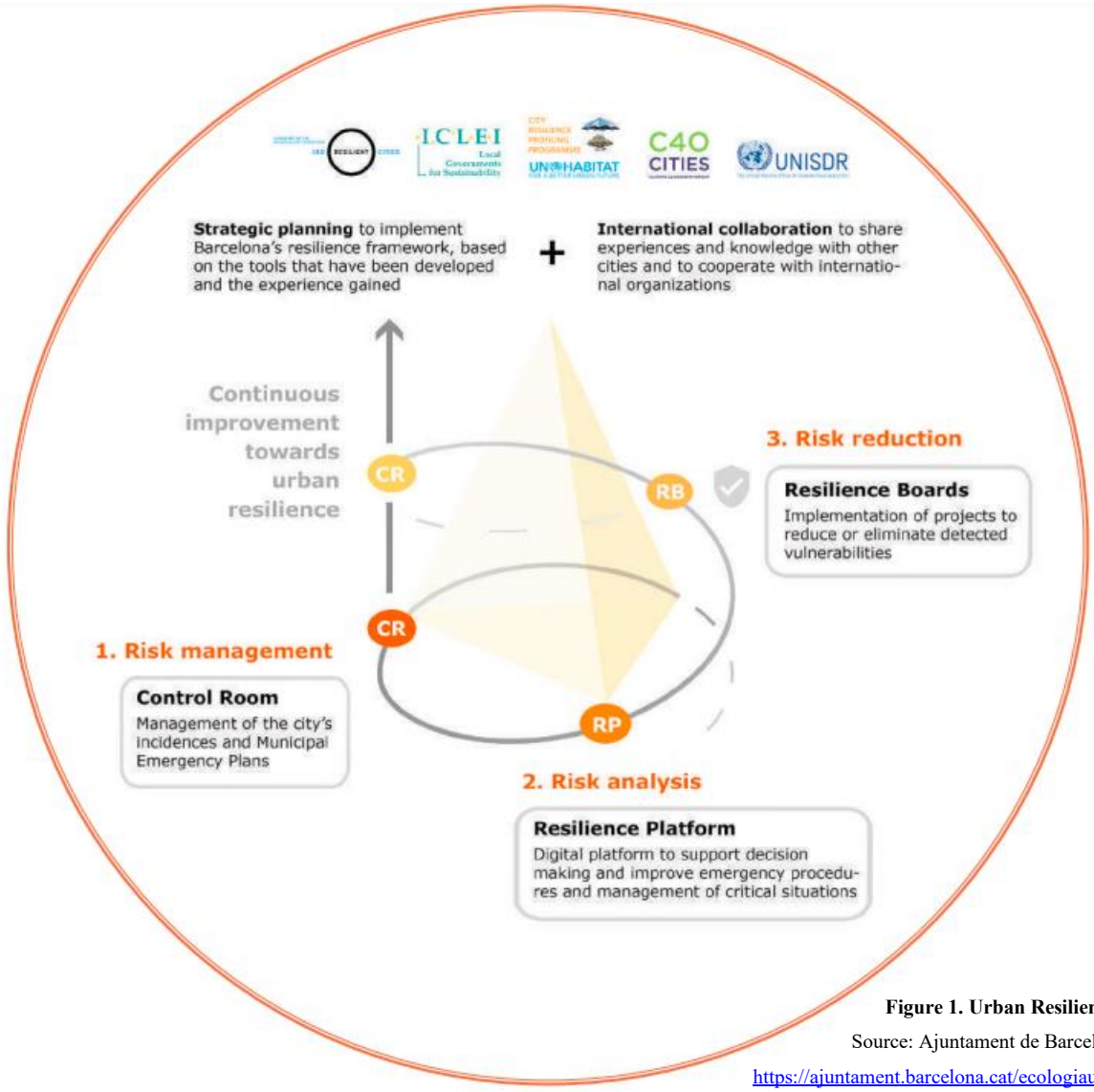


Figure 1. Urban Resilience Model

Source: Ajuntament de Barcelona. p 21. https://ajuntament.barcelona.cat/ecologiaurbana/sites/default/files/ModelResilienciaBarcelona.pdf

1) **Risk management, through the urban space operations centre and coordination with the other control centres in the city;**
2) **Risk analysis, using the information management and resilience analysis system; and;**
3) **Risk reduction, through the resilience boards.**

As Figure 1 shows, the process in the Urban Resilience Department begins by coordinating and managing incidents by the different municipal venues. Then, second stage is achieved through "information management and resilience analysis using the municipal platform". And, finally, the resilience boards, implement and improve the projects in order to reduce any vulnerabilities detected, "and improve the city's capacity to respond when faced with exceptional or emergency situations" (Ajuntament de Barcelona 2016). In addition, the process can be related to what is going to be tackled in the following Contextualization and Development chapters.

Moreover, and agreeing with climate expert from the Barcelona's Office of Sustainability, Irma Ventayol, about resilient planning in Barcelona "the city is and might be exposed to climate-related risks, other natural risks, technological and human-induced risks. Furthermore, there might be non-linear cascading effects triggered by some of them" (Ventayol, 2014). In addition, and this is what is going to be discussed throughout the coming research, technological and man-made hazards have been historically important in Barcelona. Yet, those hazards have affected infrastructure, services and building's safety (UNISDR, 2014). For example, in 2007, a series of critical events took place: "severe drought in the region threatened water supply in the city, problems with the high-speed rail line and, above all, a three-day electric blackout that directly affected 323,337 users" (Ajuntament de Barcelona, 2013a, p.7). However, now it is necessary to take a step forward and mainstream the approach in order to include cyber risks and its cascading effects, and to make disaster risk management even more inclusive and multisectoral.

2. Contextualization

2.1. How are risks studied?

Over the last century, the study of risk has grown into an increasingly important field of scientific research. In that sense, two academic disciplines have emerged to develop the concepts, theories, and methods to manage, assess, understand, and communicate risks: Security Studies, and Safety Science. On the one hand, scholars that study security aspects, do so through Security Studies, a sub-discipline of International Relations. It is important to note that a "condition" for an activity to be considered as a security threat, is that such activity is instigated intentionally. According to Wolfers (p. 451), security "measures the absence of threats to acquired values". That is to say, it prevents intentional threats that could damage not only human beings, but also their acquired values. This may imply that, if security aims to prevent threats, its emphasis would be on the cause of the threat, rather than on the "victim".

On the other hand, Safety Science studies risks with an opposite perspective. One of the aspects that makes this discipline different from Security Studies, is that safety, or the study of accidents, comes from non-intentional aspects, rather than intentional. Consequently, the effects of natural hazards such as earthquakes or floods, as well as the spread of a virus, or chemical and food safety, could be studied through Safety Science. The detailed description of both disciplines can be found in Annex 1.

The approach mostly used in this discipline is called "risk management". Even though this new concept will be broadly discussed in the coming paragraphs (as it is the tool that will be used for the project) it is important to mention that it "seeks to establish how dangerous or potentially harmful phenomena can be reduced to what has come to be termed as "acceptable risk levels"" (Aven, T. 2018; Giddens, A. 1999; Hollnagel, E. 2014). It aims to prevent and mitigate such risks in the future. Another aspect that contrasts the Security discipline is that Safety Science is more focused on protecting first, rather than taking away the cause. Thus, those "receiving end" of the dangers could be prevented from an unintentional harm (B. van den Berg & Prins, n.d.).

So far, the traditional approach that these two disciplines have, seems to be contradictory, in the way that one looks after the causes, while the other addresses the prevention, mitigation, likelihood and impact of a risk. Nevertheless, the reason why these two have been introduced is not due to a simply descriptive matter. In fact, what this PDF will try to achieve, is to interconnect them in order to address cyber risks through risk

management. And, more concretely, disaster risk management. Cyber risks are threats traditionally tackled through the security discipline. Yet, with the help of the three pillars mentioned in the introduction: the Sustainable Development Goals, the Sendai Framework, and the Global Assessment Report from the UNDRR, as well as with the support of some analytic models, I will study the integration of cyber risks into the disaster risk management approach.

2.2. Cyber Risks and Cyber Resilience

Cyber risks, according to NorthBridge Insurance, commonly refer to any "risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems" (Northbridge Insurance, 2016). Cyber risk could then materialize in a variety of ways, for example: deliberate and unauthorized breaches of security to gain access to information systems, unintentional or accidental breaches of security, and operational IT risks due to factors such as poor system integrity (Idem).

The way they are approached, internationally (in UN terms) speaking, is through the International Telecommunications Union, which in collaboration with the United Nations Office of Drugs and Crime, has developed, among others, the GCA framework, ITU–IMPACT alliance which provides an "open partnership platform for international cooperation between governments, industry leaders, academia and law enforcement agencies in order to facilitate the establishment of cybersecurity strategies and critical information infrastructure protection" (Ntoko, 2011). In Catalonia, for example, the principal tendencies in cybersecurity are: the evolution of ransomware, the organized cybercrime, attacks to the supply chain, internal threats, disinformation, geopolitics and the cybersecurity sector (Agència de Ciberseguretat de Catalunya).

Moreover, a very meaningful topic that will be also addressed once the Barcelona case is introduced is the concept of cyber resilience. According to the United Nations University, cyber resilience enhances the "ability of individuals, communities, cities, and countries to achieve the desired level of functioning in the face of adverse cyber incidents (United Nations University Institute in Macau, 2020). The reason why it is important is that it could be related to what is proposed for urban resilience, which, as stated in the first pillar, is a goal in SDG 11. And, in addition, it is also present in the New Urban Agenda, as well as in the Sendai Framework.

2.3. Risk Management, Disaster Risk Management (DRM), and Disaster Risk Reduction (DRR)

As previously introduced, risk management is the approach or tool mostly used by Safety Scientists in order to address risks. But what are risks? According to (H.-P. Berg, 2010), "risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives" (H.-P. Berg, 2010). Risks may vary and change over time thus its categorization should not be static, and its assessment either. Risk management therefore is an approach that sets the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues (H.-P. Berg, 2010). These words are essential: identify, assess, understand, act, and communicate. This integrative approach, as also shown in Figure 1, permits by its definition that emerging risks can be further included and studied.

Nevertheless, this project intends to take a step further and introduce a concept which is often interchangeable with risk management: risk reduction, and more specifically, Disaster Risk Reduction (DRR). First of all, in international relations, "disaster risk management is the application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk and manage residual risk, contributing to the strengthening of resilience and reduction of disaster losses" (UNDRR 2015). It can be taken from this quote that DRM and DRR fall into technical but also political dynamics that integrate the study of risks into policy outcomes.

Moreover, and to link it with the first and second pillar (SDGs and Sendai Framework), according to the UNDRR, "disaster risk is an indicator of poor development, so reducing disaster risk requires integrating DRR policy and DRM practice into sustainable development goals" (UNDRR, 2017). Historically, DRR focused on natural hazards' disaster, though it broadened its scope at the end of the 20th century and included disasters that were not only natural, and embraced that it is only by "reducing and managing conditions of hazard, exposure and vulnerability that we can prevent losses and alleviate the impacts of disasters. Since we cannot reduce the severity of natural hazards, the main opportunity for reducing risk lies in reducing vulnerability and exposure" (United Nations Office for Disaster Risk Reduction, 2015)

According to the United Nations, it is estimated that in 2050, more than two-thirds of the world's population will live in cities. This hugely rapid urbanization, as well as population growth, are drivers for the increase in disaster risks, namely in climate matters. (World Bank, 2020) In this sense, "governments need to invest in the collection, management and dissemination of risk information, including disaster loss and impact statistics, hazard models, exposure databases and vulnerability information". (UNDRR, 2017). Notwithstanding, the importance of the Sendai Framework, mentioned in the Literature Review, arises again. DRR and the Sendai Framework state that managing risks is everybody's business. Therefore, it must involve every part of our society, including governments, civil-society organizations, the private sector, and even academia. The current stage of DRM can be found in Annex 2.

2.4. The importance of mainstreaming DRM into Cyber Risks

At this point, by sticking to the traditional definitions and scope of the risk disciplines, it may be assumed that cyber risks are commonly tackled through a security approach, and risk management is used to address natural, and some man-made hazards. However, the approach that this Project aims to give, as stated above, is a more integrated one, where, in the case of cyber risks, there can be a wider view that includes the impact, the protection, and the solution to reduce the security threat; something that risk management does. A very insightful Working Paper published in 2020 by UNDRR, states that "the cascading impacts of a successful hybrid attack against national power grids during a period of national and / or global emergency, such as COVID-19, could be unimaginable in terms of their reach" (UNDRR, 2020). Following the COVID-19 crisis, in the health sector, for example, we saw patients being able to contact with their families, but also others fighting for their lives. Cyber events have increased since the outbreak last year, and, hackers, for example "disabled computer systems at the Düsseldorf University Hospital and a patient died while doctors attempted to transfer her to another hospital" (Tidy, 2020).

The increasing usage of digital tools, especially since the COVID-19 outbreak, has made us expose program information, as well as our personal data. Consequently, the lack of training and experience in cyber security has also made us, and every level of our society more likely to experience any kind cyber threat. For example, in Italy, "a cyberattack on [its] social security system (INPS) revealed Personally Identifiable

Information to applicants as they were attempting to claim benefits". Or, for example, hackers crushed into Skype and Zoom meetings, "disrupting conversations of government officials who conduct remote discussions" (Toregas, 2020). Some other threats identified have been: "phishing, using the subject of coronavirus as a lure; malware distribution, using COVID-19-themed lures; registration of new domain names containing wording related to coronavirus or COVID-19; and attacks against newly and often rapidly deployed remote access and teleworking infrastructure" (Wright & Goel, 2020). Seeing how this increase in attacks is affecting not only our personal data, but is disrupting the course of work of many sectors, some solutions have been brought up. One of those being cyber resilience. A "whole-of-society agenda that goes beyond just protecting critical information infrastructure" (Mamello & Debora, 2020). A good link that will be introduced after, is that cyber resilience, or any aspect of resilience involves the participation of different stakeholders, as well of resources. In that sense, cyber resilience could bridge the gaps between cyber risks and disaster risk management and make an all integrated approach possible.

However, cyber risks have not been approached in a fully integrated manner especially in terms of "reducing potential disaster risk through comprehensive, joined up approaches" (UNDRR, 2020). This could be attributed to the variance of views, including among States, as to "whether cyber risk should be approached – in conceptual, institutional, policy and operational terms – as not only a security issue, but also as one of DRR, thereby forming an integral part of the Sendai Framework" (UNDRR, 2020). This is consequently due to some reasons, for example, when cyber risks are not appropriately considered at the national resilience priorities and capabilities. And, the "traditional practices of approaching cyber risk from a largely security/law enforcement rather than risk mitigation perspective; to a sometimes imbalanced focus on the DRR benefits rather than the accompanying potential risks of technological innovation" (UNDRR, 2020).

That is to say that such divergences among countries in practice are not attributable to the allowance of the Sendai Framework which "makes adequate provision for DRR within the context of man-made and technological risk which extends to cyber risk, including hybrid scenarios" (UNDRR, 2020). This opens the door for rethinking the existing approaches and adapt the language for States and their national infrastructures to achieve the maximum resilience. "In addressing such risks, whether natural or man-made, most Governments, together with the multi-national institutions within and alongside

which they operate" (Idem), need to provide major policy emphasis and weight to prevent the risk and the possible cascading effects.

According to the UN Secretary General in the political declaration of the 2019 SDGs Summit, he stated that "DRR is included as one of the 10 priorities of the decade of action for the Sustainable Development Goals. Over the next decade and beyond, all development policies and investments should be risk-informed and based on an inclusive, multi-hazard risk assessment" (United Nations Secretary General, 2020). This is the best occasion and opportunity to mainstream DRR into new risks, as the GAR 2019 also mentions. We are currently, as some authors say, in the Fourth Industrial Revolution, where, "society's dependency on the resilience of information and communications technologies (IT), cannot be understated" (Idem). It is said that reaching consensus may be easier at certain moments, for example "after a disastrous event when there is a general perception of the need to do something" (UNDRR, 2019b). COVID-19 is currently a disastrous event as it has shown, besides the sanitary consequences, other cyber vulnerabilities. So, it is an excellent opportunity for a smart and global city like Barcelona, to take the opportunity to lead, as a pioneer city, an innovative approach as proposed in this FDP.

2.5. Barcelona as a Case Study

"From earthquakes to flooding, rapid immigration to cyber-attacks, all cities face a range of shocks and stresses, natural and human-made. Today, cities and city inhabitants are facing additional and amplified challenges as a result of rapid urbanization, a changing climate and political instability, among other" (Chelleri & Baravikova, 2021). Barcelona is one case. It adopted a growth model due to its physical limits and the need of expansion due to different pressures (demographic, social, economic). The high rates of tourism, as well as the mobility of people that come from the outskirts to work, has made it an economic driver for the Southern part of Europe (Ajuntament de Barcelona, 2017). However, as it happened in many other places, during the 2020 national lockdown and even some time before, Barcelona and Catalonia experienced cyber-attacks in different sectors. According to La Vanguardia (Muñoz & Sans Tarragona, 2021), in the middle of the pandemic, for example, the servers of the Moisès Broggi hospital in Sant Joan Despí and other smaller health care facilities in the Regió Sanitària Metropolitana Sud were attacked. In 2019 it was the Hospital del Mar, causing serious problems when managing

the records of all its patients. The University of Girona (UdG), for instance, also suffered the ravages of a computer attack.

Nevertheless, in technological terms, according to The Financial Times (Financial Times, 2020) in its report Tech Cities of The Future for 2020/21, Catalonia has the second-best strategy in Europe for attracting investment in technology. Barcelona ranks eighth in Europe and first in Southern Europe as a technology city of the future. However, investment in IT in Europe dropped from 2019 to 2020: from 1.2 to 1.1 billion among small and medium enterprises (SME), and from 74.1 to 54.3 billion among large companies. Yet, investment in cybersecurity in the overall IT budget has gone from 23% to 26% among SMEs, and from 26% to 29% among large companies, according to Kaspersky.

In risk terms, the UN Resilience Hub states that the main issues regarding natural hazards in Barcelona are: flooding, heat island, heat wave, drought, and forest fire. For other types of risks, they also mention terrorism (Urban Resilience Hub, 2019). As it can be noted, cyber risks or any technological aspect are not considered. Moreover, and as an achievement of the city, Barcelona has a strong collaboration with UN-Habitat, with whom works to deliver the United Nations operational urban resilience projects, "contributing to the achievement of global agendas (Agenda 2030 and Sustainable Development Goals, New Urban Agenda, Paris Agreement on Climate Change and Sendai Framework for Disaster Risk Reduction), sharing innovative practices from Barcelona globally and linking Barcelona with global initiatives such as the Making Cities Resilient 2030 and the World Urban Forum" (Urban Resilience Hub, 2019) In this sense, Barcelona is a city that is strongly committed to the Agenda 2030, as well as with the implementation of the Sendai Framework, meaning, two pillars of the Project are being worked in.

The resilience model that Barcelona is implementing is being discussed in different international forums such as 100 Resilient Cities, recently turned on Resilient Cities Network. This implies that globally, Barcelona has a say and a commitment towards the implementation of the different international standards mentioned before. Why wouldn't then try to implement cyber risks on its resilience strategy? In this matter, the UN University Institute in Macau offers a very accurate insight: cyber resilience in smart cities. Cyber resilience, here, implies the ability of "individuals, communities, cities, and countries to achieve the desired level of functioning in the face of adverse cyber incidents – which can emanate from technical or socio-technical, as well as natural

or man-made sources. Resilience as a goal is articulated in Sustainable Development Goal 11 "Sustainable cities and communities", the New Urban Agenda, as well as in the Sendai Framework" (United Nations University Institute in Macau, 2020). This insight could offer a link to implement cyber threats in the urban resilience strategy of Barcelona, which, at the same time, would infer that DRM also take this risk into consideration. In order to assess and address cyber resilience, the steps recommended to create an effective are: understand the threat, protect, and respond (PA Consulting, 2018). These steps are very similar to those of risk management. In that sense, moving from the technical part where cyber security strategies are developed by engineers, computer scientists, or Safety Scientists, with cyber resilience, other actors could take part. And additionally, adopt a whole-in-society approach to address multi-dimensional risks such as cyber risks through DRM.

> "*Resilience is further enhanced through redundancy, which is achieved when more stakeholders are involved in multi-level governance – for example, when local governments are able to allocate more resources and implement more stringent measures in response to the lack of resources or lack of leadership from national governments to coordinate actions*." (Mamello, 2020).

3. Development

For the development of the Applied Project, some analysis tools have been used in order to frame the study by considering many aspects of our society, the stakeholders, the value proposition, its impact, and even how is it going to be structured. The tools used have been: PESTL, SWOT, and Canvas, which are going to be tackled in that order with the aim to introduce the final outcome of the project which is a policy brief (found in Annex 6). It is important to highlight that the data for these sections has been literature, but also valuable qualitative and quantitative information from interviews (see Annex 5) conducted to different experts on the DRR or cyber fields.

3.1. PESTL[1]

Having introduced the general situation or the current state of the study in the previous chapters, this analysis tool has contributed to its specification. PESTLE is a tool which stands for: P-Political, E-Economic, S-Social, T-Technological, L-Legal, and E-Environmental. It is widely used by companies in order to track the environment in which they operate or when they intend to launch a new product, service, or project. In this case, it has been used in order to concentrate in the Barcelona study while addressing the cyber risk issue. It is important to highlight that for this part, DRM will not be directly addressed because at the author's discretion, it would be more relevant to start the study by drawing some lines that define Barcelona's "cyber" situation to later be able to discuss the accuracy of working it with DRM.

The **Political** sphere has a very strong or significant impact on this subject of study because as it will be referred to in the SWOT analysis, political will determine the materialization of this project. Although the detailed description of the political factors is found in Annex 3, it can be concluded that on cybersecurity specifically, the Plenary of the Parliament of Catalonia approved, in 2017, a law creating the Catalan Cybersecurity Agency (G. Juanes, 2017). This is body in charge of "preventing, detecting, responding to and investigating incidents or threats […] and collaborate with police forces and judicial authorities" (Idem). As it can initially be perceived, when addressing cybersecurity only security and law enforcement bodies are cited as external ones to collaborate or coordinate with.

In regards to the Barcelona City Council, and according to the interview with the Head of the Urban Resilience Department, Ares Gabás, the Urban Resilience Office was created in 2014, becoming one of the first cities in the world to create a resilience office. In Barcelona, work on resilience (although this is not a new concept) began specifically in the first decade of the 2000s, motivated by various infrastructures and services crises. From that experience and in order to reduce the current vulnerabilities of the city, the resilience boards were created (see Figure 1). Their objective has been to reduce vulnerability to risks related to infrastructures and services, as well as natural and man-made risks that can alter the functional continuity of city services. The current priorities of the boards are under the Climate and Social resilience agenda. And, as it can be noted,

[1] This PESTEL analysis does not include the environmental (E) factor since, in this case, it is not seen relevant enough for the project.

cyber risks are not in the agenda of resilience. But this is interesting because of the transversal nature of those boards, and who participates there. The boards are made up of multidisciplinary teams in which technical staff from the City Council work with non-municipal entities, both public and private. In this sense, the communication and work are transversal and integral. On the other hand, the cybersecurity competences, as stated previously, are given to the Cybersecurity Agency or the Municipal Institute of Informatics (IMI).

On the **Economic** sector, different aspects need to be considered. Mainly, the expenditure that either the Barcelona City Council or the Generalitat of Catalonia have for cyber security, or the money that would be needed in order to implement this project. Yet, before analyzing those data, a very interesting study made by Dr. Costis Toregas and his colleague Joost Santos, suggests with an econometric analysis the way that the "IT sector (taken as surrogate for cyber connectivity and impact among sectors) interrelates to other economic sectors" (Toregas et al., n.d.) In this sense, the scarcity of historical data (which will be addressed in the SWOT) can be compensated with this way of rate setting for cyber risks. This study proves that in the case of a cyber-attack or related threat, which would cause the inoperability of the IT sector, would also cause inoperability in other economic sectors in a cascading way due to their dependency on the IT sector. Although this model will not be fully replicated in this Project due to its limited nature and for external features such as outdated data from the Generalitat of Catalonia's datasets, it has been very helpful in order to determine which sectors are dependent on the IT sector. And also, what could be the impact of a cyber risk in terms of cascading effects towards them. The detailed description and calculations of the study can be found in Annex 4.

Consequently, from the analysis, it could be emphasized that sector interdependence is very important when addressing cyber-risks because it takes the contribution of different stakeholders, mainly public and private in order to mitigate the possible threats. For example, a cyber-attack could disrupt the normal functioning of the electricity, gas, steam and air conditioning sector that could consequently provoke a big blackout as commented in chapters before, or scarcity of gas or steam. If traditional cyber risk management has been done through private consultancy, then this study suggests that a shared strategy between cyber security sector, insurance industry, and government

could be made (Toregas et al., n.d.). This also stresses the idea that DRM could focus on the more dependent sectors and the need for data in cyber-security operations.

In addition, there are other economic factors that could be considered when studying cyber risks. The annual budget of the Generalitat of Catalonia was also analyzed in order to check the investment in cyber-security. Nevertheless, the budget used was the 2020 budget, since the Decree 146/2020 of 15 December, established the criteria for the application of the extension of the budgets of the Generalitat for 2020, until those of 2021 enter into force (Generalitat de Catalunya, 2021). The first thing to highlight is that in the area of knowledge, innovation, and economic dynamism, it is stated as a priority to: Launch the Cybersecurity Agency of Catalonia. This lunch is accompanied with an increase of 14.3 million euros to their budget (Generalitat de Catalunya, 2020).

In the case of the Barcelona City Council, the initial budget of 2021 was 2,437.7 million euros. (Ajuntament de Barcelona, 2021). Moreover, an interesting feature is that one of the priorities for investing was in Information systems with a 26.7%. However, disaggregated data was not found, thus it is not specified what this investment includes. In the area of Security and citizen security, from the 339.7 million euros' budget, 203.1 million goes to citizen security, and 9.54 million euros to General administration of prevention and safety. This data has been brought in order to compare the general investment that is made to security and citizen security from the city of Barcelona, mainly excluding cyber-security, with the budget that the Cibersecurity Agency of Catalonia has for the whole autonomous community. Finally, it should be also highlighted that due to the COVID-19 crisis, it is expected a 11.2% decrease in the Catalan GDP, meaning that next year's budget can show different results (Ajuntament de Barcelona, 2021).

According to the World Economic Forum's Global Risk Report 2021, the "rapid digitalization of human interactions and the workplace has also expanded the suite of essential digital skills—including communication, cyber safety and information processing" (Mclennan, 2021). And, additionally, "cybersecurity failure" was rated as the 4th of its list of clear and present dangers, according to the respondents' forecast (Idem). This perception mainly increased due to the confinement measures and remote working experience during the COVID-19 pandemic. So here, in the **Social** sphere, cyber risks are also present. Cyber risks in Barcelona have been present on an individual basis, as users suffering cyber-attacks, but also institutions such as hospitals or city councils (Muñoz & Sans Tarragona, 2021). Our society is exposed and therefore it should also participate and

take action in this topic. On the one hand, society needs to be informed and trained in digital skills and therefore become less vulnerable to cyber threats. But, on the other hand, they should also know the benefits of addressing cyber risks through DRM.

The **Technological** impact on cyber risks is quite intuitive. From what has been previously stated, technology usage has increased exponentially since last year. This in turn, has led to more cyber threats. According to Genís Margarit, a cybersecurity expert and consultant who was interviewed, with COVID-19, there was an increase in users of information systems; from 15% of remote working to a vast majority. And what it needs to be highlighted is that many people started using platforms of that type for the first time. From here, it can be deducted that more people working remotely implies an increase in cases of cyber threats, but the significant increase in users has to be related to users who were less digitized. In that sense, training is needed. Margarit also commented that each of the large cities worldwide is equipped with its own security, and with its own security forces, which has been an advantage. However, in the case of Barcelona, it has to be noted that there is no cybercrime coming from Barcelona itself. Barcelona is not a nest for cybercriminals, according to the interviewee. Cyberattacks do not come out of Barcelona, they come from China, Russia, India, or the US. So Barcelona, although it receives cyber threats, all these threats are not originated from within.

Finally, in the **Legal** factors, the cybersecurity sector is bounded by the *Estrategia Nacional de Ciberseguridad* made by the central government (Gobierno de España, 2013). Nevertheless, the European Union has been promoting through the EU Agency for Cybersecurity (ENISA) the creation of national cybersecurity agencies, which aim to protect the digital life of companies, institutions and people (ENISA, n.d.). In Spain, it is in INCIBE which has a long history of more than a decade, as it was created in the second term of Zapatero. In Catalonia, the cybersecurity agency was launched this last legislature with Puigdemont. At the same time, it should also be highlighted that Spain is a NATO member, thus it is bounded by the internal legislation on cybersecurity.

This analysis tool has shown that even if all factors are important for the cyber risk situation in Barcelona, some of them add up more than others. This is the case of the political, economic, and technological factors. Even if the technological seems to be quite

an intuitive guess, it is necessary to be redundant and realize the following. For a smart city like Barcelona, the increase of technology and its usage (brought in part by the Fourth Industrial Revolution and exacerbated during the COVID-19 confinement) has been quite noted. Thus, as a direct effect, cyber threats have increased as well. In the case of the economic factor, it is important not only because more investment in cybersecurity is needed, but an economic analysis of the perturbation that a cyber threat could provoke in the economic sectors could bring a realistic perspective into the further study. Also, the outcomes from the political factor offer a path for remarkable improvements. For instance, breaking someway silos' work-style, incorporate other stakeholders, multidisciplinary teams and a holistic approach, and considering cascading effects clearer and more specifically. If considered together with the economic factor, they would probably offer higher possibilities to contribute to improve cyber resilience. The next chapter will offer reinforcing arguments for this outcome.

3.2. SWOT

The SWOT analysis is used in order to identify the internal and external environment of the business, or in this case, the project. For the first, Strengths and Weaknesses are assessed; and, consequently, Opportunities and Threats determine the external environment. This analysis tool has been found very appropriate because it shed a light on the current DRM circumstance, viability, and possible threats to the project. In the case of the threats, the political will, data availability, and readiness of the different stakeholders to engage in a common objective have been, in my opinion, determinant for the success of the project. For this reason, the interview with Mr. Sanjaya Bhatia focused on these main challenges. Bhatia works on the mainstreaming of DRR in different countries as well as promoting resilient cities. He strongly agreed that convincing policy makers is a very big challenge, and the best way to overcome it is by trying to explain to them how disasters push back development and make societies waste a lot of resources. Consequently, investing in DRM and resilience should not be seen as a cost but a long-term investment (strength N.4).

Lack of data, as also discussed, tends to be another challenge. The reason is that it normally comes from different sources: public institutions, private companies, or other businesses where the public sphere does not have the authority to claim it. To overcome this, there are a number of initiatives that are trying to raise awareness of the importance

of data, for example the World Council for City Data. However, this project has an additional difficulty which is that cyber risks are not usually studied through these platforms, therefore, the lack of data is even higher (weakness N.1,2,3; and threat N. 2). Finally, putting different stakeholders together is another challenge, and a clear example has been with the COVID-19 crisis. However, it is needed as well as advocacy, because it creates conversation and engagement. And once this is created, with the help of policy tools such as the policy brief (or a simple toolkit which integrates cyber risks into the different strategies), policy-makers can be better persuaded.

This analysis made clear that the external environment, even if Barcelona seemed a suitable place to apply it, poses many challenges in terms of will, priorities, and lack of data. Nevertheless, that does not mean that in a future the same challenges will remain; there is a door open for its mainstreaming.

Strengths	Weaknesses
1. Policy brief can be easily distributed to policy makers. 2. The Project provides an original and new approach which aims to enable a single framework (Sendai) address and tackle an additional risk (cyber risks). 3. Stimulates stakeholder interaction. 4. The investment would not be significant, as in low- and middle-income countries, investing in more resilient infrastructure yields $4 in benefit for each $1 invested. (World Bank, 2020) 5. Cyber risk as an inherent element of DRM and resilience.	1. Finding historical data on cyber risks (in comparison to other risks contained in the Sendai Framework) is difficult, especially because it is owned by private companies. 2. Finding updated data on cyber risks in Catalonia is a challenge due to its scarcity. 3. There is limited documentation in regards to the integration of cyber risks into DRM. 4. The lack of experience and previous case studies that integrate cyber risks with DRM could make this Project lose sight of some factors.
Opportunities	**Threats**
1. DRM strategies not only provide resilience, but they also yield positive economic, social and environmental side-effects (co-benefits) (World Bank, 2020). 2. The growth of digitalization exponentially increases the risk from this exposure factor, and cascading effects and the concept of systemic risk are key issues to focus on and try to address them in the most integrative way. 3. It can be done through public policy. And the public policy guidelines for DRR and resilience emanate from what UNDRR recommends, what is established in the Sendai framework and what is being evaluated in the Global Platforms for DRR, like the GAR. 4. Barcelona is a Smart City compromised with both the implementation and fulfillment of the SDGs as well as with the New Urban Agenda, so in this sense the mainstreaming of DRM could be done.	1. Lack of other case studies aiming to mainstream DRM into cyber risks. 2. Reluctance either from the Security sector to work together with DRM, or from the DRM's scope to adhere a new risk on their working program. 3. Uncertainty and lack of data. 4. If this approach is found accurate, it would take time for the national and international authorities to implement and adapt it to their language. 5. There is inconsistent practice among States regarding the extent to which cyber risk is reflected within their national DRR strategies. (UNDRR, 2020) 6. Lack of unanimity regarding the types of activities that actually contribute to DRR.

Table 1. SWOT
Source: self-made

3.3. CANVAS

Between all the different Canvas models, the most suitable for this project, due to the need of different stakeholders to work together and collaborate, was the collaborative model. In this model, the value proposition has been drafted in order to be in line with the objectives of the project, and, the mission and vision have been stated emphasizing cyber risks as an increasing threat that should be tackled additionally through DRM. Moreover, in the collaboration goals' section, it can be seen that currently, the capacity of this collaboration has been rated as low since there is no communication between the actors that work on DRR or resilience with those that work on cyber risks or cybersecurity. Moreover, I found that this collaboration would not need to build a whole new infrastructure in order to implement this project, thus it has been rated as efficient. And, as stated in the resources' section, perhaps a tool that could enhance both the capacity and efficiency of the collaboration is an internet platform for them to communicate and work closer.

The stakeholders added to that list have been those that have been referred to throughout the paper, but those who already work in Barcelona have been differentiated from those who are in institutions, companies, or organizations abroad. The risks also reflect the threats and weaknesses named in the SWOT analysis, and the impact aims to cause a change in the way cyber risks are tackled. Finally, the structure of the project, as commented in the methodology, will be a proposed example of policy brief which aims to be distributed to the Barcelona City Council for its further consideration and implementation. The following section will go over the structure and content of the policy brief, as well as it will provide a better understanding of its use.

<table>
<tr><th>Mission + Vision</th><th>Collaboration Goals</th><th>Stakeholders</th><th>Value Proposition</th><th>Structure</th></tr>
<tr><td>The mission is to include cyber risks into the DRM's scope of Barcelona so when authorities need to deal with different risks, they can do so by an all integrated approach.

The vision is to provide the bridge between the traditional approach towards risks and the emerging cyber threats.</td><td>Capacity: weak or lose communication between agencies that work towards Urban Resilience/SDGs achievement with those that work on cyber issues.

Efficiency: it is more efficient to work with what already exists rather than building up something from scratch and overlapping with the already-existing institutions.</td><td>Internal stakeholders: Barcelona City Council with the departments of urban resilience, as well as those that deal with Agenda 2030, the Institut Municipal d'Informàtica, and the Agència de Ciberseguretat de Catalunya.

UN Habitat's office of Barcelona.

Experts and academia.

External stakeholders: UNDRR, Resilient Cities Network, private consultancy, academia, experts.</td><td>I intend to offer a new approach to cyber risks, where they are additionally tackled through DRM; to local and national governments, as well as international and regional organizations so that they will be able to study, address, assess and mitigate within one framework, an emerging issue which is cyber risks.</td><td>Policy brief-based outcome

Draft of policy brief that would be presented to the Barcelona City Council and that would include the scope of the study and some policy recommendations.</td></tr>
<tr><th colspan="2">Risks</th><th colspan="2">Resources</th><th>Impact</th></tr>
<tr><td colspan="2">Lack of stakeholders' engagement.

Lack of political will in order to adapt the already existing material.

Difficulty to adapt in other contexts (other cities, higher level scales).</td><td colspan="2">Academia and expert support.

An internet platform for stakeholders to interact and to develop the different webinars.</td><td>A better, more inclusive and integrated approach towards risks, where new emerging tendencies are also taken into account.

Diversity of stakeholders working together towards resilience.</td></tr>
</table>

Table 2. Canvas
Source: self-made

3.4. Development of the policy brief

The structure for the policy brief that has been chosen is from the Food and Agriculture Organization (FAO, n.d.), which has a specific "lesson" on how to draft policy briefs. It has been selected because UN staff members tend to draft policy briefs on a regular basis, thus the source is reliable, and the format is simple.

Nonetheless, before jumping into the structure and its content, it is important to define what a policy brief is, and its different types. First of all, a policy brief is a "concise summary of a particular issue, the policy options to deal with it, and some recommendations on the best option. It is aimed at government policymakers and others who are interested in formulating or influencing policy" (FAO, n.d.). So far, there are two types of policy brief: advocacy brief, and objective brief. The former "argues in favor of a particular course of action", whereas the latter, "gives balanced information for policy makers to make up their mind" (Idem). Since the purpose of this study has been to actually mainstream DRM into cyber risks, the type that will be used will be the advocacy brief.

Normally, the length of a policy brief would range between 1 and 4 pages long. In addition, there must be a thorough work of summarizing and selecting the most relevant and appropriate information. The use of these policy briefs can vary in many ways. For example, it can be used as printed hardcopies and handed in to policymakers. The way could be either in person or via email, or also distribute it to other stakeholders either at workshops or conferences. Moreover, they can also be used as softcopies that can be emailed or uploaded in websites. This is also a good strategy for distributing through social media or networking sites. Yet, FAO advises not to spam and distribute them consciously (FAO, n.d.).

3.4.1. Parts of the policy brief

Policy briefs are composed by several parts, and the FAO document will be again used as a reference (FAO, n.d.). The aim of this section is to develop or briefly introduce the content of the policy brief that could be presented to the Barcelona City Council authorities.

- ***Title*** – the title would be the same as this FDP: Mainstreaming Disaster Risk Management into cyber risks: policy brief proposal to Barcelona.
- ***Summary*** – the summary would introduce the main points for the policymakers to get and would be brief and short.

- ***Recommendations*** – the recommendations will be stated in bullet points in a side bar at the beginning of the page, so they can be more visible for the reader. Although the final version of the policy brief will be found in the Annex 6, the recommendations that will be stated and have been decided after all the process of research and data collection are:
    - Develop platforms where dialogue can occur consistently and periodically with stakeholders from the DRM and cybersecurity sectors. In addition, let civil society participate in those discussions so advocacy can take place.
    - Develop a communication strategy for decision makers that convinces them that hazard is not unavoidable but disasters can be significantly reduced by having a DRM strategy, as cyber threats are increasingly affecting and exposing compromised and personal data.
    - Promote through universities learning sessions or webinars where both sides (or different stakeholders) can sit down to hear each side's scientific foundation.
    - From all of the stated above, make cyber risks a priority in the resilience agenda, as the strategic cross-cutting outcome of the previous recommendations.
- ***Introduction*** – here the "problem" would be stated. The topic would be introduced and since for this paper a lot of background research has been made, the main stakeholders, the causes of the current situation and its current stage will be stated.
- ***Body*** – in the body, with the help of different headlines, some of the issues raised during the contextualization and the previous research will be introduced.
- ***Policy implications*** – this part would be more aligned with the recommendations, by adding some suggestions to the current policies and situation. And, finally the effects and the potential benefits of the application of this project will be presented.
- ***Conclusions*** – although conclusions are not always recommended, it is advised not to repeat what has been already stated. This space will be devoted to talk about the urgency of addressing this topic or the importance to make it a priority.

4. Conclusions

If I were asked again: can disaster risk management be used to study and address cyber risks? I would still say yes.

With the development of this project, different conclusions have been drawn and some reflections have been made as well. In regards to the general and specific objectives, I have learned how to provide the Barcelona City Council with recommendations for addressing cyber risks with DRM. This learning process has been accompanied by the literature research as well as the analysis tools and data collected, mainly through the interviews. To draft the recommendations, it was necessary to first understand the position and situation of Barcelona both for cyber risks and DRM. In that sense, the previous understanding and studying of Barcelona made me identify that cyber risks are not a current priority for the Barcelona City Council in terms of urban resilience. And, as a consequence, the recommendations could not be as ambitious as intended. Consequently, they aim to develop a platform or a communication strategy that can bridge together the different stakeholders (cyber sector and DRM sector).

At the first stage of the research, I thought that I could ask the Barcelona City Council for concrete measures in terms of cyber risks and DRM. But in reality, what is necessary is to first create a communication channel between the stakeholders to start from a common ground and later make it a priority.

Moreover, the specific objectives were also accomplished. The first one was to analyze the current situation and study the accuracy of the project. As mentioned previously, the study was done thanks to the all analysis tools used, especially the PESTL. In regards to the accuracy, the SWOT analysis and the interviews with Sanjaya Bhatia and Ares Gabás, made it clear that the threats were heavier than the rest of the factors and that political will, as well as data access and availability, are determinant. In the case of this project, the fact that cyber risks are not a priority in the resilience agenda makes it very difficult to be considered. However, the same fact that the communication channel is meant to be built either inside or outside the political sphere, could facilitate its future viability.

The second specific objective was to adapt cyber risks into DRM language. Although it seems an ambitious objective, the interview with Luis Miguel Laguna assured that the concepts of DRM can be applied to most types of risks, being them caused by

natural hazards, man-made ones, or specifically in this case, by cyber threats. The concepts of DRM tackled in this project were resilience, integration of different stakeholders and experts; the holistic vision; the interrelated sectors and factors that can produce cascading effects, and that if you had not analyzed and quantified those dangers before when it happens you are caught by surprise. In this sense, cyber risks can be approached by the language of DRM if moved from its purely technical and security approach.

Furthermore, after all this research and development process, I am still confident that Barcelona is a model city for the applicability of this project, though in the coming future. Barcelona's advances in urban resilience, as well as their methods of work in the City Council through the resilient boards, makes it very dynamic and open for future-risk priorities, as Figure 1 shown in the Literature Review. At the same time, Barcelona has the Catalan Cybersecurity Agency, that as Genís Margarit stated in the interview, is starting to move from its pure technical perspective and involve experts from different fields. Barcelona is advancing in both topics, it has the infrastructure for mainstreaming DRM into cyber risks, though both are moving in separate ways.

Cyber risks and the perception of them as risks have increased over the years as the World Economic Forum states in its Global Risk Report (Mclennan, 2021). This means that probably in the coming years, cyber resilience, and the study of it as part of DRM can be better known. As for future areas of work left open by this project, according to some experts, this study could be replicated in other cities. If done so, it could create more debate and call the attention of experts and policymakers.

The fact that all this project has been sustained under three pillars (international standards) also demonstrates that international relations are very important for its development. The SDGs and the Sendai Framework have been essential to understand the principal guidelines that the Urban Department uses in its work, and have some lines of action that permit the mainstreaming of DRM into cyber risks. For example, that SDG 11 stands on resilience, and cyber resilience could be connected to that. In regards to the GAR 2019, besides being a link between the SDGs and the Sendai Framework, is a platform where case studies are published and from that publication, debates are promoted.

Additionally, a very meaningful perspective for the international relations field is that this project has taken a local standpoint. Cities are irrupting in the international scene and this was a great opportunity to show Barcelona's capacity to stand by international

standards and commitments. My personal motivation for international and national politics, as well as international organizations has been reflected in the materialization of the project. The design of a policy brief as a document for the local government was a challenging exercise of revising, adapting, and adding the context of the previous research in a more dynamic format and being able to mix both research topics.

To end, despite the limitations of data and academic literature regarding the topic, and the challenge of adapting the technical language and different academic disciplines into one language, it can be assumed that the empiric nature of the study has shown some positive results and conclusions. There are still many parts and questions to answer and many items to deepen on, thus, future research is deeply encouraged in some years to come.

5. Bibliography

Accenture. (2018). *The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience*.

Ajuntament de Barcelona. (2021). *Presupuesto 2021*. https://ajuntament.barcelona.cat/pressupostos2021/es/

Ajuntament de Barcelona. (2016). *Barcelona. Building a Resilient City*. https://ajuntament.barcelona.cat/ecologiaurbana/sites/default/files/ModelResilienciaBarcelona.pdf

Ajuntament de Barcelona. (2017). *Barcelona: Building a Resilient City*.

Aven, T. 'What is safety science?', *Saf. Sci.*, vol. 67, no. 925, pp. 15–20, 2014.

Baum, S. D. (n.d.). Risk and Resilience For Unknown, Unquantifiable, Systemic, and Unlikely/Catastrophic Threats. In *Systems, and Decisions* (Vol. 35, Issue 2). http://sethbaum.com*http://gcrinstitute.org

Berg. H.P. (2010) '*Risk management: procedures, methods and experiences', Reliable Theory Applied*, vol. 1, no. 17. Germany.

Branscombe M. The New Stack; 2020. *The network impact of the global COVID-19 pandemic*. https://thenewstack.io/the-network-impact-of-the-global-covid-19-pandemic/

Calabozo, A. (2020, April 22). *Resilient Cities and Urbanism: A Case of Barcelona*. https://www.re-thinkingthefuture.com/uncategorized/resilient-cities-and-urbanism-a-case-of-barcelona/

Centre de Seguretat de la Informació de Catalunya (CESICAT). (2019). *Estratègia de Ciberseguretat de la Generalitat de Catalunya 2019-2022*.

Chelleri, L., & Baravikova, A. (2021). Understandings of urban resilience meanings and principles across Europe. *Cities*, *108*. https://doi.org/10.1016/j.cities.2020.1029855

Chickowski, E. (2020). *Cybersecurity Risk Management Framework, Best Practices Explained*. AT&T Cybersecurity. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-risk-management-explained

Eggers, W. D. (2016). *Government's cyber challenge Protecting sensitive data for the public good*. www.deloittereview.com

ENISA. (n.d.). *National Cybersecurity Strategies* . https://www.enisa.europa.eu/topics/national-cyber-security-strategies

FAO. (n.d.). *Writing Effective Reports: Preparing policy briefs*. www.cde.unibe.ch/userfiles/file/NCCR_

Filippi, M. (2014). *Planning in a complex, changing and uncertain urban reality: The emergence of a resilience planning paradigm in the city of Barcelona*. https://www.ucl.ac.uk/bartlett/development/sites/bartlett/files/wp194.pdf

Financial Times. (2020). *London storms inaugural Tech Cities of the Future ranking*. Financial Times. https://www.fdiintelligence.com/Locations/Global/London-storms-inaugural-Tech-Cities-of-the-Future-ranking

G. Juanes, G. (2017). *El Parlament aprueba la creación de la Agencia de Ciberseguridad de Cataluña*. Cuadernos de Seguridad. https://cuadernosdeseguridad.com/2017/07/parlament-aprueba-la-creacion-la-agencia-ciberseguridad-cataluna/

Generalitat de Catalunya. (2020). *Pressupost 2020, Catalunya 2030*.

Generalitat de Catalunya. (2021). *Pròrroga 2021. Departament de la Vicepresidència i d'Economia i Hisenda*. http://economia.gencat.cat/ca/ambits-actuacio/pressupostos/2021/prorroga-2021/

Giddens, A. 'Risk and responsibility', *Mod. Law Rev.*, vol. 62, no. 1, pp. 1–10, 1999.

Gobierno de España. (2013). *National Cyber Security Strategy*.

Guarnieri, M. 'Landmarks in the history of safety', *J. Safety Res.*, vol. 23, pp. 151–158, 1992.

Habitat III. (2017). *New Urban Agenda* (pp. 1-66, Rep.). Quito: United Nations.

Hollnagel, E. 'Is safety a subject for science?', *Saf. Sci.*, vol. 67, pp. 21–24, 2014.

Instituto Geofísico. *Riesgos*. https://www.igepn.edu.ec/

Mamello, T. (2020). *Building resilience in the time of Covid-19 and beyond*. Global Dev. https://www.globaldev.blog/blog/building-resilience-time-covid-19-and-beyond

Mamello, T., & Debora, I. C. (2020). *Cyber resilience in the time of Covid-19 and beyond*. South China Morning Post. https://www.scmp.com/tech/enterprises/article/3083818/cyber-resilience-time-covid-19-and-beyond

Marr, B. (2018). *The 4th Industrial Revolution Is Here - Are You Ready?* Forbes. https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/?sh=7b873ff4628b

Mclennan, M. (2021). *The Global Risks Report 2021* (16th ed.). http://wef.ch/risks2021

Mello, J. P. (2020). *Cyber resilience: What it is, why it matters—and how to get started*. TechBeacon. https://techbeacon.com/security/cyber-resilience-what-it-why-it-matters-how-get-started

Mizutori, M. (2019). *Our Work*. https://www.undrr.org/about-undrr/our-work

Muñoz, T., & Sans Tarragona, S. (2021, January 22). *Una veintena de ayuntamientos, atacados por ciberdelincuentes*. La Vanguardia. https://www.lavanguardia.com/local/barcelona/20210122/6189766/veintena-ayuntamientos-atacados-ciberdelincuentes.html

Northbridge Insurance. (2016). *What is cyber risk, and why should I care?* https://www.nbins.com/blog/cyber-risk/what-is-cyber-risk-2/

Ntoko, A. (2011). *Global Cybersecurity Agenda (GCA): A framework for international cooperation*.

PA Consulting. (2018). *Smart cities demand smart cyber resilience*. PA Consulting. https://www.paconsulting.com/insights/smart-cities-demand-smart-cyber-resilience/

Regional Technical Centre for Disaster Risk Management, Sustainability and Urban Resilience (DiMSUR). (2020). *City Resilience Action Planning Tool* (pp. 1-39, Rep.). Kenya: United Nations.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 49–71. https://doi.org/10.1080/136698798377321

Smart City Hub. (n.d.). *Barcelona: showcase of smart city dynamics*. https://smartcityhub.com/technology-innnovation/barcelona-showcase-smart-city-dynamics/

Tidy, J. (2020). *Police launch homicide inquiry after German hospital hack*. BBC News. https://www.bbc.com/news/technology-54204356

Toregas, Costis. (2020). *COVID-19: When a health crisis drives cyber risk*. Prevention Web. https://www.preventionweb.net/experts/oped/view/71249

Toregas, Constantine, Santos, J., Jahn, M., Oemichen, W. L., Treverton, G. F., David, S. L., Rose, M. A., Brosig, M., Hutchison, W. K., Rimestad, B., & Otto, T. (n.d.). *Cybersecurity and its cascading effect on societal systems*.

UNDRR. (2020). *Bridging Cybersecurity and Disaster Risk Reduction Working Paper*. 1–4. https://www.preventionweb.net/publications/view/71543

UNDRR. (2017). *Disaster risk reduction & disaster risk management*. Prevention Web. https://www.preventionweb.net/disaster-risk/concepts/drr-drm/

UNDRR. (2019a). *Global Assessment Report*. https://gar.unisdr.org

UNDRR. (2019b). *Words Into Action: Local Disaster Risk Reduction and Resilience Strategies*. www.undrr.org

United Nations. (2015). *Goal 11 of Sustainable Development*. https://sdgs.un.org/goals/goal11

United Nations. (2017). New Urban Agenda. *United Nations Conference on Housing and Sustainable Urban Development (Habitat III)*, 1–66.

United Nations Digital Blue Helmets. (n.d.). *Cyber Risk*. https://unite.un.org/digitalbluehelmets/cyberrisk

United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015 - 2030*.

United Nations Secretary General. (2020). *Implementation of the Sendai Framework for Disaster Risk Reduction 2015-2030 Report of the Secretary-General*.

United Nations University Institute in Macau. (2020). *Smart Citizens Cyber Resilience*. United Nations University Institute in Macau. https://cs.unu.edu/smart-citizens-cyber-resilience

Urban Resilience Hub. (n.d.). *What is Urban Resilience*. Retrieved March 4, 2021, from https://urbanresiliencehub.org/what-is-urban-resilience/

Urban Resilience Hub. (2019). *Barcelona*. Urban Resilience Hub. https://urbanresiliencehub.org/city-hazards/barcelona/

van den Berg, B., & Prins, R. (n.d.). *Security and Safety: A Conceptual Analysis*.

Ventayol, I. (2014) '*Barcelona, resilient city: Climate change adaptation*. Presentation (March 2014)'. Barcelona

What is SixSigma. (2018). *Business Risk Management (BRM)*. https://www.whatissixsigma.net/business-risk-management/

Wolfers, A. "National Security" as an ambigious symbol', *Polit. Sci. Q.*, vol. 67, no. 4, pp. 481–502, 1952.

World Bank. (2020). *Disaster Risk Management Overview*. World Bank. https://www.worldbank.org/en/topic/disasterriskmanagement/overview#2

Wright, J., & Goel, S. (2020, May). *Advancing cyber resilience in a COVID-19 world*. Willis Towers Watson. https://www.willistowerswatson.com/en-IN/Insights/2020/04/advancing-cyber-resilience-in-a-COVID-19-world

6. Annex

Annex 1. Historical evolution of Safety and Security disciplines

In our daily lives, it is quite common to hear about food safety, cyber security, or child safety. But what is exactly the difference between safety and security? And why are they studied separately?

On the one hand, scholars that study security aspects, do so through Security Studies, a sub-discipline of International Relations. Historically, the discipline achieved leverage during the Cold War, when it was related more to nation states' security. But, it was in the 70s and 80s that its conceptualization gradually started to change (B. van den Berg & Prins, n.d.). For example, the notion broadened in order to include threats like crime, environmental degradation, or cyber security; risks other than military. At the same time, scholars also added that security did not only target national levels, but also sub and supra state levels, such as individuals or regions (B. van den Berg & Prins, n.d.).

Nevertheless, it is important to note that a "condition" for an activity to be considered as a security threat, is that such activity has to be instigated intentionally. In other words, according to Prins, "we only call something a threat when there is an active, purposeful intent behind the activity that causes that threat". In international relations, with the emergence of non-state actors in the security realm, we find terrorist activities as security threats or risks, in that such activities are inflicted intentionally and purposefully towards a target. But what is exactly security? According to Wolfers (p. 451), security "measures the absence of threats to acquired values". That is to say, it prevents intentional threats that could damage not only human beings, but also their acquired values. This may imply that, if security aims to prevent threats, its emphasis would be on the cause of the threat, rather than on the "victim".

On the other hand, Safety Science studies risks with an opposite perspective. Safety, as different as security, was first studied during the 1900s in order to understand in a better way the cause of accidents (Guarnieri, M. 1992. p. 152). For example, with the Industrial Revolution and thus the beginning of the mechanization of work, workers started to increase their chances of having workplace accidents. In that sense, Safety Science concluded embracing different themes and fields that studied accidents and other ways that people could get harmed, for instance, natural disasters or diseases (B. van den Berg & Prins, n.d.). However, one of the aspects that makes this discipline different from

Security Studies, is that safety, or the study of accidents, comes from non-intentional aspects, rather than intentional. As just mentioned, the effects of natural hazards such as earthquakes or floods, as well as the spread of a virus, or chemical and food safety, could be indeed studied through Safety Science.

The approach mostly used in this discipline is called "risk management". Even though this new concept will be broadly discussed in the paragraphs below (as it is the tool that will be used for the Project) it is important to mention that it "seeks to establish how dangerous or potentially harmful phenomena can be reduced to what has come to be termed as "acceptable risk levels"" (Aven, T. 2018; Giddens, A. 1999; Hollnagel, E. 2014). Here, Safety Scientists would try to understand the vulnerabilities, the existence of risks, their likelihood to happen, and their possible impact. It aims to prevent and mitigate such risks in the future. Another aspect that contrasts the Security discipline is that Safety Science is more focused on protecting first, rather than taking away the cause. Thus, those "receiving end" of the dangers could be prevented from an unintentional harm (B. van den Berg & Prins, n.d.).

Annex 2. Current stage of Disaster Risk Management

The current stage of the implementation of the Sendai Framework (2015-2030) as well as the process made towards achieving the targets, shows the necessity to increase countries' commitment. The UN Secretary-General (United Nations Secretary General, 2020) pointed out that in terms of the target E of the Framework, which calls for local DRR strategies to be implemented before 2020, needs a substantial increase of participants. One of the reasons behind the low participation is the scarcity of data collection on the seven targets of the Framework, as well as from disaster loss and damage statistics (Idem). In that sense, there is a very good initiative made under the Global Centre for Disaster Statistics and the United Nations Development Program (UNDP) that aim to establish a "global cloud-based platform for the collection and analysis of disaster loss and damage statistics" (United Nations Secretary General, 2020). A very accurate tool, since it helps to institutionalize data collection for monitoring on disaster losses.

Even if countries are still implementing and designing the best strategies to implement the Sendai Framework, it is necessary to stress what this Framework permits and tries to work on. The Sendai Framework articulates the better understanding of disaster risk and its dimensions; the vulnerabilities as well as the hazard's characteristics; the importance and strengthening of disaster risk governance which include national and local platforms; the recognition of the role of the stakeholders; "mobilization of risk-sensitive investment to avoid the creation of new risk; resilience; strengthening of international cooperation and global partnership" (UNDRR 2015). Here, agreeing with Manello et. al, the Sendai Framework "provides a useful outlook for operationalizing the polycentric resilience approach in multi-level institutional arrangements and governance. The framework explicitly recognizes that effective risk governance involves multiple actors operating at different levels" (Mamello, 2020).

Annex 3. Political factors determining Barcelona's cyber situation

The political sphere has a very strong or significant impact on this subject of study because as referred to in the SWOT analysis, political will determine the materialization of this project. In this case, some insights will be brought: on cybersecurity specifically, the Plenary of the Parliament of Catalonia approved, in 2017, a law creating the Catalan Cybersecurity Agency, in the majority of points by 88 votes in favor (JxSí, PSC and CSQP), 24 against (Cs) and 19 abstentions (PPC and CUP) (G. Juanes, 2017). Moreover, the law creates the Catalan Cybersecurity Agency, a body that replaces the previous Information Security Center of Catalonia (CESICAT) and that will be in charge of "preventing, detecting, responding to and investigating incidents or threats to electronic communications networks and public information systems, and to plan, manage, coordinate and supervise cybersecurity in Catalonia, minimize damage and recovery time to networks and systems in the event of a cyberattack and collaborate with police forces and judicial authorities" (Idem). As it can initially be perceived, when addressing cybersecurity only security and law enforcement bodies are cited as external ones to collaborate or coordinate with.

In regards to the Barcelona City Council, and according to the interview with the Head of the Urban Resilience Department, Ares Gabás, the Urban Resilience Office was created in 2014, becoming one of the first cities in the world to create a resilience office. In Barcelona, work began specifically on resilience (although this is not a new concept) in the first decade of the 2000s, motivated by various infrastructures and services crises. In 2010 UNDRR (at that time named UNISDR) launched the pioneering and flagship initiative "Making Cities Resilient" global campaign. In April 2013 Barcelona signed up joining the Campaign, being also appointed as "Role Model City on Infrastructure and Services). Also in 2013, UN Habitat began setting up the resilience program and signed a partnership agreement with the City Council. In addition, the Rocker Feller Foundation also promoted the 100 Resilient Cities initiative, that is now the Resilient Cities Network, in which Barcelona is also included. Here is where Barcelona showed off as an example of a resilient and smart city.

From that experience and in order to reduce the current vulnerabilities of the city, the resilience boards were created (see Figure 1). Their objective is to reduce vulnerability to risks related to infrastructures and services as well as natural and man-made risks that can alter the functional continuity and the provision of city services. The current priorities

are under the Climate and Social resilience agenda. As it can be noted, cyber risks are not in the agenda of resilience. But this is interesting because of the transversal nature of those boards, and who participates there. The boards are made up of multidisciplinary teams in which technical staff from the City Council work with non-municipal entities, both public and private. In this sense, the communication and work are transversal and integral. On the other hand, the cybersecurity competences, as stated previously, are given to the Cybersecurity Agency or the Municipal Institute of Informatics (IMI).

Annex 4. Economic Data and factors determining Barcelona's cyber situation

The link attached bellow will redirect you to a Drive Folder named "Economic Data – FDP" where an Excel sheet named *Marc Input-Output de Catalunya 2014* + Calculations FDP can be found. This document contains the original data from the Generalitat of Catalonia and some calculations. The self-made calculations are found in the sheets named *Matrix A, Table 2 ITD, and Matrix-A asterisco*.

https://drive.google.com/drive/folders/1QPZmI7_2M3APgMCYMKsELWhs1tK0THNB?usp=sharing

In order to measure the impact of a cyber risk in terms of cascading effects towards them, the study of Toregas and Santos, mentioned in chapter 3.1, was replicated with Catalan data.

In this case, what it has been done, as both experts did, was to consult the IO (input-output) dataset, which is of public access, of the Generalitat of Catalonia. Unfortunately, the latest version is from 2014 thus this outdated dataset does not reflect the current situation of the Catalan economic sectors in terms of their inputs and production outputs. Nevertheless, it gives us an idea of the dependence they had back before the so-called Fourth Industrial Revolution implying, for example, the adoption of cyber-physical systems, the Internet of Things and the Internet of Systems (Marr, 2018) which would be probably reflected on an updated version.

Having said that, "the economic input-output (IO) model represents an economy as a system of interdependent sectors, which provides a systematic accounting of the flow of consumed and produced goods through the system" (Toregas et al., n.d.). This econometric model as stated above tends to be of public access so its availability of "high-resolution economic data and social accounting matrices has further enhanced the applicability and relevance of the model" (Idem). The first thing that was done, then, was to look for the Interdependency Matrix which was provided by the Generalitat de Catalunya called "*Taula d'origen a preus bàsics, Marc Input-Output de Catalunya 2014*".From that matrix, the 64 economic sectors addressed there were organized by code assignation in the Table 1 showed below. As it can be seen, the Computer activities and information services' sector, or IT sector, has been designated with the S40 code.

Table 3. Economic Sector Classification

Code	Description
S1	Agriculture, livestock and related services
S2	Forestry and logging
S3	Fishing and aquaculture
S4	Extractive industries
S5	Food, beverage and tobacco industries
S6	Textile, clothing, leather and footwear industries
S7	Wood and cork industry
S8	Paper industries
S9	Graphic arts and recorded media
S10	Coking plants and oil refining
S11	Chemical industries
S12	Manufacture of pharmaceuticals
S13	Manufacture of rubber products and plastics
S14	Industries of other non-metallic mineral products
S15	Metallurgy
S16	Manufacture of metal products, exc. machinery
S17	Manufacture of computer and electronic products
S18	Manufacture of electrical materials and equipment
S19	Manufacture of machinery and equipment nec
S20	Manufacture of motor vehicles, trailers and semi-trailers
S21	Manufacture of other transport materials
S22	Furniture and various manufacturing industries
S23	Repair and installation of machinery and equipment
S24	Electricity, gas, steam and air conditioning
S25	Water collection, purification and distribution
S26	Sanitation, waste management and decontamination
S27	Construction
S28	Sale and repair of motor vehicles and motorcycles
S29	Wholesale trade and intermediaries, exc. motor vehicles
S30	Retail trade, exc. motor vehicles and motorcycles
S31	Ground transportation; transport by pipes
S32	Maritime and inland waterway transport
S33	Air transport
S34	Storage and transport-related activities
S35	Postal and postal activities
S36	Accommodation, food and beverage services
S37	Edition
S38	Audiovisual activities
S39	Telecommunications
S40	**Computer activities and information services**
S41	Financial mediation
S42	Insurance and pension funds
S43	Auxiliary activities of financial mediation and insurance
S44	Real estate activities
S45	of which: imputed real estate rents
S46	Legal, accounting and tax consultancy activities
S47	Architectural and engineering technical services
S48	Research & Development
S49	Advertising and market research
S50	Other professional, technical and veterinary activities
S51	Rental activities
S52	Employment-related activities
S53	Travel agencies and tour operators
S54	Security activities, building services and administrative activities
S55	Public administration, Defense and compulsory SS
S56	Education
S57	Health activities
S58	Social services activities
S59	Artistic and cultural activities; games of chance
S60	Sports and recreational activities
S61	Associative activities
S62	Computer repair, personal and household effects
S63	Other personal service activities
S64	Home activities

Source: self-made with data collected from IO 2014 dataset

For the second step, it should be highlighted that all of the values presented in the IO dataset were normalized with respect to the total output so their scale range from 0 to 1. So far, since the important part of this study was to measure the interdependence of the IT sector with the other sectors, I only focused on the IT sector (S40). Since the matrix is quite large, this was only done with the elements associated with the row of the IT sector. In this case, each sector that provided an input to the IT sector (output) was multiplied by 100 and then divided by the total output of the IT sector. Table 2 consequently shows the results in a rank-ordered list.

Based on the results of Table 2, it could be stated that the 10 sectors with higher dependence, besides the same IT sector which is quite intuitive, as also the experts noted, are: S39 Telecommunications; S49 Wholesale trade and intermediaries, exc. motor vehicles; S54 Security activities, building services and administrative activities, S48 Research & Development; S24 Electricity, gas, steam and air conditioning; S62 Computer repair, personal and household effects; S46 Legal accounting and tax consultancy activities; S47 Architectural and engineering technical services; and S56 Education.

From this part, it could be concluded that taking into consideration that this is data from 2014, there were already sectors dependent on the IT sector, and that in the case of a cyber-attack, they could receive "collateral damage". The next step would be to use the concept of inoperability in the IT sector in order to suppose an "attack" and be able to calculate (also the monetary value) the damage or disruption that it could cause on the other sectors. Nevertheless, this brief analysis has been made in order to emphasize that sector interdependence is very important when addressing cyber-risks because it takes the contribution of different stakeholders, mainly public and private in order to mitigate the possible threats. For example, a cyber-attack could disrupt the normal functioning of sector S24 Electricity, gas, steam and air conditioning that could consequently provoke a big blackout as commented in chapters before, or scarcity of gas or steam. If traditional cyber risk management has been done through private consultancy, then this study suggests that a shared strategy between cyber security sector, insurance industry, and government could be made (Toregas et al., n.d.). This also stresses the idea that DRM could focus on the more dependent sectors and the need for data in cyber-security operations.

Table 4. Rank-Ordered List of Sectors Based on their % Information Technology Dependence (ITD)

Rank	Code	Description	ITD
1	S40	Computer activities and information services	91,63%
2	S39	Telecommunications	2,12%
3	S29	Wholesale trade and intermediaries, exc. motor vehicles	1,49%
4	S54	Security activities, building services and administrative activities	0,72%
5	S48	Research & Development	0,62%
6	S24	Electricity, gas, steam and air conditioning	0,58%
7	S62	Computer repair, personal and household effects	0,49%
8	S46	Legal, accounting and tax consultancy activities	0,39%
9	S47	Architectural and engineering technical services	0,33%
10	S56	Education	0,32%
11	S41	Financial mediation	0,16%
12	S27	Construction	0,14%
13	S59	Artistic and cultural activities; games of chance	0,12%
14	S38	Audiovisual activities	0,11%
15	S57	Health activities	0,091%
16	S12	Manufacture of pharmaceuticals	0,069%
17	S30	Retail trade, exc. motor vehicles and motorcycles	0,061%
18	S61	Associative activities	0,060%
19	S51	Rental activities	0,059%
20	S50	Other professional, technical and veterinary activities	0,058%
21	S7	Wood and cork industry	0,057%
22	S16	Manufacture of metal products, exc. machinery	0,053%
23	S42	Insurance and pension funds	0,037%
24	S9	Graphic arts and recorded media	0,036%
25	S53	Travel agencies and tour operators	0,032%
26	S43	Auxiliary activities of financial mediation and insurance	0,032%
27	S5	Food, beverage and tobacco industries	0,029%
28	S34	Storage and transport-related activities	0,029%
29	S1	Agriculture, livestock and related services	0,015%
30	S4	Extractive industries	0,015%
31	S10	Coking plants and oil refining	0,014%
32	S49	Advertising and market research	0,012%
33	S13	Manufacture of rubber products and plastics	0,010%
34	S22	Furniture and various manufacturing industries	0,010%
35	S63	Other personal service activities	0,004%
36	S60	Sports and recreational activities	0,003%
37	S23	Repair and installation of machinery and equipment	0,002%
38	S21	Manufacture of other transport materials	0,001%
39	S25	Water collection, purification and distribution	0,000%
40	S2	Forestry and logging	0,000%
41	S3	Fishing and aquaculture	0,000%
42	S6	Textile, clothing, leather and footwear industries	0,000%
43	S8	Paper industries	0,000%
44	S11	Chemical industries	0,000%
45	S14	Industries of other non-metallic mineral products	0,000%
46	S15	Metallurgy	0,000%

47	S17	Manufacture of computer and electronic products	0,000%
48	S18	Manufacture of electrical materials and equipment	0,000%
49	S19	Manufacture of machinery and equipment nec	0,000%
50	S20	Manufacture of motor vehicles, trailers and semi-trailers	0,000%
51	S26	Sanitation, waste management and decontamination	0,000%
52	S28	Sale and repair of motor vehicles and motorcycles	0,000%
53	S31	Ground transportation; transport by pipes	0,000%
54	S32	Maritime and inland waterway transport	0,000%
55	S33	Air transport	0,000%
56	S35	Postal and postal activities	0,000%
57	S36	Accommodation, food and beverage services	0,000%
58	S37	Edition	0,000%
59	S44	Real estate activities	0,000%
60	S45	of which: imputed real estate rents	0,000%
61	S52	Employment-related activities	0,000%
62	S55	Public administration, Defense and compulsory SS	0,000%
63	S58	Social services activities	0,000%
64	S64	Home activities	0,000%
		Total	100,00%

Source: self-made with data collected from IO 2014 dataset

Annex 5. Interviews

Considering that the lack of literature on DRM and cyber risks has been an ongoing challenge, interviews and data collection have been essential. The participation of different experts both in cyber risks, DRM, or urban resilience has contributed to a clarification and exemplification of the current situation and the accuracy of this FDP. It is important to highlight the international profile of all interviewees. I have tried to move from a Barcelonan Spanish-centered data collection and therefore, interviewees were placed in Europe, Asia, North America, and South America, making their approach even more insightful.

In that sense, 7 interviews were conducted. The format of the interviews was the following: 1 structured interview, where all questions were sent previously to Ares Gabàs; and 4 semi-structured interviews, where standard questions were combined with the additional information that the interviewee provided. This was the case of the interviews with Luis Miguel Laguna, Costis Toregas, Genis Margarit, and Sanjaya Bhatia. The two remaining interviews were made as a source of feedback. The first one was held with Mateo Loaiza, an Econometrics graduate student from *Universidad de las Américas* from Quito, Ecuador. Mateo's knowledge was essential to understand the Input-Output dataset, as well as the replication of Torega's study for Barcelona. The last interview was held to Mr. Ricardo Mena, current Director of UNDRR. His interview was essential in the first stage of the study, as he helped me to get the best sources and contacts. Finally, he was contacted again at the end of the project in order to show the outcomes and the results. His feedback was very positive as he found that this FDP contributes to the current literature, and encouraged me to keep researching on the topic. Nevertheless, this interview has not been included because the results have not been used in the paper.

Consequently, the interviews that have directly contributed to the research and development process of this FDP can be found below.

Interview 1. Luis Miguel Laguna

Source: LinkedIn profile

Luis Miguel is an engineer and a DRM and resilience expert. His broad background as consultant in DRR projects management and strategies have provided him with a wide knowledge on other interconnected fields such as climate change, resilience to disaster, and cross-cutting related areas of management.

What are the advantages and benefits of taking a disaster risk management perspective?

In essence, DRR is a risk management concept that basically comes from the united nations. The theme of DRR is a rather generic concept that attempts to convey the concept of disaster risk management.

These concepts are integrated into the management of any issue, at the level of a company, a country, any entity, any other private company, it is a way of dealing with risks. It has a series of principles and a series of basic ideas such as that everything must be contemplated within the same cycle, where it is necessary to study, prepare for the risks that may arise, this implies investing, allocating resources, setting up strategies, work plans, tools... so that when a possible impact produced by an external element or danger occurs, to be better prepared to face it and at the same time to build the principles and whatever is necessary to face it. This is applicable to any type of risk, be it cybernetic or natural.

United Nations were the first, focusing on natural hazards. During the 1990s with natural hazards such as earthquakes, tsunamis, hurricanes, because they were events that were thought to be less controllable, or how to deal with them. But then it became clear that there are also biological hazards that can also cause similar phenomena such as pandemics. Technological risks or man-made hazards. For hazards and risks, the main formula we have been working with is that risk is a product of the probability of a given hazard occurring due to the vulnerability of the exposed assets and the exposure itself.

And what about cyber risks?

All these DRR concepts are applicable to many economic and human activities of civil society. In managing a city, cyber risks should be taken into account, I believe that the issue of cyber risks is a matter of the city's own responsibility. I think so, but it is a matter of getting into it. A lot is being learned very quickly on these issues.

Many things people already know, especially specialists, the important thing is to integrate some things with others, to break centuries of work, where we have become accustomed to working from technical, social, economic specialties, each one separately and not communicating well and believing that the others are not important.

Can we talk about the role of cities?

United Nations promote and lead, although in the last decade new actors and initiatives such as the resilient cities network have grown. We must focus on cities and work at the local level. This is something that is a novelty compared to previous decades, because then it was only through the governments. It has been seen that governments are essential but cities are necessary. All these initiatives have integrated older initiatives with more actions, before it was more about awareness and networking, now it is intended to move to action.

The topic you are interested in can be approached perfectly from this point of view, this provides very general concepts for what you need, but if you do not incorporate these concepts that emanate from the Sendai Framework and other initiatives, you would lose many important points, especially the holistic vision, the vision of systemic risk, that there are many interrelated things that can produce cascading effects, dangers occur and that if you had not analyzed and quantified before, when it happens you are caught by surprise.

It is very important because the people who have to make investment decisions, whether they are politicians or managers, if you do not go with the economic data, you do not convince them, and this is already happening a lot. The particular tools for hazards can be provided by a specialist, but not only the hazard has to be analyzed, the study has to be extended to vulnerabilities, exposure, how to implement it later, it has to be inclusive, you have to sit down with all partners and stakeholders and design together,

integrate the concepts of risks as something systemic. Many of these things are not even considered by cyber specialists because they are specialists in very specific topics.

What is needed to be done?

Put the issue in context from that perspective and see if the concepts are integrated.

And what about Barcelona?

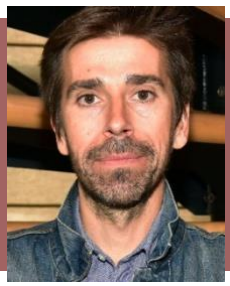
Barcelona is the best place is Spain for these issues. It is not doing like Barcelona anywhere else. In other places things are being done but not as much as in Barcelona, things are not approached from resilience, to unify so that things work together in the same line, because this makes everything more efficient. There are many scattered actions but they are not called by the name of resilience.

How expensive would it be to apply this FDP idea?

It is not so expensive because you are seeing that investing in prevention is a saving when the danger is triggered, if invested properly. You have to consider it as an investment and not as an expense, but this is the problem of wanting to see short-term benefits.

It's everybody's business.

Interview 2. Genís Margarit



Genís is a Telecommunications Engineer from the Universitat Politècnica de Catalunya with more than 15 years as a consultant in cybersecurity, data privacy and IT. His professional specialties are data protection, TIC teaching, and networking.

Source: LinkedIn profile

What is the current "cyber situation" in Catalonia?

Catalonia has followed the European directive on cybersecurity - it has been developed in the last decade, the member states have been requested to create cybersecurity agencies, which should not have only one approach purely technical or technological, if not risk management. If there is a cyber threat, it affects the Catalan economy, society, citizenship, because if your mobile credentials are stolen, it harms you as a person, and also the services.

I would not hesitate to say: in the field of cybersecurity to date, unfortunately, we have only been working technologically and this is not enough. In fact, what we are experiencing now are failures. Cyber risk management has to escalate towards the governance bodies and wherever they are doing risk management and they also have to do cyber risks.

All people, whether they are physical or legal, have a digital life, no one can imagine a natural person in the 21st century without a digital life, and neither can a legal person without a digital life, and this digital life is protected through cybersecurity measures. With this the framework is mounted.

What is being done in European democracies?

The creation of cybersecurity agencies is being promoted - and these agencies aim to protect the digital life of companies, institutions and people.

In Spain it is in INCIBE which has a long history of more than a decade - second term of Zapatero. In Catalonia, the cybersecurity agency was approved this last legislature. All political parties agreed to set up the cybersecurity agency. From the social and political

point of view of risk government, you reinforce saying that there are no political lines or ideologies that do not see importance in cybersecurity, all parties agreed.

Have we been more technologically exposed during the pandemic?

With COVID, there has been an increase in users of information systems, who were not a minority but used 10-15% of working people and now use 100% of people who now telecommute. Many people started using platforms of this type for the first time.

More people teleworking implies an increase in cases - a significant increase in users has been related to users who were less digitized.

Is Barcelona a cyber-secure city?

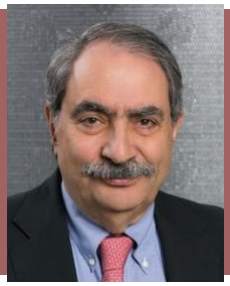
Each of the large cities worldwide is equipped with its own security, and with its own security forces. From Barcelona there is no cybercrime. Barcelona is not a nest for cybercriminals. Cyberattacks do not come out of Barcelona - we are not on the crest of the internet core either, these are China, Russia, India, the US, and there you can see that cyberattacks come out of there. Spanish telecommunication operators are not tolerant of actions. We are not a digital paradise. We are more diligent, it is a healthy system.

From a local point of view. If we talk about the local government, the IMI department - of the Barcelona city council (Institut Municipal d'Informatica) - they have a very well-equipped cybersecurity department.

And what about cyber resilience?

Resilience from the point of view of an attack is difficult because it is debated whether to save or transition to the cloud - autonomy is lost, and our resilience depends on Microsoft or whoever it is - municipalities are reluctant to these things, usually they keep them on hard drives.

Interview 3. Costis Toregas



Source: GWU

Costis is the Director of the Cyber Security and Privacy Research Institute at The George Washington University, where he manages and conducts research projects in cybersecurity. His research interests include workforce development, and the role of insurance in cyber risk management. He has many publications and has contributed in GAR 2019 and other UNDRR initiatives.

This interview was be based on two different types of questions: him as a cyber expert (very technical-engineering), and as form his experience with UNDRR (less technical, and more policy oriented).

How did you thought that engineers need DRR for addressing cyber-risks and cybersecurity?

From both views: from a human and an intellectual point.

From a human viewpoint, around 2017 or so I was convinced that cybersecurity threats that I was seen had to be viewed and responded to in a more dynamic way that they were before. This interrelationship between events, the cascading effects, were very important to me and I was absolutely intrigued with the fact that no one was talking about that in an engineering way. Because engineers do cascades all the time but not in the cybersecurity space. A friend of mine in GW introduced me to Joost Santos which was from another part of the School of Engineering. He has done many papers of cascades and cyber risks and so we partnered in order to professional and make more engineering approaches to risks.

Then something happened, the GAR 2019 issued a call for papers. And we found it very interesting prestigious, well cited, so we decided to do a paper. From my position in DRR, I was one of the expert group for DRR to help Global Risk Assessment Framework (GRAF), there I met Ricardo.

In my mind this is all about human relations and human connections. My relationship to Joost was creative.

Any comment on DRR's traditional way of work?

You say in your paper as well is that DRR is right now a very traditional organization of individuals. They have been set for a very long time. And in Barcelona they know about it, but generalizing, the don't like new ideas. When you come up with someone that says computers run our lives and relate to other computers so it is not a particular project of a computers, it's everything, because everything is related. And here is where they say, this is for mathematicians, for computer scientists it's not for us in DRR. So it's an interesting challenge to get DRR people to even understand that computers should be included in their scope.

I wanted to try to help the DRR community understand that computers, computer science, cybersecurity, blockchain all these things are tools for them.

I found very interesting the concept of cyber resilience because since DRR is linked to the Sendai Framework, this Framework is also linked to the SGS, and resilience is a main component of them, working towards cyber resilience could work as the bridge between these two sides.

This is because it is not in the mindset of people yet. Maybe your paper could help to develop a discussion. There is a lot of active participation now, it is now slowly starting. The way that you get DRR and DRM folks to understand the importance is to constantly present them with the reality of what's happening in the world.

I don't know what else to do in the DRR community to convince them that the strategies they deploy cannot only be strategies of material logistics but also about data. The reality is that we all depend on that that if we didn't have it would be a truly disaster.

I spoke to the Head of Urban Resilience Department from the Barcelona City Council and we discussion that cyber risks are not a priority for Barcelona. She did not identify cyber risks as a priority. Then my viewed changed a bit and started to be convinced that it can be a matter of political will, all along with the traditional view that cyber risks are addressed through security. Have you had a similar thought?

For about 30 years I was not in computers and cyber security, I was working on innovation for local governments and I run a network of local governments in the US that had relationships around the world, and Barcelona was a very progressive city, with

Pascual Maragall. And everything that Barcelona did was ahead of every city in the world, it was very smart. The way they used incentives and prepared for the Olympics. It had a marvelous administration and management so what you say worries me and saddens me. **It's very sad that they did not give priority to cyber security, when what they only need to do is to look at the cities and hospitals that have been taken by criminals and have lost millions of dollars**. Or just the shutdown of operations and traffic systems and water systems. I hope that the hackers don't read your papers.

What would you advise to policy-makers in order to mainstream DRM into cyber risks, and start to take them into account?

It goes both ways, mainstream DRM into cyber risks or mainstream cyber risks in DRR. Definitely both sides need to understand each other. So recommendations would include: communications platforms. Usually DRR people would never meet the cyber security people. There is no reason for them to meet. So you have to develop platforms where people can sit down and share problems and solutions to those problems. Whether it is a monthly meeting to review all major risks for the city, or for the region. Or whether is to develop an inside to a specific risk for DRR people like computer risks. You need that meeting place periodic and with outcomes designated.

The second thing is the communication to the top policy-maker has to be done early and has to be done well. Most policy makers don't understand computers, cyber risks, that is not their domain. Their domain is to shake hands and have good programs. But, if you can somehow develop a communication strategy to the decision maker that talks about that risk is not unavoidable and bad things can be avoided if you have a DRR strategy and they accept that as a foundation, and if they accept that as within DRR they we are talking about multirisk, multiple risks, like earthquakes, water contamination, but also cyber risks. And they you go through a process to prioritize and make sure that someone is in charge of the major risks and has a responsibility to report back to the major.

Any final thought?

The last thing I would say is that I thought that **you did a very courageous thing to do an analysis and to present Table 2 (Economic Data Annex)**, which what you show is that there is a self-impact towards computer. But in my mind, I think it was accurate that you mentioned the top 10 and give this to DRR people in the discussion and make them

see if that relationship is unusual or expected to see that relationship. If they say that this is unusual, they could perhaps prepare a little bit better. The challenge is always that DRR people don't see cyber-attacks as their responsibility but for the computer guys and that's not true. Because computer guys are worried about computer inoperability, but who is worried about municipal inoperability? The fact that hospitals may not work, that police department may not get on their cellphones because the cell towers are not working. Inoperability is not only a computer event, it is an operational event. Not for the computers networking but for the city networking. So all of the sudden, Barcelona has to understand that it is not for the computer people.

And I think that if you get it on your paper, you may get a good reading from the Municipality and the region.

Interview 4. Ares Gabàs

Ares is an architect and the Head of the Urban Resilience Department of the Barcelona City Council. Currently she is in charge of the development of the resilience strategy and project implementation carried out through the Resilience Boards.

Source: Ajuntament de Barcelona

1. **What is your vision of the SDGs and the Sendai Framework?**

We have them as a reference, these types of agendas set global objectives and benchmarks that are good for us for long-term visions; they give us guidelines. They are not day-to-day instruments but are linked to a more strategic, conceptual or work methodology planning. These frameworks help us to focus our goals.

Since this mandate of 2 years ago, an area of the 2030 Agenda city council was created, with a team that is in charge of studying the SDGs.

2. **Is Barcelona an example of a resilient city?**

It is one of the leading cities because we have been working on this for quite some time. Here in Barcelona, work began specifically on resilience (although this is not a new concept) in the first decade of the 2000s, motivated by various infrastructures and services crises. Everything was failing all at once and the mayor at that time questioned what was happening, a diagnosis was made and work began. Some urban infrastructure and services boards were created that later became the resilience boards because they were projects to reduce or eliminate these risks. It was what later led to the resilience program and later the department. We are one of the first cities to start working on it. In 2013, UN Habitat began setting up the resilience program and we made the agreement, but the Rocker Feller Foundation also promoted the 100 Resilient Cities initiative that is now the Resilient Cities Network.

Before that, there weren't many cities, we were quite alone. But now it's very good. These programs were the triggers, also due to the investment it had. Now it seems that it is something relatively common, but it was not really like that. So yes, from the experience we have, it could be said that Barcelona is an example of a resilient city.

4. How is your work dynamics in the resilience department? Do you create smaller working groups with specific topics? Are professionals from different fields involved? Or these have a more technical profile. For example, if you are dealing with a climate change issue, the participants come from the environmental sector, and experts in health, migration, etc. do not participate.

The boards have evolved, we are about to launch them. They have always had a transversal vocation. It has progressively implemented a more holistic vision. Now the working groups involve private service companies; because competitions in cities are often not only public or municipal. The transversal spirit has not changed, but the approach has, since we have incorporated other types of risks. Now we are in a process of reviewing the methodology to relaunch the working groups at the municipal level under the umbrella of the Municipal Management, which guarantees that they are in some way transversal and that they are decision-making spaces, which had evolved at a level very technical but they have to continue working like this, just raising a little, so that all areas (because they are managers' boards) can make decisions. The focus is also to reduce risks and vulnerabilities and now also as a result of the pandemic it has been that we have responded well and that the crisis management mechanisms (which have experience) have worked well. This experience also serves us as learning and work material.

It is important to address these issues in a transversal way and not vertically. The vision of analysis in databases and information management has to support decision making.

5. What other departments of the City Council do you work with? By chance with the IT department (IMI)?

With several. With one of those we work most closely that also has a very similar nature to ours is the Office of Climate Change, which is very transversal, especially because of the Barcelona Climate Plan, it touches many areas. We are also part of the Climate Plan. Historically we also work with Infrastructure, Mobility, Urban Services, also with Social Rights, since now we also touch on these issues in resilience. Potentially, with the boards with anyone, although you can't tackle it all at once. With the boards are all the generic areas involved, Economy, Urban Ecology.

With the IT sector, in some way we have a relationship, but because of the specified and because sometimes security issues are difficult to determine, and because now it is not the most worrying thing, fortunately. We see that things have happened, they inform us,

but we have not entered because we cannot tackle everything at once. Computer topics are also a bit opaque because it is a more difficult topic.

6. **What is your relationship with the most political sector of the city council? Do you consult your work with / do you have the support of the political forces of the City Council?**

You can never be independent, but it has been an issue, for example climate change with resilience at the political level has not been so worked. It has been taken more at a technical level, although without a prior political decision nothing can be done. not so much has been explained to citizens.

There are a number of priority issues or issues that become more representative that they want to highlight as main, and it is implicit that the issues of resilience are there, but explicitly so far they have not transcended so much. But the support is there. Resilience is now also a topic that I understand better with the pandemic, and that is why we now believe that it can be better explained. It is a fairly invisible issue and traditionally has not been explained to politicians because it is not attractive either. Instead, it is something you see when things fail.

7. How difficult is it to integrate a new risk into your work schedule?

We try to align ourselves with the city's agenda, but we are also doing analysis to determine new priorities. Climate change, for example, is now a priority issue, as we focus on it. Also, with unexpected events. You have to see how we recover, there are things that put themselves on the agenda.

What you have to do is change the focus on prevention issues to advance them as much as possible. Any type of risk does not prepare you for another, but the culture of prevention and action does; the way it is approached and posed helps to manage other risks. This has happened to us with the pandemic.

Interview 5. Sanjaya Bhatia

Source: GETI

Sanjaya is the Head of the Office of UNDRR Office for Northeast Asia (ONEA) and Global Education and Training Institute (GETI) for Disaster Risk Reduction in Incheon, Korea. He has trained more than 300 government officials and has supervised capacity building programs for local governments. He works in mainstreaming DRR.

How can you convince policy-makers that DRM is essential?

The most important thing is to try to explain how disaster push back development so if you move this much forward that pushes back again you waste a lot of resources. Investing in DDR or resilience is definitely a way. But we need to look at as investment to the future and not as a cost.

We also give examples of cities that have faced disasters, and try to bring city champions who can be examples. When a government talks to another government, they understand better and they feel that if someone does it they can also do it. Mixing cities is a very good initiative.

How do you deal with the lack of data?

Lack of data has become a constraint. There are a lot of challenges with data that we have come across with some governments – data comes from different sides.

The quality of data is also important because it has to be cleaned. In that sense, there are a number of initiatives that are making aware how important data is – like the World Council for City Data.

And how do you deal with the lack of political will?

Political will is another vast challenge, so we try to convince majors in many aspects of resilience, through making cities resilient.

Cyber risks can become a priority definitely – one of the things that they talk about when they talk about resilience is prepare for the unexpected – now with the COVID there are many governments are unprepared, and for example, there have been cyberthreats to hospitals.

Annex 6. Policy Brief

Even though this FDP was aimed to develop a study that could permit the design of a policy brief for the Barcelona City Council, it was though appropriate to materialize such idea and finally have as an outcome a policy brief document. In that sense, and as described in chapter 6.4.1, the steps were followed and a 4-page policy brief was drafted.

It should be noted beforehand that this is only a proposal. In order to have a final document, more research time, resources, knowledge and expertise would be needed in order to share it with the political authorities. So far, it intends, as the recommendations show, to create a communication strategy between the different stakeholders to facilitate their common perspectives and start to collaborate within one voice. As a personal reflection, this work has meant a materialization of my current interests, mainly politics and DRM. It has been a very challenging exercise since all the content of this FDP has been summarized and adapted to a less technical language.

Mainstreaming Disaster Risk Management Into Cyber Risks

Policy Brief Proposal to Barcelona

Blanquerna RAMON LLULL UNIVERSITY | School of Communication and International Relations

Policy recommendations

- **Develop platforms** where dialogue can occur consistently and periodically with stakeholders from the DRM and cybersecurity sectors. In addition, let civil society participate in those discussions so advocacy can take place.
- **Develop a communication strategy** for decision makers that convinces them that hazard is not unavoidable, but disasters can be significantly reduced by having a DRM strategy, as cyber threats are increasingly affecting and exposing compromised and personal data.
- **Promote** through universities **learning sessions** or webinars where both sides (or different stakeholders) can sit down to hear each side's scientific foundation.
- **Train, train, and train.** Provide major policy emphasis to prevent risks and their possible cascading effects. Thus, promoting the good and safe practices of technological tools.
- **Make cyber risks a priority in the resilience agenda**, as the strategic cross-cutting outcome of the previous recommendations.

Cyber risks and incidents have augmented in the past decade with the increasing usage and development of internet services. Consequently, national and regional cybersecurity agencies have been set to protect us. But, let's take a step forward.

Cyber risks have been traditionally tackled by a security and law enforcement approach. Thus, leaving aside meaningful tools that adopt a whole-of-society approach when tackling risks. This is the case of **Disaster Risk Management** (DRM), that, for example, makes sure that prevention pays off and looks after the interconnection of different stakeholders.

For that reason, this brief provides an exercise for bridging together an efficient tool (DRM) with an emerging risk (cyber risks).

The Global Risk Report 2021 from the World Economic Forum rated "cybersecurity failure" the 4th of its list of clear and present dangers, according to the respondents' forecast. The increase of cyber risks and their consequent impact on different sectors of our society, as well as on our data, is creating a necessity to adopt a new approach to address and assess them.

Disaster risk management is a whole-of-society tool that aims to produce and apply policies to prevent new disaster risks while trying to strengthen resilience. This tool permits that a holistic approach can be taken for specific risks and its study. Thus, a more integrated and multisectoral response can be given to reduce vulnerabilities and risk exposure.

While this practice integrates several international standards that will be introduced further on, national and local strategies are also needed to put this into practice. This brief aims to take a local perspective and propose recommendations to the local political authorities.

Having said that, cities are having an impact internationally and are marking a new trajectory for a lively global future. Many global initiatives have provided cities with a voice and a space to network and collaborate for action, which in this case has been working towards resilience.

As many experts would agree, Barcelona has been recognized as an example of a resilient city. As a city committed to the promotion and implementation of the Agenda 2030 for Sustainable Development and the Sendai Framework of Disaster Risk Reduction, it is one of the most accurate places in the world for exemplifying this study.

Nevertheless, as the brief will show, the lack of political will and proper data collection, makes this initiative even more challenging. Yet, as the recommendations suggest, it is necessary to first build a communication channel between the stakeholders, and later address this topic within one voice. Additionally, it is also relevant that those participating as well as the rest of society, train for good and safe practices to avoid risks.

Stakeholders

International standards including the Sendai Framework for Disaster Risk Reduction state that managing risks in everybody's business. Therefore, risk management, assessment, and reduction must involve every part of our society, making it transversal and holistic. In the case of this study:

- **Local government** → Barcelona City Council, Department of Urban Resilience, Institut Municipal d'Informàtica, Agència de Ciberseguretat de Catalunya.
- **Civil-society organizations**
- **Private sector**
- **Experts and academia** → in fields of cybersecurity, disaster risk management, urban resilience.

The three main pillars

The Sustainable Development Goals reveal on its goal 11 to "*make cities and human settlements inclusive, safe, **resilient** and sustainable*". The emphasis on implementing integrated policies towards resilience of disaster at different levels of the government, such as local, makes it relevant and accurate for framing this initiative.

Additionally, the Sendai Framework for Disaster Risk Reduction from the United Nations Disaster Risk Reduction (UNDRR) was adopted the same year as the SDGs. Besides reinforcing the importance of including resilience in policies, plans, and programs at national and local levels, it established the following 4 priorities that should be considered once addressing cyber risks with DRM:

(i) Understanding disaster risk;

(ii) Strengthening disaster risk governance to manage disaster risk;

(iii) Investing in disaster reduction for resilience and;

(iv) Enhancing disaster preparedness for effective response, and to "Build Back Better" in recovery, rehabilitation and reconstruction.

The Sendai Framework mentions the better comprehension of disaster risk and its dimensions; such as the hazard's characteristics and its vulnerabilities; the importance of disaster risk governance; and the recognition and importance of the role of the stakeholders and making partnerships.

Finally, the Global Assessment Report on Disaster Risk Reduction of 2019 provides a comprehensive approach combining both the Sendai Framework and the SDGs and gives risk-updated data. This pillar is fundamental because it acknowledges that "*new risks and correlations are emerging in ways that had not been anticipated*". This assumption gives space for interpreting that new risks could be cyber risks and thus a new approach could be adapted to the current new circumstances.

These three pillars coming from international standards provide a general work frame that contributes to a better understanding of the possible interconnection between cyber risks and disaster risk management.

Disaster Risk Management and its current state

Starting with the premise that disaster risk is an indicator of poor development, the integration of disaster risk management into policies should be in line with the SDGs. Moreover, rapid urbanization, as well as population growth, have been drivers for the increase in disaster risks, namely in climate matters.

> *"Disaster risk management is the application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk, contributing to the strengthening of **resilience** and reduction of disaster losses".*

For this reason, governments, national and local, need to invest in collecting and promoting risk information; with impact statistics, databases and vulnerability information. And this means adopting the Sendai Framework and building national and local strategies.

UN Secretary General, Antonio Guterres, stated that disaster risk reduction is *one of the 10 priorities of the decade of action for the Sustainable Development Goals*. In this sense, inclusive, transversal, and multi-hazard risk assessment should be included in development policies.

He also remarks that, nevertheless, due to the lack of data collection from disaster loss, and damage statistics, there is a low participation of countries in these initiatives.

Cyber risks and cyber resilience

The increasing usage of digital tools, especially since the COVID-19 outbreak, has made us expose program information, as well as our personal data. Consequently, the lack of training and experience in cyber security has also made every level of our society more likely to experience any kind cyber threat.

Seeing how this increase in attacks is affecting not only our personal data, but is disrupting the course of work of many sectors, some solutions have been brought up. One of those being cyber resilience. A "*whole-of-society agenda that goes beyond just protecting critical information infrastructure*".

Cyber resilience "*focuses on what happens when cybersecurity measures fail, as well as when systems are disrupted by things such as human error, and power outages*". In that sense, moving from the technical part where cyber security strategies are developed by engineers and IT practitioners, cyber resilience permits other actors take part. This means that disaster risk management, which also has the strengthening of resilience as a goal, and provides a whole-in-society approach, can be adopted to address additional multi-dimensional risks such as cyber risks.

However, traditional practices approach cyber risks from a security and law enforcement, rather than with a risk mitigation perspective. Therefore, it could be difficult to identify cyber risks as an additional urban resilience feature.

The importance of mainstreaming DRM into cyber risks

According to some authors, cyber risks have not been "*approached in a fully integrated manner especially in terms of reducing potential disaster risk through comprehensive, joined up approaches*". In that sense, the characteristics that DRM offers provide a wider and holistic vision that could permit that public actors and decision-makers, such as the Urban Resilience department of any city, could consider cyber risks as a priority risk.

Integrating cyber risks and its consequent cyber resilience as part of the urban resilience strategies (determined by the usage of DRM) permits that it can benefit from the international standards mentioned above. And, related to SDG 11, contribute to making the city a safer and more resilient place.

In the end, it is an emerging risk that is increasingly affecting us personally, our institutions, and our workplaces. Addressing, integrating, and identifying cyber risks from a more transversal approach would not only permit that resilience is strengthen, but local disaster plans and responses could be more effective.

The case of Barcelona

*Barcelona in 2014 became one of the first cities in the world to create an Urban Resilience Office. Motivated by various infrastructures and services crises, the resilience work from a local basis, started with the creation of the **resilience boards** to reduce vulnerability to those risks. Furthermore, they nowadays consider natural and man-made risks that can alter the functional continuity and the provision of city services.*

The current priorities are under the Climate and Social resilience agenda. In this regard, Barcelona is very committed to the promotion and implementation of the Agenda 2030 for Sustainable Development and the Sendai Framework of Disaster Risk Reduction.

*The dynamics of how the resilient boards work is quite insightful. They are made up of **multidisciplinary** teams in which technical staff from the City Council work with non-municipal entities, both **public** and **private**. In this sense, the communication and work are **transversal** and **integral**. This **dynamism** permits that new risks can be considered if are found as a priority.*

*On the other hand, Barcelona has the **Catalan Cybersecurity Agency**, that is starting to move from its pure technical perspective and involve experts from different fields as well.*

In this sense, Barcelona is advancing in both topics, it has the infrastructure for mainstreaming DRM into cyber risks, though both fields are moving in separate directions.

Policy implications

It has been proved by DRM practitioners that **investing** in more resilient infrastructure yields $4 in benefit for each $1 invested. However, obtaining estimates of the disaster impact that cyber risks may provoke is currently a challenge.

On the one hand, traditional cyber risk management has been done through private consultancy, thus historical data is not available.

Nevertheless, one study calculated the dependency that different economic sectors have with the IT sector, proving that a cyber disruption on the former would provoke **cascading effects** on the latter. Yet, when tried to replicate the study in Barcelona, it was found that the datasets were **outdated**. Thus, the **lack of data** makes quantifying cyber risks an additional challenge.

On the other hand, and in the particular case of Barcelona, the current weak or lose communication between agencies that work towards Urban Resilience with those that work on cyber risks is another issue.

It makes that cyber risks are not considered a priority in the Urban agenda and can be tackled through DRM by the public sector.

Yet, even if external threats (lack of data and political will) in the Barcelona case show that mainstreaming DRM into cyber risks is difficult, this exercise could be replicated in another city, or even country.

In order to mitigate possible threats, the contribution of different stakeholders, mainly public and private is essential. For example, a cyber-attack could disrupt the normal functioning of the electricity, gas, and steam sector that could consequently provoke a big blackout, or scarcity of gas or steam. Therefore, a holistic and all-hazards approach would be needed in that situation, so needless duplication is avoided, and a future strategy to address this can be built. And this is what DRM could bring to cyber risks.

The final goal is to mainstream DRM into cyber risks. However, literature and data from Barcelona show that to achieve that, it is necessary to build first and create a communication channel between the different stakeholders. With that created, they could start from a common ground and later make the topic a priority.

If derived from the traditional technical language and security vision where cyber risks are approached, the language of DRM could be adapted to their study and assessment. It is relevant to advance strategies to prevent disasters. The increasing cyber threats and society's IT dependence during the last decade should shed a light on the rethinking of the most suitable and effective policies, for both local and national levels.

The brief stresses that a whole-of-society approach where different stakeholders participate in the assessment, prevention, and response to cyber risks - by implementing a DRM vision and having a proper data collection – is very meaningful as it could enhance resilience. And, as a consequence, participate in the achievement of SDG 11 and implementation of the Sendai Framework.

References

Ajuntament de Barcelona. (2016). *Barcelona. Building a Resilient City*. Retrieved December 27, 2020, from https://ajuntament.barcelona.cat/ecologiaurbana/sites/default/files/ModelResilienciaBarcelona.pdf

Centre de Seguretat de la Informació de Catalunya (CESICAT). (2019). Estratègia de Ciberseguretat de la Generalitat de Catalunya 2019-2022.

FAO. (n.d.). *Writing Effective Reports: Preparing policy briefs*. www.cde.unibe.ch/userfiles/file/NCCR_

Giddens, A. 'Risk and responsibility', *Mod. Law Rev.*, vol. 62, no. 1, pp. 1–10, 1999.

Habitat III. (2017). *New Urban Agenda* (pp. 1-66, Rep.). Quito: United Nations.

Mamello, T. (2020). *Building resilience in the time of Covid-19 and beyond*. Global Dev. https://www.globaldev.blog/blog/building-resilience-time-covid-19-and-beyond

Mclennan, M. (2021). *The Global Risks Report 2021* (16th ed.). http://wef.ch/risks2021

Mello, J. P. (2020). *Cyber resilience: What it is, why it matters—and how to get started*. TechBeacon. https://techbeacon.com/security/cyber-resilience-what-it-why-it-matters-how-get-started

Mizutori, M. (2019). Our Work. Retrieved February 14, 2021 from https://www.undrr.org/about-undrr/our-work

Smart City Hub. (n.d.). *Barcelona: showcase of smart city dynamics*. Retrieved April 18, 2021, from https://smartcityhub.com/technology-innnovation/barcelona-showcase-smart-city-dynamics/

Toregas, Costis. (2020). *COVID-19: When a health crisis drives cyber risk*. Prevention Web. https://www.preventionweb.net/experts/oped/view/71249

Toregas, Constantine, Santos, J., Jahn, M., Oemichen, W. L., Treverton, G. F., David, S. L., Rose, M. A., Brosig, M., Hutchison, W. K., Rimestad, B., & Otto, T. (n.d.). *Cybersecurity and its cascading effect on societal systems*.

UNDRR. (2020). *Bridging Cybersecurity and Disaster Risk Reduction Working Paper*. https://www.preventionweb.net/publications/view/71543

UNDRR. (2017). *Disaster risk reduction & disaster risk management*. Prevention Web. https://www.preventionweb.net/disaster-risk/concepts/drr-drm/

UNDRR. (2019a). *Global Assessment Report*. https://gar.unisdr.org

United Nations. (2015). Goal 11 of Sustainable Development. Retrieved December 27, 2020, from https://sdgs.un.org/goals/goal11

United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015 - 2030*.

Ventayol, I. (2014) '*Barcelona, resilient city: Climate change adaptation*. Presentation (March 2014)'. Barcelona

World Bank. (2020). *Disaster Risk Management Overview*. World Bank. https://www.worldbank.org/en/topic/disasterriskmanagement/overview#2

This brief proposal has been produced as the outcome and exercise of an Applied Final Degree Project. The full paper on this theme can be found in Fundació Blanquerna's repository.

The Mainstreaming of DRM into cyber risks Project is an International Relations Final Degree Project developed by student Alicia Amorós Fuster-Fabra. For more information about the project contact aliciaaf@blanquerna.url.edu

Special thanks to all experts that have participated in the data collection for this project, Luis Miguel Laguna, Genís Margarit, Ares Gabás, Costis Toregas, Sanjaya Bhatia, and Ricardo Mena.