

# Resilient infrastructures in the Anthropocene

## Abstract

Through analysis of examples in the United States and Canada and a case study on Hurricane Maria in Puerto Rico, this article explores the impacts of natural disasters on critical infrastructures, as well as the barriers and levers to create resilient infrastructures in the Anthropocene, a geological epoch in which complex interconnections and interdependencies between nature, humans, infrastructures, and digital technologies create risks to security. These harms have been little examined by green criminology that has little-explored interconnections between humans, objects-technologies, and ecosystems, as well as resilience as the development of systems' capacities to manage complex crises. While interdependencies create destructive cascades that interrupt essential flows, resilience uses digital interconnection and analyses to educate and mobilize the system through risk knowledge to reduce the impacts of future risks. Resilience requires more attention to disparities in vulnerabilities related to political and economic inequalities across space, as well as enhancing governance capacities for adaptation within a context of uncertainty.

Key-words: Resilience; critical infrastructures; risk; natural disasters; Anthropocene

## Introduction

How can we ensure the resilience of critical infrastructures given the increase in socio-technical and socio-ecological risks in the Anthropocene? This article explores the concept and practices of resilience as a way of responding to increasing threats to security during a geological epoch in which the destruction of nature by human, industrial and

technological actions intersects with the extensive digitalization of human activities. Studying resilience in the Anthropocene is embedded into an approach that considers reality as the interaction, interconnection and interdependency between human beings, nature, objects and technologies across space. This perspective is interested in the risks posed to the security of humans, ecosystems and infrastructure by the complex interconnections and interdependencies between them. This is happening within a context in which the effects of human actions on ecosystems and through technologies are creating harms to the wellbeing and survival of ecosystems, populations and objects. This includes a rise of environmental disasters, climate change, pandemics, pollution, species extinction, natural degradation, unbearable climate conditions, infrastructures' disruptions, interdependencies, cascade effects, compound events, technology dependence, and so on (Bonneuil and Fresco 2013; Autor reference; Klein 2014). Here we adopt a view of security that includes environmental security beyond a state view of it as a threat to the state (see Holley et al. 2018) and is interested in the harms resulting from the effects of human and technological actions on ecosystems.

This view of security goes beyond criminal justice and is embedded within the field of green criminology that focuses on environmental harms (Benton 2013). Since the 1990s, green criminology has enlarged the boundaries of the discipline beyond criminal justice by studying the effects of human and systemic economic activities on the survival and catastrophic collapse of ecosystems (Benton 2013) by considering a continuity between human and animal life that gives importance to animal rights and animal abuse (Beirne 2013). Attention is paid to the effects of economic exploitation and inequalities on natural degradation and the concepts of social justice and ecological justice that focus on the interaction between humans and animals and how environmental and socio-economic injustice harms both humans and animals (White 2013). Research has studied, for example,

harms produced by nations states and multinational corporations that are legal but destructive. Attention has also been paid to the unequal distribution of risks that affect and harm developing countries, minority groups and economically disadvantaged populations, generating environmental victims (White 2013). For example, Sandra Wachholz (2013) shows that women are more vulnerable than men to the impacts of climate change and their experiences, responses, and recovery from natural disasters and other risks and hazards are different. They are more vulnerable to male violence that increases in the aftermath of natural disasters, which shows that climate change has to be understood within a context of unequal power and privilege. In turn, Diane Heckenberg and Ingrid Jhonston (2012) study the differential vulnerabilities and effects of natural disasters on women, girls, boys and men. Others have studied the impacts of natural disasters on crime and social control (Nobo and Pfeffer 2012).

The effects of social climate change, inequality and environmental injustice include hunger, migration, lack of water, increasing conflicts, local environmental degradation, changing sea levels and extreme weather events (Kramer and Michalowsky 2012; White 2012). These changes threaten the survival of societies and ecosystems and take the form of an ongoing slow crisis (Agnew 2012). The study of security in this context has to do with governing these problems to create social and ecological wellbeing and mitigate and adapt to climate change (Fussey and South 2012). However, these urgent actions are blocked by a lack of meaningful action, sense of obligation and inaction (Agnew 2012). While some authors have suggested the relevance of systemic analysis and resilience response and adaptation in this context (Fussey and South, 2012), with a few exceptions (see Keiran 2015; Walklate et al. 2012), there is little discussion on resilience in criminology and on how to prepare societies and security professionals to be resilient to natural disasters. While green criminology has paid much attention to the interaction between humans, animals and

ecosystems (Beirne 2013; Beirne and South, 2013; Benton 2013), it has been less focused on the role, interactions, interconnection and interdependency with objects and technologies, including critical infrastructures. This paper first discusses the concept of resilience in the Anthropocene as a security approach that uses risk knowledge through digital technologies and networks' governance to prepare systems to mitigate the catastrophic effects of these new harmscapes (see Author reference). Second, this paper examines the cascade effects of natural disasters on critical infrastructures through different examples in the United States and Canada. Third, examples are discussed to identify barriers and levers to resilience implementation. We use a broad range of material such as policy outlines, academic literature, and journalistic research to look at the impacts of natural disasters on critical infrastructures as well as on developments in creating resilient infrastructures, focusing on examples in the United States and Canada with a focus on a case study on Hurricane Maria in Puerto Rico in 2017. This case study is based on a scoping review of the academic and grey literature on Hurricane Maria, its impacts on Puerto Rico and the response and recovery.

The United States and Canada were among the first countries to adopt the United Nations' frameworks for Disaster Risk Reduction and begin developing resilience strategies, prompted in part by increasing exposure to adverse weather conditions and hydrological disasters, particularly in coastal zones of the United States. Recent natural disasters in the US include the 2021 tornados, winter storms, wildfire season and Hurricanes Ida and Eta, the 2020 Hurricane Dorian, California wildfires in 2018 and 2020, Hurricanes Maria, Irma, and Harvey in 2017, and floods in Louisiana and West Virginia in 2016. Floods and wildfires have increased in size and number in Canada over the same period, particularly affecting the First Nations communities, including the 2011 Prairie floods, the 2013 Toronto urban flood, the 2016 Fort McMurray wildfire, the 2017 British Columbia flood and wildfire seasons, the 2018 and 2021 heatwave, wildfires and floods in British Columbia.

While disasters are often caused by interdependency and interconnection and their cascading effects, resilience uses digital interconnection and digital analyses of information to minimize the impacts of emergencies by encouraging effective coordination through sharing risk knowledge and enhancing communications systems. As an infrastructure system is a network that connects nodes, enabling the movement and circulation of flows through the system, resilience is about how the system reorganizes itself to resist multiple uncertain and possible future hazards that can not be predicted. New technologies, information technologies, and geospatial technologies are critical in this dynamic and cyclical process because they enable access, analysis, and communication of information as well as coordination of actions in the system that is the base of the reorganization process (Author reference). Technologies also aid resilience activities by providing real-time information to managers and operators and enabling analysis of information by making the network visible, identifying the hazards that threaten critical assets, and aiding assessment of adverse effects. This information provides a basis for planning activities to deal with eventual hazards. It helps determine which assets need to be strengthened to mitigate the consequences of future hazards and where redundancy and diversity are required. Redundancy is an integral part of the ecological concept of resilience. A diverse array of similar functional elements with different responses to stressors encourages continued functionality in contexts of disturbance and helps avoid cascades in critical infrastructures (Author reference).

We argue, however, that research on critical infrastructure resilience should not only focus on resilient technologies but should also pay more attention to the effects of socio-economic inequalities and governance on the capacities of societies to provide resilient critical infrastructures. The examples analyzed here show that the increased severity of disasters damages electricity and communication systems, obstructing security professionals' response and recovery activities. Enhancing the resilience capacity of societies requires

reducing vulnerabilities that go beyond digital and technical issues such as political and social-economical ones as well as improving governance capacities, including collaboration across networks, adaptation capacities including the improvisation skills of local responders, as well as the flexibility of regulation, roles, and procedures.

## 1. Resilience in the Anthropocene

### 1.1. Resilience and crisis management

In a global context of increasing occurrences of severe environmental disasters that harm populations and the built environment, the United Nations has promoted resilience as a goal of disaster risk reduction (DRR), encouraging societies to enhance their capacity to withstand environmental crisis through the 1994 Yokohama Strategy for a Safer World (United Nations 1994), the 2005 Hyogo Framework for Action (United Nations 2005), and the 2015 Sendai Framework for Disaster Risk Reduction (United Nations 2015).

The idea of resilience has emerged, rather suddenly, across several disciplines as a term capturing considerable attention. At the crux of these developments has been thinking, particularly in ecological sciences inspired by work in the material sciences of materials returning to an original state after being shifted to another -- e.g. a spring. These ideas, and the underlying metaphor of a system recovering from a shock either by returning to a previous equilibrium (the spring idea), or shifting to a new one (the concept of a tipping point that leads to a system reorganizing itself), have found considerable resonance with scholars and professionals operating within various security arenas. The source of this resonance has been an emerging sense that established harms, for which harm management processes are deeply embedded, have been joined by new and unexpected harms that have been experienced as unforeseen shocks within a context of radical uncertainty.

Ecologist Crawford S. Holling (1973) was concerned with the inability of ecological models inherited from physics to integrate external and unexpected changes to ecosystems that persist instead of disappearing. In analyzing the consequences of man's activities on lake systems, the author showed that despite the high ability of ecosystems to absorb changes, their resilience decreased when changes exceeded certain limits and the condition of the system was changed, increasing fluctuations and leading to the appearance or disappearance of entire populations. The author was less concerned with the stability of ecosystems than with their persistence in a changed configuration. He described two different behaviours, one called stability, enabling the system to return to equilibrium after a disturbance, and the other one termed resilience, in which systems persist and absorb change and disruption and maintain their relationship with populations and state variables (1973 p. 14). Holling defined resilience as the capacity of an ecosystem that has suffered an external and unexpected change to persist, absorb and be transformed by the change while maintaining its interactions with populations and state variables.

Resilience has become a way to make sense of social and ecological experiences and govern these experiences in particular ways (Grove 2018). In civil security, resilience is considered a new paradigm calling for the development of new capacities for adaptation and flexibility to improve the ability of systems to manage complex crises (Normandin et al. 2019). This capacity depends on the construction of collaborative networks focused on vulnerability mitigation, preparedness, response and recovery (Therrien et al. 2021). Resilience implementation requires coordination across systems and developing actors' capacities of adaptation and flexibility, common goals, values, interpretations, and a common language (Therrien 2010; Therrien et al. 2019). Therrien and colleagues (2021) show that local authorities and stakeholders face resilience implementation challenges. This requires

governance changes, including enhancing networks' mobilization, knowledge sharing and division of work and responsibilities among partners to manage uncertainty. One of the leading implementation challenges concerns inter-agencies coordination and collaboration between stakeholders. Resilience also requires adaptive governance and co-management to promote and evaluate adaptive capacity. This includes collecting information about systems, identifying vulnerabilities, and enhancing participatory processes involving actors at all scales and citizens' participation (Crowe et al. 2016).

## 1.2. Security in the Anthropocene

The concept of resilience is helpful to reflect on how to enhance the capacities to protect security in the Anthropocene. Integrating the social and natural sciences has become increasingly urgent to understanding the effects of human actions on the Earth and the Earth's reactions to human activities in the Anthropocene. This concept proposed by the Nobel laureate in chemistry Paul Crutzen in 2000 has not yet been officially recognized by the International Commission of Stratigraphy as being a new geological time following the Holocene, characterized by stable temperatures and sea levels. However, the concept has a broad acceptance by the natural and social sciences despite different perspectives and epistemological divides that also call for new collaboration opportunities between social and natural sciences (Brondizio et al. 2016). While Crutzen argued that the Anthropocene started with the Industrial Revolution, others state that it began with the Great Acceleration in 1945 and the large-scale burning of fossil fuels which led the planet to enter a new geological era. Stratigraphers regard the Anthropocene as a new interval in the history of geology, a turning point in rock strata that, if validated, could be considered a new geological era. In turn, earth system science sees the Anthropocene as a change in the earth system characterized by massive changes such as sea-level rise and large-scale species extinction. A third view of the



Anthropocene focuses on human impact on the planet and natural processes as a telluric force induced by urbanization, landscape changes, and resource extraction. The Anthropocene implies increasing environmental disasters, new risks, increasing temperatures and sea levels, acid seas and new sufferings (Hamilton et al. 2015). In the Anthropocene, humans' destructive force include an increase in the planet's temperature due to the emission of greenhouse gases in the atmosphere, the extinction of at least 20% of species in 2030, the acidification of oceans, the modification of the normal cycle of water due to the construction of dams, over-consumption of terrestrial biomass, and an increase in environmental crises and migrants (Bonneuil and Fressoz 2013). Other consequences are dangerous sea-level rise due to the disintegration of the West Antarctic ice sheet that could displace millions of people, extreme heatwaves, and loss of biodiversity and ecosystems. The consequences of the progressive death of the Amazon deserve particular attention because this affects rivers, ecosystems, local communities, agriculture and energy production (Klein 2014).

The Cartesian conceptualization of the rational man, whose consciousness stands from its capacity of objectifying nature as different from and dominated by man, is challenged by the advent of the Anthropocene, industrialization and its carbonification of the atmosphere, and the destructive character of human actions on the Earth (Bonneuil and Fressoz 2013).

Modern thought objectifies nature, creating a separation between nature and the human world. In consumer societies, where labour and consumption become part of the same process that enables life, nature is instrumentalized. It becomes a tool in a world where the short duration of objects and things make them lose their value and meaning (Arendt 1958).

### 1.3.Socio-ecological and socio-technical systems

As an alternative to modern ideas, the Anthropocene challenges the separation between humans and nature and leads to new conceptualizations of human beings as part of ecosystems. The concepts of a social-ecological system and a social-technical system are relevant for analyzing human and technological actions in the Anthropocene because they enable the integration of humans, nature and technologies as part of social-ecological and social-technical systems. The concept of social-ecological systems refers to how social, economic, and ecological systems are interdependent and integrated. Ecological systems provide ecosystem services to humans, enabling life, wellbeing and security. Still, human actions on ecosystems create vulnerability and insecurity and decrease ecosystems' resilience capacity and ability to provide ecosystem services (Folke et al. 2010). Ecosystems services are "flows of materials, energy, and information from natural capital stocks which combine with manufactured and human capital services to produce human welfare" (Constanza et al. 1997 p. 254).

In turn, the concept of socio-technical systems refers to the idea of how networks having institutional and material dimensions use technologies to provide social functions such as water service, transport or electricity. Socio-technical systems are networks of interrelated actors within specific institutional and technological contexts that create flows of knowledge and expertise (Geels 2004). Essential services are produced by complex socio-technical systems that adapt and emerge from the interaction between humans, technical infrastructures and social institutions of governance (Merwe et al. 2018).

#### 1.4. Resilience and critical infrastructures

Reflecting on security in the Anthropocene requires acknowledging the interconnections and interdependencies between human beings, material and digital infrastructures, and nature

across space on multiple geographical scales, as well as its resulting cascade effects in a globalized world in which there is expansion and acceleration of the movement and circulation of flows of commodities, capital, people, and information (see Brenner 1999). The consequences of the interconnectivity and interdependency of societies are evidenced in the problem of the interdependency between the different critical infrastructure sectors that makes that the disruption of one sector creates cascades on the other sectors, harming the well-being and security of human beings, physical infrastructure and nature. Critical infrastructures are living, moving, and changing socio-technical assemblages that make possible the circulation of flows of essential elements – such as water, food, electricity, information, people, and goods – that enables modern life (Amin 2014; Aradau 2010; Bridge et al. 2018). Infrastructure systems are networks that connect nodes, making the circulation of flows possible. Flows are governed through socio-technical assemblages in digital societies. The interdependent and interconnected character of societies that increasingly rely on information technologies for communication makes security governance and institutional functioning dependent on information technologies for critical infrastructure operations and the transmission of digital information, knowledge, and coordination. Protecting the flows of digital information has become a crucial part of protecting critical infrastructure. As framed by the United Nations, resilience is a goal of Disaster Risk Reduction (DRR). This approach can be regarded as an extension of the idea of a post-industrial world risk society (see Beck 2009), in which the threats to life created by industrialization must be managed through scientific knowledge and technologies. DRR, while recognizing that environmental and technological hazards are unpreventable and unpredictable, is based on the premise that all possible hazards should be assessed through technological advances – such as geospatial information technologies (GIT) – that make possible the visualization and mapping of risks to anticipate their possible effects. By analyzing the interaction of all possible hazards and the

specific vulnerabilities of a particular society, the impact of potential hazards can be minimized. Emergency managers can develop early-warning systems and implement strategies that increase resilience. DRR focuses on reducing the effects of future risks by applying principles of mitigation and prevention to reduce the impacts of past and future threats; preparedness to anticipate future events improve response – the actions taken before, during, and after an event to minimize losses and accelerate recovery – the actions taken after an event to repair damages and prevent future harms (see United Nations 2015; 2005; 1994). DDR has to do with anticipating possible scenarios resulting from future hazards to allow better planning to deal with a possible but uncertain future event.

In this context, risk analyses become central to security efforts in the Anthropocene, enabling the production of risk knowledge, actionable for security practices. Analysis of digital information allows risk anticipation, making it possible to create activities that reduce risk. Mareile Kaufmann (2016) argues that analysis of digital information about risks and emergencies gathered through technologies that make it possible to visualize and map risks, damages, losses, impacts, and responses has become a central element of resilience security practices. Combining knowledge and geospatial information technologies (GIT) makes it possible to develop geographic information systems and maps and provide location-based disaster risk information to security managers and populations at risk (Kaufmann 2016).

Building resilient infrastructures involves locating infrastructure in low-risk areas, making assets more resilient and less vulnerable to hazards, and designing systems that can continue to function even if some of their components are damaged. For critical infrastructures to be resilient, assets such as power lines, roads, bridges, buildings, and cellphone towers must be built to deal with natural hazards and cyber-risks. For example, using more resistant materials in cell phone towers, pipes, and cables could help them withstand high winds and earthquakes. Deeper foundations for water and power plants increase resilience to

earthquakes, while higher dykes increase resilience to floods. Infrastructure resilience also requires enhancing infrastructure networks to ensure the continuity of flows and services, based on criticality analysis, diversification, redundancy, and nature-based solutions. Networks must be designed to maintain their functionality despite the loss of assets. Criticality analysis can help by using digital technologies to increase risk knowledge and minimize the impacts of future risks. Such analyses make it possible to map a network, its assets and vulnerabilities, to identify possibilities for potential failures and their consequences for service continuity and vulnerable populations. Redundancy, which may involve replacing existing systems and introducing other elements in infrastructure resilience, is expensive. Still, criticality analysis helps identify the most critical parts of the network in which vulnerabilities should be reduced through redundancy in critical assets. Criticality analysis also makes it possible to map interdependencies between assets and sectors and identify where cascade effects are likely. One alternative to redundancy is diversity or the availability of different sources of resources or technologies (Hallegate et al. 2019). For instance, meshed networks with multiple supply points can be created for various nodes on the grid. This sort of diversification makes it easier to tackle different vulnerabilities, ensuring that if, for instance, one source of energy is disrupted, others can still supply the power needed.

Discussions about the resilience of critical infrastructure focus on technical and technological dimensions with less attention to governance aspects and other dimensions raised by green criminology, such as the effects of political and socio-economic inequalities on critical infrastructures or how the unequal distribution of risk impacts critical infrastructures. In the next section, we examine the cascade effects of natural disasters on critical infrastructures and how these effects are related to inequalities at the political and socio-economic levels.

## 2. The risks to critical infrastructure from environmental disasters

### 2.1. Interdependencies and cascade effects

Understanding the insecurities of the Anthropocene requires understanding the problem of interdependencies between natural, technological and social factors and the resulting cascade effects. In recent years, there has been an increase in events that combine multiple hazards or climate drivers, such as the magnification of wildfires by heatwaves, the co-occurrence of sea-level rise and tropical cyclones, or an earthquake that leads to a tsunami (Pescaroli and Alexander 2018: 2247). These compound events are characterized by unusual combinations of complex causal chains exacerbated by climate change and human activity, making them difficult to predict and respond to (Zscheischler et al. 2018). Compound events can create cascading risks with social and technical implications as environmental hazards interact with vulnerabilities at the physical, social, and critical infrastructure levels, magnifying the consequences of events. Climate change is causing unexpected events, such as floods following heavy and unexpected rain or the combination of rain and melting snow. The severe floods in 2017 in British Columbia, for example, were caused by a frigid and dry winter, followed by heavy rains in the spring. The 2018 Camp Fire in California, which lasted 17 days, covering 153,000 acres and causing 85 fatalities, \$16.5 billion in damages, and the destruction of almost 19,000 structures, including 95% of the buildings in the towns of Paradise and Concow, was caused by a combination of technical and natural factors, including a faulty electric transmission line that was the origin of the fire, an intense drought the previous fall, heavy grass after a wet spring, and high, dry, hot winds that reduced humidity and increased the spread of the fire (Californian Department of Forestry and Fire Protection 2018). Alberta's Fort McMurray wildfire, among the costliest disasters in

Canadian history (\$37 billion), lasted from May to mid-June 2016 and destroyed 1,500,000 acres of forestland and 2,600 structures, forcing the evacuation of 88,000. The fire was influenced by increasing temperatures, hot and dry air, low humidity, high winds, and a dry fall and winter followed by a warm spring (Hayward 2016).

Thus, environmental disasters are related to the interaction and interdependency between natural, physical, technological, and human factors, harming assets, creating cascades, and interrupting essential flows. There are different kinds of interdependencies, such as physical, cyber, and geographic. The increasing use of information technologies and computer systems has created complex cyber-interdependencies (Leavitt and Kiefer 2006), while the intersection between natural and technological or human triggers can create cascade effects that lead to catastrophic damage from fires, floods, and landslides. Natural hazards such as earthquakes, floods, or hurricanes can cause industrial accidents or interrupt electricity, transport, and telecommunications services. For example, the 2011 9.0 magnitude earthquake in Japan that killed 28,000 people was followed by aftershocks that caused a tsunami that flooded land and destroyed infrastructures such as roads, buildings, ports, and railways, not only impeding evacuation and relief but leading to the destruction of a nuclear power plant (Kadri et al. 2014).

## 2.2. Exemples of cascade effects in Canada and the United States

The following examples show different problems related to the cascade effects of natural disasters on critical infrastructures, mainly: The level of destructive impact natural disasters can have on critical infrastructures on which human life depend; the cascade effects generated by critical infrastructure dependence on electricity; and how the impacts of natural disasters on information systems disrupt response efforts.

The 1998 North American ice storm is a relevant example of the cascade effects on other sectors from the destruction of electric powerlines. The ice storm involved simultaneous storms in Ontario, Quebec, New Brunswick, Nova Scotia, Northern New York, and Maine. The storms lasted for more than 80 hours, generating a landscape of icy trees, icy cars, melted transmission towers, and fallen power lines. More than 1,000 transmission towers and 35,000 wooden utility poles were damaged, causing power outages that left four million people without electricity and water (Gazette 1998). Bridges and tunnels had to be closed because of ice on the roads and falling ice chunks. 80% of the trees in Montreal were damaged. Although Montreal's power lines had been designed according to strict standards that mandated the use of high-quality materials, this was not sufficient to prevent their collapse in the face of unexpected environmental conditions. Twenty-five people died of hypothermia and 12 drowned (Environment and Climate Change Canada 2017). Indirect deaths were caused by carbon monoxide from generators.

The case of Hurricane Katrina, which devastated New Orleans on August 28, 2005, showed the level of dependence on digital information and technological communication systems, highlighting the need to avoid digital dependency in managing emergencies and improving flexibility. New Orleans' communications system, including central offices, communication company facilities, radio stations, cell towers, and its 911 system, was destroyed, impeding the coordination of emergency response operations. Public agencies are dependent on digital information and communication between agencies. Without information about incident response, authorities were guided by rumours and speculation, eroding confidence in public institutions. Some argue that security professionals had failed to recognize infrastructure interdependencies (Leavitt and Kiefer 2006) and the need to create redundancy in critical nodes of the communications network (Miller 2005), which shows problems in resilience implementation, but also to what extent it is difficult to implement



resilience efforts that are based on information sharing and coordination practices in the context of unexpected and destructive disasters.

### 1.3. Infrastructure maintenance, vulnerabilities and social inequality: The case of Maria in Puerto Rico

Other problems are related to poor infrastructure maintenance, which reveals inequalities in societies' capacities to guarantee resilient infrastructures. The increasing number and scale of natural disasters in the past three decades relative to the past 100 years has affected every country, particularly developing countries in Africa, Asia, and Latin America (Mijalković and Cvetković 2013). For these countries, problems with infrastructure maintenance magnify the consequences of disasters. The differential distribution of vulnerabilities and risks related to differential exposure to hazards and differences in the capacities of societies to create resilient infrastructures has not received sufficient attention. Recent discussions about the resilience of critical infrastructures have shown the differential impact of different types of hazards on different infrastructures (see Hallegate et al. 2019). Still, there has been little discussion about the effects of the unequal distribution of risks and vulnerabilities on the resilience of critical infrastructures.

The category 4 Hurricane Maria that devastated Puerto Rico on September 20, 2017, is a relevant case study for the analysis of risks and vulnerabilities that shows how political and socio-economic inequalities impeded Puerto Rico from developing proper infrastructures able to resist the magnitude of the impact of the disaster. Since the 1950s, the island, an unincorporated territory of the United States, has adopted an economic model based on industrial manufacturing where tax breaks are offered to foreign companies to attract private investment. Despite implementing austerity and restructuring measures, a lack of government

spending power caused an unresolved fiscal crisis and made it challenging to fund the required investments in infrastructure modernization and maintenance. The island's public debt is now over 100% of its Gross National Product of \$72 billion (Quiñones-Pérez and Seda-Irizarry, 2016). Puerto Rico's power grid is managed by a public utility, Puerto Rico Electric Power Authority (PREPA), which has increasingly borrowed money from the municipal bond market without meeting its fiduciary obligations, leading to a reduction in maintenance activities and failure to renew its ageing infrastructure (Kim Park and Samples 2017). When Hurricane Maria hit, 60% of the system was 50 years old and 30% was composed of low-efficiency elements (Kwasinski et al. 2019). This socio-technical vulnerability related to the socio-economic and political vulnerabilities of the island intersects with its socio-ecological vulnerabilities and with the increasing risk of hurricane intensity, constraining its resilience capacities. Maria was part of the highly active Atlantic hurricane season of 2017, one of the most intense seasons on record that included 17 named storms and 10 hurricanes, 6 of which were severe (Klotzbach et al. 2018). The frequency and intensity of tropical cyclones in the Atlantic have increased since 1995 due to changing environmental conditions caused by global warming, making wind speed and rainfall more intense and hurricanes more destructive (Knutson et al. 2010; Van Aalst 2006). Small Caribbean islands are particularly vulnerable to hurricanes due to their topography and their location in the path of ocean corridors. Their remote location also complicates emergency response activities, which are further limited by low levels of natural and economic resources (Shultz et al. 2019). In Puerto Rico's case, the island's geography makes it vulnerable to landslides, increasing the vulnerability of electric towers and transmission lines. The heavy rain and winds that were part of Hurricane Maria crossed the island from the southeast to the northwest, causing floods, over 400,000 landslides, and the destruction of houses, roads, and

critical infrastructures, overwhelming the capacities of local authorities to respond to the disaster.

The case of Puerto Rico also shows to what point electricity disruption cause cascades on other infrastructure sectors. The problem of communications disruption also occurred in the case of the response to Hurricane Maria in Puerto Rico, where the devastation of the power system led to a total collapse of critical infrastructure that lasted for months. The cascade effects of a lack of electricity on the water, health, and telecommunications networks caused deaths, suffering, and distress. The population had to cope for months without water or power, unable to refrigerate food or communicate with family members. Schools were closed. Due to access problems and delays in FEMA's recovery efforts, Damaged homes remained without roofs. The first official death toll was 64; by August 2018, the official estimate was 2,975 (Cange and McGaw-Césaire 2019). According to an independent study conducted by Kishore and colleagues (Kishore et al. 2018) using a stratified community-based sample to estimate mortality causes, many deaths were caused by interrupted or delayed access to medical services. Access to medications was impeded, and equipment requiring electricity, such as ventilators or dialysis machines, was unavailable (Alcorn 2017). This demonstrates a lack of consideration for redundancy and diversity of equipment in resilience infrastructure efforts.

Electricity disruption also caused water service interruption. Puerto Rico's aqueduct and sewer authority, the *Autoridad de Acueductos y Alcantarillados*, had problems restoring service due to the lack of electricity and difficulty in accessing equipment because of fallen trees and powerlines. The largest water facility in the west at Anasco River had flooded and access was obstructed by debris. Plants had to wait months to obtain the electric generators needed to get water treatment plants functioning (Harmsem 2018). 83% of households in

remote areas experienced a loss of electricity, water, and cell phones for long periods. Damage to the telecommunications system was difficult to repair, mainly due to downed cellular communication towers, which prevented the use of cell phones for months – 95.2% of cell sites were out of service and were restored only gradually over the six months following the hurricane (Public Safety and Homeland Security Bureau 2018). Damage to electrical transmission and distribution infrastructures was severe. Puerto Rico had 2,478 miles of transmission lines with a small number of underground lines and 55 miles of submarine cable. Many transmission lines were in overgrown mountainous areas, and only 15% had been designed to be resistant to wind. Almost all the transmission lines in the eastern part of the island were severely damaged. 847 transmission structures collapsed, and at least 10% of poles were damaged because they had been installed in holes that were too shallow (Alcorn 2017).

The case of Puerto Rico also shows inequities in response and recovery processes relative to political and regulatory barriers. Unlike recovery processes in New Jersey and New York after Hurricane Sandy, where greater available access to technicians and technologies made it possible to restore electricity after a few days, the recovery process in Puerto Rico was prolonged: 90% of the territory was without power one month after the storm, 50% were without electricity two months after the hurricane, and 20% were still without power after 6 months (Harmsem 2018). This shows inequities in response and recovery infrastructure efforts across space with longer restoration times in remote areas. Beyond the delay caused by the remote location of the island, legal and political constraints related to restrictions in contracting and shipping and the country's debt situation limited the availability of outside assistance and led to a lack of sufficient material, particularly mobile transformers and diesel generators to power larger utilities and small gasoline and diesel back-up generators to provide electricity to homes (Kwasinski et al. 2019). The case of

Puerto Rico shows how differences in the response were influenced by the unequal political relation of the United States to the island by contrast with other continental states and how this relation is reinforced by the island's economic domination and lack of economic development opportunities. The same legal constraints that maintain the economic hegemony of the US over Puerto Rico and have historically impeded its economic independence and development hindered the response effort. This shows a need for legal flexibility to support resilience. In such a context of total devastation of the critical infrastructure system and the built environment, humanitarian needs should prevail over legal and fiscal considerations and legal restrictions to receive humanitarian aid should be lifted. Furthermore, international cooperation and funding are required for response and recovery efforts and critical infrastructure maintenance as part of the preparedness and mitigation efforts of small islands and developing countries vulnerable to natural disasters.

### 3. Barriers and levers to the resilience of critical infrastructure

As the Puerto Rican case shows, creating resilient infrastructure in risk areas and reducing vulnerabilities through investments in the maintenance and renewal of infrastructures is an unequal endeavour and is related to political and economic inequities that require a change of mentality, adaptation and flexibility to be able to prioritize humanitarian needs over political and economic concerns. However, problems in critical infrastructure maintenance are not only related to economic inequities. A significant barrier to critical infrastructure resilience is negligence in ensuring proper infrastructure maintenance, which can be considered a governance problem requiring networks' education, surveillance and enforcement. This requires that the population and utilities cooperate with security measures, maintenance practices, and risk reduction initiatives. For instance, in the case of the

California Camp Fire, the burn zone had been previously identified on a fire map drawn up by Cal-Fire and Pacific Gas and Electric (PG&E) as at either elevated or extreme risk. PG&E, however, neither implemented mitigation measures nor carried out the necessary maintenance on its infrastructure. Thus, resilience discussions need to evaluate their implementation's political, economic, and institutional contexts.

Another barrier to critical infrastructure resilience is given by the limits of digital technologies and analyses in predicting the weather in the context of climate change, which impacts the decisions of security managers. For example, the 2017 flooding in British Columbia was caused by a freezing and dry winter, followed by heavy rains in the spring. Climate change makes such events very difficult to predict, limiting the ability of digital technologies and analyses to provide accurate information and creating problems for security professionals and communities. The security professionals who, working with available data, including weather predictions and water surveys, decided to increase outflow tried to balance the quantity of water maintained in the lakes to prevent a flood without altering the ecosystems that depend on water from the lakes. However, this increase, combined with unexpected rain and melting snow that exceeded weather predictions resulted in floods in the Thompson Okanagan (Government of British Columbia 2018).

Another barrier to resilience implementation is a lack of flexibility in regulation. The Anthropocene has brought an increase in the number and scope of disasters whose outcomes are impossible to predict (Boin and McConnell 2007), requiring security managers to demonstrate increased flexibility and the ability to improvise. This need for flexibility was apparent in the response and recovery efforts in the 2017 wildfire season in British Columbia. Cell phone towers burned, highways were closed, and electricity was cut off, affecting response and recovery. An evacuation order could not be issued because such an order

required consultation between the city council and the chief security manager, which had become impossible. This situation shows that this regulation is not adapted to the new harmscapes of the Anthropocene, where the severity of disasters' impacts disrupts communications. This example also indicates that the context of severity and unpredictability of disasters in the Anthropocene requires adaptation capacities that include developing sensemaking and adaptation skills by security responders. As the expansion of the fire was devastating and given the absence of a clear emergency plan, security managers had to adopt flexible alternatives on the fly and, recognizing the importance of mobile communications for emergency responders, decided to focus on protecting critical infrastructure such as the remaining transmission lines and cell phone towers (Government of British Columbia 2018). Developing sensemaking as part of adaptation capacities to improve decision-making is a critical lever to critical infrastructure resilience. Research on sensemaking shows that organizations undertake socio-cognitive activities in contexts of unexpected events. Specific representations of the situation enable common understandings, influenced by culture, values, attitudes, and the construction of narratives that help interpret the situation (Leedom 2003).

Another feature highlighted by the examples above is that emergency plans are becoming obsolete in such contexts of devastation and uncertainty. In Puerto Rico, authorities and those responsible for different critical infrastructure sectors had emergency plans, but these had not been developed to deal with the degree of destruction caused by Hurricane Maria. In this case, improvisation had to take place within a context of total devastation. For example, radio broadcasters adapted their practices and began to share information about their neighbourhoods, using the few cell phones available. They also had to learn new technical skills, such as operating a generator – it is not by chance that the only radio station operating after the hurricane was owned by broadcasters with a background in engineering. Radio broadcasters also had to redefine their roles, adapting their practices to the

context, having to struggle to get gas and being among the first to bring help and aid to communities, answering questions, and providing information while also learning to manage exhaustion and keeping professionalism in a context in which they had to inform about a disaster that they were also living (Nieves-Pizarro et al. 2019). Interestingly, this example shows the role of technical skills on adaptation capacities and the importance of values and the representations these journalists had of their professional role and identities. This capacity to redefine their role and practices to help the population, in turn, influenced their decisions and their ability to remain professional.

The development of adaptation and improvisation capacities also requires networks' mobilization and collaboration across public, private and third sectors for response and recovery activities to share resources. As shown by Therrien and colleagues, resilience is about networks' capacities of adaptation and flexibility to manage a complex crisis (Normandin et al. 2019; Therrien et al. 2021), which requires collaboration, coordination, as well as shared goals, language, values, and interpretations (Therrien 2010; Therrien et al. 2019). This requires governance changes for networks' mobilization, knowledge sharing and division of work and responsibilities among partners to manage uncertainty (Therrien et al. 2021). Adaptive governance needs to enhance the participatory processes of actors at all scales (Crowe et al. 2016). The recovery of the power system and the wireless network in Puerto Rico provides another example of improvisation in a context where equipment was unavailable. Reaccessing the power system and wireless network required improvisation, such as using system interconnections to share power from plants that still had some capacity or linking towers and equipment from different communication companies. "Creative improvisation," or the spontaneous creation of solutions and new forms of mutual assistance, resulted from collaboration and cooperation between infrastructure operators, NGOs, and the private sector (Lugo 2019). Attractive solutions use existing networks or create new ones to



make companies or organizations cooperate. For example, the NGO NetHope used its network to assist federal and local governments and the private sector, mobilizing teams of responders to help transport equipment (Lugo 2019).

## Conclusion

Green criminology provides a new lens to the study of security within the discipline by focusing on the catastrophic harms of human activities on ecosystems. It considers the interdependencies between human and animal life, as well as socio-economic and socio-ecological injustices. This paper extended the analysis to harms produced by the interdependency between environmental risks, human activities, and critical infrastructure in the Anthropocene, when natural disasters have become more frequent, severe, and unpredictable in a context of unequal distribution of risks and socio-economic inequalities. No matter how far critical infrastructures can appear from the boundaries of the discipline, their inclusion in the analysis of environmental harms is increasingly relevant. This analysis shows how in the context of climate change, multiple climate hazards interact with critical infrastructures vulnerabilities and social inequalities to produce disasters. As the combination of climate hazards magnifies the impacts of storms on electricity infrastructures and communication systems, the cascades generated by the dependency on the power system by the other infrastructure sectors such as health, communications, and water systems, magnifies the consequences of disasters and disrupts response activities. The case of Hurricane Maria in Puerto Rico illustrates the unequal distribution of risks. The location and topography of small islands such as Puerto Rico make them more vulnerable to the intensity of the storms powered by increasing sea temperatures, sea levels and a combination of climate drivers. The island's vulnerability is also due to its old and poorly maintained power infrastructure. This is

related to the lack of Puerto Rico's financial capacity to invest in resilient infrastructures due to its fiscal problems that follow a history of political, economic, and racial domination and dependency from the United States. This case study also shows inequities in crisis response and recovery activities caused by political, economic, and racial elements and how inadequate regulatory measures block response and recovery activities.

Considering the unequal distribution of risks and socio-economic and racial inequalities is relevant when reflecting on the resilience of critical infrastructures. Resilience requires addressing these inequities to ensure adaptation, mitigation, response, and recovery capacities based on equity. This includes regulatory flexibility and international cooperation and funding to enable small islands and developing countries that are more vulnerable to environmental risks to invest in the renewal and maintenance of critical infrastructures, which are essential to mitigate the impacts of future disasters. A change of mentality is needed to put humanitarian needs over political and economic considerations. This implies orienting actions toward the common goal of saving lives, which requires redefining values, meanings, and building a common language, while questioning the imbalances of power among countries, nations and ethnic groups that orient priorities and political decisions. While much attention is given to resilient technologies and to the role of digital and geographic information technologies and analyses in predicting and mitigating risks, this paper shows the limits of depending on these technologies in the context of climate change and the destructive impact of disasters on information systems and other critical infrastructures. Many of the problems deriving from resilience implementation are not only technological, but are also related to governance issues. The development of resilient infrastructures and societies is limited by governance barriers such as lack of legal flexibility and proper infrastructure maintenance. Addressing these problems requires governance solutions. This paper shows that the levers to the resilience of critical infrastructures can only be found through the

mobilization of networks of public-private and third sector actors based on collaboration, cooperation, knowledge-sharing and resource-pooling. This involves developing adaptation, improvisation and sensemaking capacities that harness common values, narratives and interpretations that place the wellbeing of populations at risk at the centre of all decision-making.

#### Funding

This work was supported by the Social Sciences and Humanities Research Council of Canada. [grant number 957376]

All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

## References

- Agnew, R. (2012). It's the end of the world as we know it : The advance of climate change from a criminological perspective. In R. White (Ed.), *Climate change from a criminological perspective* (p. 13-26). New York: Springer.
- Alcorn, T. (2017). Puerto Rico's Health System after Hurricane Maria. Hurricane Maria has Put Pressure on Puerto Rico's Health-care System, but a Looming Budgetary Shortfall Could be Even More Devastating. (No. 390). Ted Alcorn Reports.
- Amin, A. (2014). Lively Infrastructure. *Theory, Culture & Society*, 31, 137–161.
- Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, 41, 491–514.
- Beck, U. (2009). *World at Risk*. Cambridge: Polity.
- Beirne, P. (2013). Animal rights, animal abuse and green criminology. In P. Beirne & N. South (Eds.), *Issues in green criminology. Confronting harms against environments, humanity and other animals* (p. 55-86). New York: Routledge.
- Beirne, P., & South, N. (2013). Introduction : Approaching green criminology. In P. Beirne & N. South (Eds.), *Issues in green criminology. Confronting harms against environment, humanity and other animals* (p. xiii). New York: Routledge.
- Benton, T. (2013). Ecology, community and justice : The meaning of green. In P. Beirne & N. South (Eds.), *Issues in green criminology. Confronting harms against environment, humanity and other animals* (p. 3-31). New York: Routledge.

- Blaustein, J., Chodor, T. & Pino, N.W. (2020). Making Crime a Sustainable Development Issue: From ‘Drugs and Thugs’ to ‘Peaceful and Inclusive Societies.’ *British Journal of Criminology* 60, 50–73.
- Boin, A. & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*, 15, 50–60.
- Bonneuil, C. & Fressoz, J.-B. (2013). *L’événement Anthropocène. La terre, l’histoire et nous*. Lonrai: Édition du Seuil.
- Brenner, N. (1999). Globalization as Territorialization: The Re-scaling of Urban Governance in the European Union. *Urban Studies*, 36, 431–451.
- Bridge, G., Özkaynak, B. & Turhan, E. (2018). Energy Infrastructure and the Fate of the Nation: Introduction to Special Issue. *Energy and Social Science*, 41, 1–11.
- Brondizio, E. S., O’Brien, K., Bai, X., Biermann, F., Steffen, W., Berkhout, F., Cudennec, C., Lemos, M. C., Wolfe, A., & Palma-Oliveira, J. (2016). Re-conceptualizing the Anthropocene : A call for collaboration. *Global Environmental Change*, 39, 318-327.
- Californian Department of Forestry and Fire Protection. (2018). Informational Summary Report of Serious or Near Serious CAL FIRE Injuries, Illnesses and Accidents (Summary No. 18- CA- BTU- 016737). Californian Department of Forestry and Fire Protection, California Northern Region.
- Cange, C.W. & McGaw-Césaire, J. (2019). Long-Term Public Health Responses in High-Impact Weather Events: Hurricane Maria and Puerto Rico as a Case Study. *Disaster Medicine and Public Health Preparedness*, 14, 18–22.
- Coden, M. & Bartol, N. (2017). Our Critical Infrastructure is More Vulnerable than Ever. It Doesn’t Have to Be That Way. World Economic Forum. URL

<https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/> (accessed 11.4.19).

Crowe, P. R., Foley, K., & Collier, M. J. (2016). Operationalizing urban resilience through a framework for adaptive co-management and design : Five experiments in urban planning practice and policy. *Environmental Science & Policy*, 62, 112-119.

Department of Defense. (2015). National Security Implications of Climate-Related Risks and a Changing Climate. United States: Department of Defense.

Environment and Climate Change Canada. (2017). Ice Storm of the Century. URL <http://www.ec.gc.ca/meteo-weather/default.asp?lang=En&n=3DED7A35-1#t1>

.

Fussey, P., & South, N. (2012). Heading toward a new criminogenic climate : Climate change, political economy and environmental security. In R. White (Ed.), *Climate change from a criminological perspective* (p. 27-40). New York: Springer.

The Gazette. (1998). The ice storm of 1998.

Government of British Columbia. (2018). Addressing the New Normal: 21st Century Disaster Management in British Columbia. British Columbia: Government of British Columbia.

Goyes, D.R. & Sollund, R. (2018). Animal Abuse, Biotechnology and Species Justice. *Theoretical Criminology*, 22, 363–383.

Hallegate, S., Rentschler, J. & Rozenberg, J. (2019). Lifelines. The Resilience Infrastructure Opportunity. Washington: World Bank Group.

Hamilton, C., Bonneuil, C., & Gemenne, F. (2015). The Anthropocene and the global environmental crisis. London: Routledge.

- Harmsem, E. (2018). CRISP 2.0 Type 2: Collaborative Research: Integrated Socio-Technical Modeling Framework to Evaluate and Enhance Resiliency in Islanded Communities (ERIC).
- Hayward, J. (2016). Fort McMurray Wildfire “Likely” Result of Human Activity: RCMP. CTV News.
- Heckenberg, D. & Jhonston, I. (2012). Climate change, gender and natural disasters : Social differences and environmental-related victimization. In R. White (Ed.), *Climate change from a criminological perspective* (p. 149-172). New York: Springer.
- Holling, C.S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4, 1–23.
- Joseph, J. (2017). Resilience, Governmentality and Neoliberalism. In D. Chandler & J. Coaffee (Eds.), *The Routledge Handbook of International Resilience*. London and New York: Routledge, Taylor & Francis, pp. 159–168.
- Kadri, F., Birregah, B. & Châtelet, E. (2014). The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study. *Homeland Security & Emergency Management*, 11, 217–241.
- Kaufmann, M. (2016). The Digitization of Resilience. In D. Chandler & J. Coaffe (Eds.), *The Routledge Handbook of International Resilience*. London and New York: Routledge, pp. 106–118.
- Keiran, H. (2015). Resilience in UK Counter-terrorism. *Theoretical Criminology*, 19, 77–94.
- Kim Park, S. & Samples, T.R., 2017. Puerto Rico’s Debt Dilemma and Pathways Toward Sovereign Solvency. *American Business Law Journal* 54, 9–60.
- Kishore, N., Marques, D., Mahmud, A., Kiang, M.V., Rodriguez, I., Fuller, A., Ebner, P., Sorensen, C., Racy, F., Lemery, J., Maas, L., Leaning, J., Irizarry, R.A., Balsari, S., &

- O. Buckee, C. (2018). Mortality in Puerto Rico after Hurricane Maria. *The New England Journal of Medicine*, 379, 162–170.
- Klein, N. (2014). *This Changes Everything: Capitalism VS. the Climate*. New York: Simon & Schuster.
- Klotzbach, P.J., Schreck, C.J., Collins, J.M., Bell, M.M., Blake, E.S., Roache, D. (2018). The Extremely Active 2017 North Atlantic Hurricane Season. *Monthly Weather Review*, 146, 3425–3443.
- Knutson, T.R., McBride, J.L., Chan, J., Emanuel, K., Holland, G., Landsea, C., Held, I., Kossin, J.P., Srivastava, A.K. & Sugi, M. (2010). Tropical Cyclones and Climate Change. *Nature Geoscience*, 3, 157–163.
- Kramer, R. C., & Michalowsky, R. J. (2012). Is global warming a state corporate crime? In R. White (Ed.), *Climate change from a criminological perspective* (pp. 71-88). New York: Springer.
- Kröger, W. (2017). Securing the Operation of Socially Critical Systems from an Engineering Perspective: New Challenges, Enhanced Tools and Novel Concepts. *European Journal of Security Research*, 1–17. doi:10.1007/s41125-017-0013-9
- Kwasinski, A., Andrade, F., Castro-Sitiriche, M.J. & O'Neill-Carrilo, E. (2019). Hurricane Maria Effects on Puerto Rico Electric Power Infrastructure. *IEEE Power and Energy Technology Systems Journal*, 6, 85–94.
- Lavelle, M. (2012). Can Hurricane Sandy Shed Light on Curbing Power Outages? *National Geographic*.
- Leavitt, W.M. & Kiefer, J.J. (2006). Infrastructure Interdependency and the Creation of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans. *Public Works Management & Policy*, 10, 306–314.



- Leedom, D. K. (2003, June). Functional analysis of the next generation common operating picture. In Proceedings of the 8th annual International Command and Control Research and Technology Symposium.
- Lugo, A.E. (2019). Recovery and Long-Term Effects. In A. E. Lugo (Ed.), *Social-Ecological-Technological Effects of Hurricane María on Puerto Rico*. San Juan: Springer, Cham, pp. 19–28.
- Mijalković, S. & Cvetković, V. (2013). Vulnerability of Critical Infrastructure by Natural Disasters. *The Academy of Criminalistic and Police Studies*, 91–102.
- Miller, R. (2005). *Hurricane Katrina: Communications & Infrastructure Impacts*. National Defense Univ Fort McNair DC.
- Natali, L. & De Nardin Budo, M. (2019). A sensory and visual approach for comprehending environmental victimization by the asbestos industry in Casale Monferrato. *European Journal of Criminology*, 16, 708–727.
- National Academies of Sciences, Engineering, and Medicine. (2018). Recoverability as a First-Class Security Objective: Proceedings of a Workshop. Washington DC: National Academies of Sciences, Engineering, and Medicine.
- Nguyen, L. (2011). Historic Prairie Flooding, Top Weather Story of 2011. *Postmedia News*.
- Nieves-Pizarro, Y., Takahashi, B. & Chavez, M. (2019). When Everything Else Fails: Radio Journalism During Hurricane Maria in Puerto Rico. *Journalism Practice*, 13, 799–816.
- Nobo, C. C., & Pfeffer, R. D. (2012). Natural disasters and crime: Criminological lessons from Hurricane Katrina. In R. White (Ed.), *Climate change from a criminological perspective* (p. 173-184). New York: Springer.
- Normandin, J.-M., Therrien, M.-C., Pelling, M., & Paterson, S. (2019). The definition of urban resilience : A transformation path towards collaborative urban risk governance.

In G. Brunetta; C. Ombretta; Tollin, N. Rosas-Casals, M. & J. Morato (Eds.), *Urban resilience for risk and adaptation governance* (p. 9-25). Springer.

O'Malley, P. (2010). Resilient Subjects: Uncertainty, Warfare and Liberalism. *Economy and Society*, 39, 488–509.

O'Malley, P. (1992). Risk, Power and Crime Prevention. *Economy and Society*, 21, 252–275.

Pescaroli, G. & Alexander, D. (2018). Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. *Risk Analysis*, 38, 2245–2257.

Public Safety and Homeland Security Bureau. (2018). 2017 Atlantic Hurricane Season Impact on Communications Report and Recommendations. Public Safety and Homeland Security Bureau. Federal Communications Commission.

Quiñones-Pérez, A. & Seda-Irizarry, I.J. (2016). Wealth Extraction, Governmental Servitude, and Social Disintegration in Colonial Puerto Rico. *Colonial Puerto Rico*, 90-98.

Shultz, J.M., Kossin, J.P., Shepherd, J.M., Ransdell, J.M., Walshe, R., Kelman, I. & Galea, S. (2019). Risks, Health Consequences, and Response Challenges for Small-Island-Based Populations: Observations From the 2017 Atlantic Hurricane Season. *Disaster Medicine and Public Health Preparedness*, 13, 5–17.

Simon, J. (1988). The Ideological Effects of Actuarial Practices. *Law & Society Review*, 771, 771–800.

Therrien, M.-C. (2010). Stratégies de résilience et infrastructures essentielles. *Télescope*, 16(2), 154-171.

Therrien, M.-C., Jutras, M., & Usher, S. (2019). Including quality in Social network analysis to foster dialogue in urban resilience and adaptation policies. *Environmental Science & Policy*, 93, 1-10.

- Therrien, M.-C., Normandin, J.-M., Paterson, S., & Pelling, M. (2021). Mapping and weaving for urban resilience implementation : A tale of two cities. *Cities*, 108, 102931.
- Thoma, K., Schart, B., Hiller, D. & Leisman, T., 2016. Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches. *European Journal of Security Research*, 1, 3–19.
- United Nations. (2015). Sendai Framework for Disaster Risk Reduction 2015 - 2030. Sendai: United Nations.
- United Nations. (2005). Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters. United Nations. Hyogo: International Strategy for Disaster Reduction.
- United Nations. (1994). Yokohama Strategy for a Safer World. Guidelines for Natural Disaster, Prevention, Preparedness and Mitigation. Yokohama: United Nations.
- Van Aalst, M. (2006). The impacts of climate change on the risk of natural disasters. *Disasters*. <https://doi.org/10.1111/j.1467-9523.2006.00303.x>
- Wachholz, S. (2013). « At risk » : Climate change and its bearing on women's vulnerability to male violence. In P. Beirne & N. South (Eds.), *Issues in green criminology. Confronting harms against environments, humanity and other animals* (p. 161-185). New York: Routledge.
- Walklate, S., Mythen, G. & McGarry, R. (2012). States of resilience and the resilient state. *Current Issues in Criminal Justice*, 24, 185–204.
- Welsh, M. (2014). Resilience and responsibility: governing uncertainty in a complex world. *The Geographical Journal*, 180, 15–26.

- White, R. (2012). The criminology of climate change. In R. White (Ed.), *Climate change from a criminological perspective* (p. 1-11). New York: Springer.
- White, R. (2013). Green criminology and the pursuit of social and ecological justice. In P. Beirne & N. South (Eds.), *Issues in green criminology. Confronting harms against environments, humanity and other animals* (p. 32-54). New York: Routledge.
- World Economic Forum. (2019). *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*. Geneva: World Economic Forum.
- Zscheischler, J., Westra, S., van den Hurk, B.J.J.M., Seneviratne, S.I., Ward, P.J., Pitman, A., AghaKouchak, A., Bresch, D.N., Leonard, M., Wahl, T. & Zhang, X. (2018). Future Climate Risk from Compound Events. *Nature Climate Change*, 8, 469–477.