MAKING CRITICAL INFRASTRUCTURE RESILIENT

UNDRR
UN Office for Disaster Risk Reduction

ENSURING CONTINUITY OF SERVICE
POLICY AND REGULATIONS IN EUROPE AND CENTRAL ASIA

SENDAI FRAMEWORK
FOR DISASTER RISK REDUCTION 2015-2030

SUSTAINABLE DEVELOPMENT GOALS

MAKING CRITICAL INFRASTRUCTURE RESILIENT

ENSURING CONTINUITY OF SERVICE
POLICY AND REGULATIONS IN EUROPE AND CENTRAL ASIA

The United Nations Office for Disaster Risk Reduction works towards the substantial reduction of disaster risk and losses to ensure a sustainable future. UNDRR supports the implementation of the Sendai Framework for Disaster Risk Reduction 2015-2030, which sets out a people-centred approach towards achieving a substantial reduction in disaster losses from man-made and natural hazards and a shift in emphasis from disaster management to disaster risk management. The Regional Office for Europe covers 55 countries and works with countries and stakeholders to reduce disaster risk in Europe and Central Asia.

The lead authors of this report are **Abhilash Panda** and **Nicholas J Ramos** (UNDRR) with **Aleksandrina Mavrodieva** (Consultant).

Graphic Design: Giulio Nocera // giulionocera91@gmail.com

For more information about the report, please contact:

United Nations Office for Disaster Risk Reduction
Regional Office for Europe
E-mail isdr-europe@un.org
Website https://www.undrr.org/about-undrr-where-we-work/europe

resilient infrastructure

CONTENTS

Calin Stan/Shutterstock.com

PREFACE

The COVID-19 pandemic has demonstrated the consequences of systematically underinvesting in resilience. The cascading nature of disaster risk, where one disaster can rapidly lead to another, coupled with insufficient investment in disaster risk reduction, makes the critical systems that trade, food, energy, transportation and health rely on increasingly vulnerable to hazards such as COVID-19.

However, the crisis is a wake-up call and an unprecedented opportunity to build back better with a renewed focus on strengthening critical infrastructure systems. There is a wide range of actions that can drive this change, and an understanding of the policies that shape infrastructure regulations is a critical first step in this effort. What are the key standards for identifying, building, maintaining and retrofitting critical infrastructure? What measures have been adopted by countries in the region? And what good practices and gaps do we see once these policies have gone into effect?

This report intends to answer some of these questions by providing an overview and an assessment of risk reduction and resilience measures in national policies and regulations. The focus is on countries in Europe and Central Asia, and the policy frameworks that countries in this region have designed to mitigate the impact of disasters and the adverse impacts of climate change.

We have just 10 years left to deliver on what we all agreed in the Sendai Framework for Disaster Risk Reduction, the Sustainable Development Goals, and the Paris Agreement: to move towards a world more free of risk, where resilient, equitable and sustainable development can be made real, and where no one is left behind. Ensuring the continuity of critical infrastructure services is an essential contribution to building a resilient future.

Mr. Octavian Bivol

Chief, Regional Office for Europe United Nations
Office for Disaster Risk Reduction (UNDRR)

FOREWORD

The etymological origin of the word “resilience” stems from Latin word resilio, meaning “to bounce back,” which is used in several areas such as physics, psychology, ecology and planning. Relating this to the present report, it can be understood as the ability to prevent, absorb and recover from shocks and even boost the response of structures. The ability to not only resist but to recover from problems is crucial to the well-being of communities and social cohesion.

As we recover from the COVID-19 pandemic, we must prioritize investing in a more resilient future. In the European Union, climate action will be mainstreamed in policies and programs financed under the Multiannual Financial Framework and the Recovery Plan, NextGenerationEU, with an overall climate minimum target of 30%. Policy makers around the world must realize that it does not suffice to mitigate climate change, we must also adapt to it. Climate Change Adaptation Strategies are necessary to minimize extreme events and climate change impacts. According to a study by the EU Joint Research Centre, damage to infrastructure due to disasters and climate change in Europe currently amounts to approximately €9.3 billion annually and is expected to increase exponentially. Ensuring that critical infrastructure is sustainable and resilient is of vital importance. This report from UNDRR on critical infrastructure policies and regulations in Europe and Central Asia is a critical first step towards understanding which gaps remain in our current policy frameworks, where we need to increase our attention including how to assess and improve resilience.

As we acknowledge that we were unprepared to deal with Covid-19 pandemic, we will move on to prevent other risks and disasters. Therefore, we must increase our infrastructure and our societies resilience. We will do this by:

Investing in resilient infrastructure An estimated €80 trillion will be invested in infrastructure globally by 2030. This should be an opportunity for Europe to avoid the creation of new risks and to adapt to extreme weather events consequences. All public investments, in infrastructure and otherwise, should undergo a robust screening process to ensure that they are resilient to future disaster and climate risk.

Fostering public private partnerships for mutual beneficial solutions Public private partnerships are key to meeting the infrastructure demand and closing the financing gap. It is necessary to invest in financing models which ensure that disaster and climate-related risks associated with new infrastructure is avoided.

Making cities resilient With increasing urbanization, the importance of having strong commitments from local level governments to enhance the resilience of critical infrastructures has become most important. However, often local governments do not have access to sufficient resources, capacity or risk knowledge to develop the necessary urban resilience plans and strategies. It is imperative that the EU supports its Member States to ensure that local governments can develop risk informed urban resilience plans based on a long-term sustainable development vision.

Using Data The possibility of technology to build opportunities to improve resilience is increasing. In many cities data collection is becoming a major advantage in implementing evidence-based public policies. When adequately promoted, data supports the innovation ecosystems to develop new solutions to emerging problems. Cities and regions must recognize data as a very important tool to the success of their resilience strategies. As risks and uncertainty seem to be inevitable in the mid and long term, we have to do more. This report is not only useful, but also acts as a warning about what we must change and must do.

I deeply thank the UNDRR the kind invitation to write this foreword, as I am sure of its relevance to public officials and decision makers.

Ms. Lidia Pereira
Member of European Parliament

SENDAI FRAMEWORK
FOR DISASTER RISK REDUCTION 2015-2030

BACKGROUND

The SendaiFrameworkforDisasterRiskReduction identifies the resilience of critical infrastructure as a key component for disaster risk reduction – in line with Goal 9 of the 2030 Agenda for Sustainable Development, which calls for "sustainable industrial development; universal access to affordable, reliable, sustainable and modern energy services; sustainable transport systems; and quality and resilient infrastructure" (UN, 2015). The Sendai Framework Monitor (SFM) reported that, in 2018 alone, 1,889 infrastructure assets in 20 countries in Europe and Central Asia were damaged or destroyed as a result of disasters, amounting to direct economic losses of over $3 billion (UNDRR SFM report, 2020).

Climate change further exacerbates disaster risks as it affects the frequency and severity of extreme weather events, droughts and floods, placing an additional burden on assets (e.g. droughts and extreme weather affect the critical supply of water for industry). The energy, transportation and water sectors in Europe are particularly at risk; climate-related hazards could significantly affect the lifespan or operation of critical infrastructure in these sectors. Estimates show a 60 per cent rise in the cost of damages due to extreme weather events in the region over the next 30 years (EU CIRCLE, 2019). Studies also indicate that the cost of the recovery of infrastructure from climate change-induced hazards could jump tenfold under a business-as-usual scenario (UNDRR, 2020).

On top of this, a number of current and emerging factors pose additional risks to assets: population growth and rapid urbanization; ageing infrastructure and a lack of investment in building new or retrofitting old infrastructure; the lack of disaster risk and climate change impact considerations in construction designs and in retrofitting projects; and unsustainable investment decisions – all of which increase exposure to hazards. An increase in cyber threats have added an additional layer of complexity, which will only continue to grow as technology develops (UNDRR, 2020).

The resilience and sustainability of critical infrastructure depends on the continuous efforts of planners, architects, developers, owners, operators and all other involved parties to implement adequate measures and comply with standards that clearly incorporate disaster risk and climate change impact considerations. Governments, public authorities and regulators are primarily responsibility for developing and adopting protection mechanisms and regulations that incorporate risk prevention, reduction and resilience measures when investing in, building, maintaining and retrofitting critical infrastructure.

These measures have been adopted, to a varying degree, by countries in the region, allowing us to identify both good practices and gaps in building the resilience of critical infrastructure.

PURPOSE AND SCOPE OF THE REPORT

The purpose of this report is to provide an overview and an assessment of the level of inclusion of risk reduction and resilience measures in national policies and regulations for the protection of critical infrastructure in countries in Europe, Central Asia and the South Caucasus against disasters and the adverse impacts of climate change. This is based on UNDRR's 2020 working paper examining options for addressing infrastructure resilience, which identified six areas that require increased attention and resources. These include:

1 MEASURING AND MONITORING THE VULNERABILITY, SENSITIVITY, INTER-DEPENDENCY AND EXPOSURE TO RISK OF CRITICAL INFRASTRUCTURE ASSETS

2 PROMOTING SHOCK-ENABLED TESTING TO ENSURE THAT CRITICAL INFRASTRUCTURE CAN OPERATE APPROPRIATELY UNDER DIFFERENT CONDITIONS

3 STRENGTHENING REGULATION FOR INCREASED CONSIDERATION OF DISASTER RISK REDUCTION

4 MAKING CITIES RESILIENT BY INCREASING LOCAL CAPACITIES AND RISK KNOWLEDGE

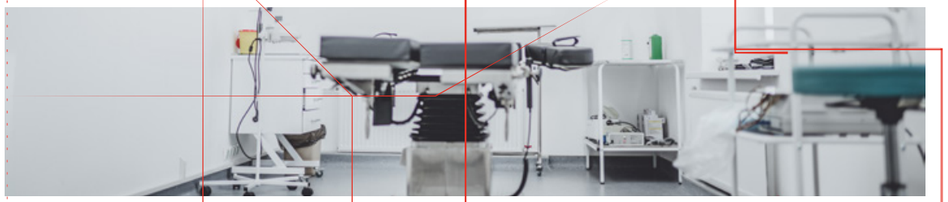
5 ENHANCING THE KNOWLEDGE AND BUILDING THE CAPACITIES OF ALL THE STAKEHOLDERS WHO PLAY A CRITICAL ROLE IN DEVELOPING AND MAINTAINING INFRASTRUCTURE

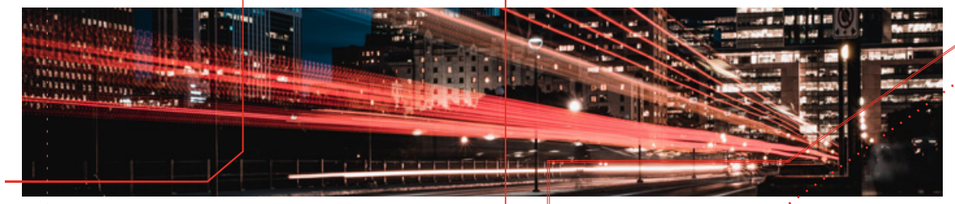
6 DEVELOPING PUBLIC-PRIVATE PARTNERSHIPS THAT CAN FOSTER CO-BENEFITS AND SUSTAINABILITY

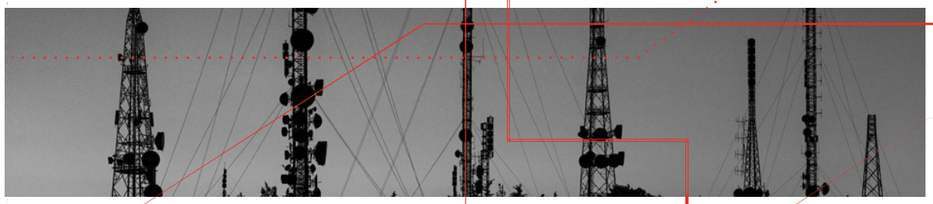
Addressing recommendation number 3 requires a review of existing policies and regulatory mechanisms, to help develop an understanding of the gaps and challenges for strengthening infrastructure resilience.

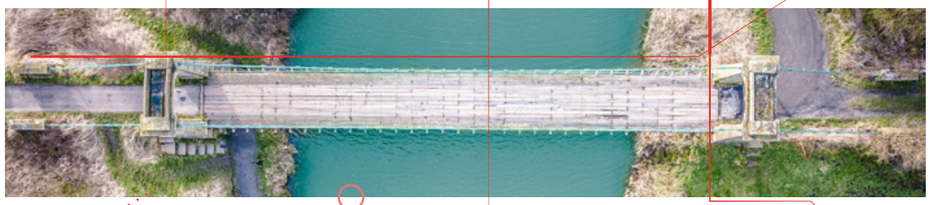
This review examines four critical infrastructure sectors: energy, water, transport and ICT. These are considered vital for securing the normal functioning of States and businesses, and for supporting the everyday life of people – often referred to as 'lifelines'. In addition, these sectors are not single systems but networks, which means that a local emergency could quickly spread and lead to severe disruptions. Finally, these sectors are becoming more and more interdependent, especially with the digitization of services. This calls for the development of resilience measures that can address the complex challenges posed by both the increased linkages and increased risks (Hallegatte et al., 2019).

FOUR CRTICAL INFRASTRUCTURE SECTORS COVERED IN THIS REPORT









Yang Liu/Unsplash.com
Arseny Togulev/Unsplash.com
Marc-Olivier Jodoin/Unsplash.com
Mario Caruso/Unsplash.com
Dan Smedley/Unsplash.com

DEFINITIONS AND METHODOLOGY

There is no universally accepted definition for what constitutes or is included in 'critical infrastructure'. While the Sendai Framework has a focus on 'critical infrastructure', it refrains from establishing a definition, leaving it for national governments to decide on elements to include when reporting on progress. However, the Framework does identify some infrastructure types that it considers critical: water, transportation and telecommunications infrastructure, educational facilities, hospitals and other health facilities.

Some of the countries covered in this report, such as Portugal and France, place more emphasis on the importance of critical infrastructure for supporting vital socioeconomic activities, while others, such as the United Kingdom, the Czech Republic, the Netherlands and Turkey, focus more on sustaining the safety of citizens and the security of the State and its organs. As the understanding of risk evolves to encompass new threats, some nations have also looked into widening the scope of what constitutes 'critical infrastructure'. Switzerland, for instance, has opted for a simpler and broader definition, to enable it to respond more rapidly to the changing environment, stating simply that critical infrastructure includes *"processes, systems and facilities that are essential for the functioning of the economy and the well-being of the population, respectively"* (OECD, 2019; CH FOCP, 2017, p. 511).

The 2009 UNISDR publication, Terminology on Disaster Risk Reduction, defined critical infrastructure as *"the primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency"* (UNISDR, 2009). According to the European Union (EU) Commission, critical infrastructure is the "physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in (EU) States" (EU Commission website, 2020). Even though definitions might vary, there is a prevailing understanding among nations and organizations that critical infrastructure constitutes both physical elements (facilities, equipment, networks) and vital services (health care, safety, etc.), and that the disruption of these elements and services would pose a serious risk to the normal functioning of society and the State (OECD, 2019).

For the purposes of this report, the definition provided in the 2016 Report of the *Open-Ended Intergovernmental Expert Working Group (OIEWG) on Indicators and Terminology Relating to Disaster Risk Reduction* will be used. Here, critical infrastructure is understood as:

"The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society" (UNGA, 2016, p. 12).

There is also a need to define what represents a 'regulatory mechanism'. Again, there is no universal definition, but one commonly used is provided by Black (2002, p. 26): "the sustained and focused attempt to alter the behaviour of others according to defined standards and purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour modification" (Koop and Lodge, 2015).

The OECD defines 'regulatory policy' as "an explicit, dynamic, and consistent 'whole-of-government' policy to pursue high quality regulation", adding that "an effective regulatory policy should be adopted at the highest political levels, contain explicit and measurable regulatory quality standards, and provide for continued regulatory management capacity" (OECD, 2011). Based on these definitions, this report takes 'regulatory mechanisms' to mean the methods and processes that public authorities employ so that certain policies, laws and measures are applied, to ensure the protection and resilience of critical infrastructure and services, in adherence with set objectives and goals.

This report represents a desk review of critical infrastructure policies, focusing on a number of countries in Europe, Central Asia and the South Caucasus – all of which are covered by UNDRR's Regional Office for Europe (the office covers 55 countries).


Dan Smedley/Unsplash.com

The information was collected from both primary and secondary sources, including official government documents and legislation, reports by international and regional organizations, academic articles and news items in mass media outlets. The report does not include information on all of the countries from the European and Central Asian region but there was a concentrated effort to showcase examples from as many countries as possible. Likewise, the report does not provide an exhaustive list of all national policy and regulatory mechanisms but focuses on some key measures and practices.

- PART 1 is an overview of current and future threats to critical infrastructure posed by disasters and climate change. Particular attention is given to the importance of understanding the interdependencies between the four sectors in view of the need for developing comprehensive, 'all-hazards' approaches.

- PART 2 explores the role of national policies and regulatory mechanisms, as the resilience of critical assets largely depends on the adequacy of policies at national and local levels.

- PART 3 provides a brief description of regional frameworks and initiatives of relevance to national mechanisms , followed by an analysis of the level of inclusion of resilience measures in national policy for each sector, with specific country examples.

The report concludes with recommendations based on the analysis and available literature.

1 DISASTER RISKS AND CLIMATE CHANGE IMPACTS ON CRITICAL INFRASTRUCTURE

1.1 CURRENT AND FUTURE RISKS
1.2 INTERDEPENDENCIES

1.1 CURRENT AND FUTURE RISKS

Natural and man-made disasters pose some of the greatest challenges to the continued operation of vital assets and services. In the space of only two months, in October and November 2019, several disastrous events occurred across Europe.

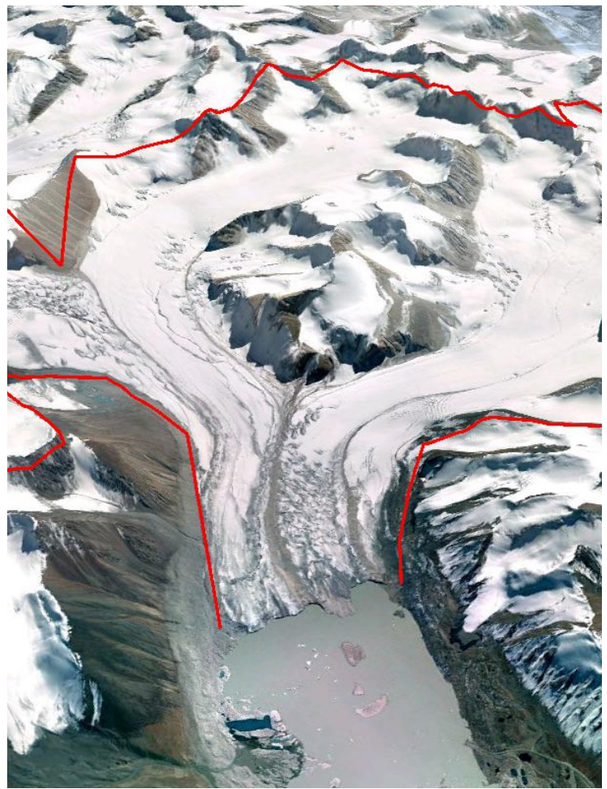
In October, heavy rainfall and winds caused severe disruption on railways and roads in France and Spain, completely submerging certain areas. In France, a number of train tracks and road pavements were washed away, while in Spain more than 25,000 people experienced power cuts (DW, 2019).

In November, mudslides caused by heavy snow disrupted train lines and caused an electricity blackout in Austria, affecting 1,700 households (AP News, 2019).

Again in November, a 6.4-magnitude earthquake struck Albania, causing the collapse of buildings, road damage and soil liquefaction, totalling €33.42 million in infrastructure damage and losses – of which €8.18 million of damages were in the energy sector and over €5 million in damages and losses were in the transport sector (BBC, 2019; Gov of Albania et al., 2020).

According to analysis by the European Environment Agency (EEA), countries in Europe and Central Asia will experience a number of changing conditions, which could pose risks to the normal and sustainable functioning of critical infrastructure. Extreme weather events, droughts and floods, rising sea levels and storms will have a negative impact on a number of vital services (EEA, 2019). Storms are the major cause of disruptions to electricity supplies in Belgium, Croatia, Portugal and Slovenia (Hallegatte et al., 2019). In 2017, UK assessed that its energy sector is highly vulnerable to climate change, in particular to rising sea levels. In the Netherlands, the Royal Netherlands Meteorological Institute has developed flood risk scenarios that show that the level of the southern North Sea will increase by 25 to 80 cm by 2100, and more frequent extreme and higher waves could be expected along the western European coast, with potential impacts on the energy and transport sectors. Climate change is expected to lead to drier conditions in southern Europe, while northern Europe will experience increased water availability but, in both cases, not evenly throughout the year. This will lead to both a reduction in water supplies for the energy industry and an increased risk of flooding across the region (EEA, 2019)

In Central Asia and the South Caucasus, it is expected that the mean temperature rise by the end of the century (2071-2099) is expected to be higher than the global average increase. For the Central Asia region, the prediction is for a 2.5-6.5 °C rise (under a 2-4 °C global warming scenario), in comparison to the 1951-1980 period. The South Caucasus will be much less affected under a low-emission scenario (up to 2°C global warming scenario), but under a 4°C global warming scenario mean annual precipitation could decrease by around 20 per cent. These changes could have disastrous consequences for the whole region, with glaciers in the high mountains retreating and an increased probability of flooding from overflowing rivers.



This would be exacerbated by ageing infrastructure and limited capacities. All critical infrastructure sectors, as well as agriculture, would also be impacted by extended seasonal droughts. Kazakhstan, Georgia and Azerbaijan are among the countries with critical assets most exposed to natural hazards and climatic risks (SDC, 2019; UNESCAP, 2020).

At the same time, the UN envisages that, by 2050, the global population will reach approximately 9.7 billion, growing to 10.9 billion by 2100. Even though the predictions for Europe indicate a negative growth rate, migration from outside the region is expected to continue (Population Matters, 2020). By 2050, it is also estimated that 83.7 per cent of the population of Europe (European territories) will be living in urban areas, compared to 74.9 per cent in 2020 and 69.9 per cent in 1990 (UN DESA, 2018). The EU Commission projects that by 2100, 31.3 per cent of the population of its Member States will be 65-years of age or older, in comparison to 19.8 per cent in 2018 (Eurostat, 2019). These demographic changes will require new infrastructure and critical services to account for the specific needs of a rapidly ageing society.

By 2050, passenger transport in Europe is expected to increase by 42 per cent and freight transport by 60 per cent, placing additional pressure on transport infrastructure and the environment. By 2040, European airports may be unable to accommodate the estimated surplus of 1.5 million flights, as demand continues to soar (EC, March 2019). Road congestion is estimated to cost more than €110 billion annually, and could become a major issue in the coming decades (Christidis and Rivas, 2012).

At the same time, despite the long-term recognition of the consequences of ageing infrastructure and the significant


Fishman64/Shutterstock.com

investments that have been made, a large number of assets remain under-maintained and at risk of damage or collapse. Over 840 bridges are at risk of collapse in France alone (McLellan, 2019). Energy infrastructure in the region is also approaching its designated lifespan, leading to degraded performance and an increased risk of failure in times of disaster (The DEFENDER consortium partners, 2017).

Power cuts due to old infrastructure are still common in some countries in Central Asia and the South Caucasus, and while improvements have been made, distribution and transmission losses remain high (Nabiyeva, 2018). In the water sector, EU programmes have supported the renewal of critical assets, including pipes, treatment plants and wastewater utilities. Nonetheless, there are still **segments of pipes that have been operating for more than 100 years, and current levels of investment cannot meet all the challenges presented by increasing urbanization, population growth and climate change** (Ramm, 2018).While the continuous development of technology has provided new opportunities for more efficient operation of critical infrastructure, it has also introduced new risks. Global economic losses related to cyber incidents range between $400 and $575 billion annually (Ganin et al., 2017). Services are increasingly being digitized, important business and personal user information is stored online, and operations in all sectors are now programmed and automated. Malicious cyber-attacks or system failures could have serious consequences in themselves but when coupled with disaster events the results could be devastating. Innovations in artificial intelligence, the expected spread of autonomous vehicles and the emergence of smart cities, all of which rely on data management, require new and flexible regulations, continuous threat assessments, and improved preparedness and mitigation measures (WEF, 2019; UNDRR (cyber), 2020).

Underinvestment in critical infrastructure resilience could lead to serious socioeconomic disruptions at the local, national, regional and global levels due to the high degree of interconnectedness between sectors and the potentially devastating effects from cascading failures across systems and networks (Drzik, 2019).

$1 → **$4**

INVESTEMENT IN INFRASTRUCTURE RESIILIENCE

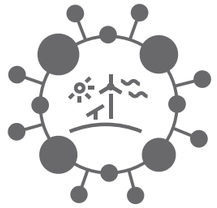
BENEFIT FOR LOW AND MIDDLE INCOME COUNTRIES

The World Bank has estimated that investing $1 in infrastructure resilience proves to be beneficial in 96 per cent of thousands of scenarios of possible future socioeconomic and climate trends.

In a median scenario, each $1 investment could bring a $4 benefit, amounting to $4.2 trillion in benefit for low- and middle-income countries globally, while the cost of inaction for the 2020-2030 period may amount to around $1 trillion (Hallegatte et al., 2019).

According to the World Economic Forum (WEF), current trends in global investment in infrastructure will amount to approximately $79 trillion by 2040 – $18 trillion less than the estimated investment needed for the same period (across 57 countries and seven sectors) (WEF, 2019).

In Europe, the EU has assessed that its members will have to budget €688 billion annually for the energy, transport, water and sanitation, and telecommunications sectors to meet investment needs (EP, 2018). In Central Asia and the Caucasus, the Asian Development Bank (ADB) estimated that overall infrastructure investment needs amount to approximately $33 billion annually until 2030 in a business-as-usual scenario, and approximately $38 billion in a climate-resilient scenario (includes the countries covered by the ADB) (ADB, 2017).



Last but not least, the current COVID-19 pandemic has highlighted the importance of properly functioning and fit-for-purpose infrastructure for the provision of essential services. Assets and services that had previously not been considered critical have become paramount in dealing with the public health crisis. Changes in daily and business habits and the sudden demand for online services have revealed the need for more robust data management (Deloitte, 2020). Transportation and logistics, waste management and ICT systems have been under pressure to adjust to the changing risks and public needs (UN, 2020). The transport sector has been particularly affected, with huge economic losses for civil aviation and water transportation. The International Civil Aviation Organization (ICAO) has estimated that European international traffic will suffer economic losses of between $57 billion in the best-case scenario and $98 billion in the worst case scenario, and domestic traffic between $10 and $18 billion as a result of the virus (ICAO, 2020).

The global pandemic underlines the fundamental role of public policies focused on prevention, resilience and sustainability, and the need for planning and investments in social protection, critical infrastructure and crisis management, as well as robust digital security. Future assessments of the effects of the pandemic will help identify structural vulnerabilities and inequalities, which would also be highly relevant for addressing gaps in critical infrastructure resilience (UN, 2020).

1.2 INTERDEPENDENCIES

The 2019 UN Global Assessment Report on Disaster Risk Reduction underlines the importance of acknowledging and understanding interdependencies between different critical infrastructure systems. These interdependencies can be broadly divided into four categories:

1 PHYSICAL — Goods or resources are transferred between infrastructure systems (e.g. electric power and water).

2 CYBER — Transfer of information and/or data.

3 GEOGRAPHIC — The physical proximity of infrastructure, where the destruction or disruption of one asset could have an impact on other assets nearby.

4 LOGICAL — Connections that cannot be categorized under the previous three types and which refer to impacts originating at the decision-making level of organizations on the distribution of human and financial resources (Lewis and Petit, 2019).

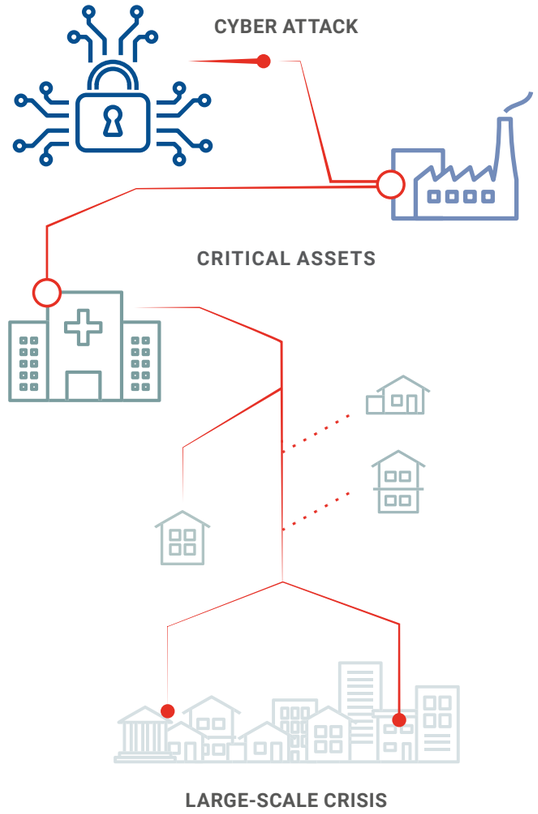
Critical infrastructure assets cannot and do not operate in isolation but rather as 'a system of systems'; the failure of one structure could result in serious disruptions in others.

(LEWIS AND PETIT, 2019)

Trinet Uzun/Shutterstock.com

In 2014, as a result of the devastating floods in Serbia and Bosnia and Herzegovina, thousands of households in both countries were cut off from electricity and telephone lines, in some cases for days. Hundreds of roads and bridges were destroyed or damaged. Access to certain areas was blocked and more than a million people experienced water supply shortages (ACAPS, 2014). In March 2015, Amsterdam and the surrounding region suffered a power outage that lasted more than five hours, affecting over one million households. The outage was caused by a technical fault at a network substation. The backup system also failed, resulting in the blackout. The disruption caused traffic jams as traffic lights stopped working, trams and the metro were brought to a halt, and flights had to be diverted from Schiphol airport (Escritt, 2015).

A malicious cyber-attack on any critical asset could have ripple effects and result in a large-scale crisis – as exemplified by the 2015 cyber-attack in Ukraine, which affected the electricity supply; and by the 2017 Wannacry and NotPetya ransomware, which heavily disrupted critical infrastructure services across Europe (the National Health Service in the UK, telecommunications in Spain, railway operations in Germany and shipping operations in Denmark) (OECD, 2019).



Panda and Bower (2020) and Walker (2012) have documented several examples, including a 2009 incident when several hospitals in the UK suffered a malware attack that resulted in a complete loss of connectivity, which left personnel unable to access the system.

These are only some of the many examples and possible scenarios illustrating how failures in one infrastructure type could lead to disruptions in others. Countries are increasingly focusing on research in this area in order to develop an all-hazard and a systems-based approach.

2 ROLE OF NATIONAL POLICY AND REGULATORY MECHANISMS IN ADDRESSING INFRASTRUCTURE RESILIENCE

CHUTTERSNAP/Unsplash.com

2

ROLE OF NATIONAL POLICY AND REGULATORY MECHANISMS IN ADDRESSING INFRASTRUCTURE RESILIENCE

The continued uninterrupted supply of water and power; road, rail, water and air transport connectivity; and secure telecommunications are vital for the functioning of societies. The increased risk of infrastructure damage and associated economic losses (both direct and indirect) is linked with the growing number of assets exposed to hazards and the lack of adequate policies and prevention measures that account for disaster and climate change impacts (UNDRR, May 2019). According to a 2019 World Bank global analysis on infrastructure performance, the quality of assets and services, as well as the effectiveness of public expenditure and the inclusion of resilience measures, are directly dependent on the quality of governance and management. **High standards, transparent decision-making processes and greater accountability are the pillars of efficient and resilient infrastructure, highlighting the importance of assessing national policies and regulatory mechanisms (Kornejew et. al., 2019).**

The responsibility for ensuring the resilience of critical assets lies, to a large extent, with the owners and operators of infrastructure – both public bodies and private companies. That said, the nature of critical infrastructure as a public good, and its importance for the safety of residents and the continuity of vital services, gives governments and public authorities an inherent and, in the majority of cases, legally-defined role in infrastructure protection. National and local authorities are responsible for establishing legislation and standards, allocating public funds, providing oversight and regulation alongside designated regulators (who could be placed within public institutions or be independent bodies outside of the government), and fostering cooperation between sectors (UK NIC, 2019; Keele and Coenen, 2019; UNDRR, 2020). Governments are also responsible for creating the environment and the legal framework for the regulation of infrastructure investments and for streamlining sustainability policies in infrastructure projects.

National and local resilience strategies and robust national regulatory mechanisms can, therefore, be a powerful tool for influencing the way financial investments are made (UK NIC, 2019).

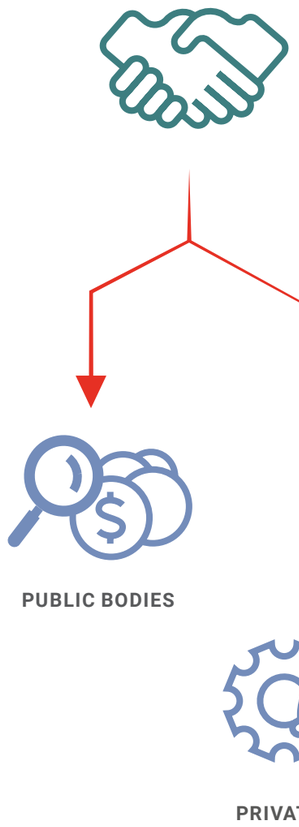
Joakim Honkasalo/Unsplash.com

In practice, a number of actors are involved in the design, planning, construction, operation, maintenance and ownership of critical assets. Traditionally, such infrastructure has been owned and managed by public bodies, but in recent years, semi-private and private companies have become increasingly involved in these processes. In some countries, public control over critical infrastructure has diminished as a result of private companies taking over services. Increased private participation can drive necessary innovation and improve flexibility, as well as increase funding opportunities. However, while private owners and/or operators usually recognize the importance of protecting assets, the perception of risk and views on the required level of security, safety and preparedness may differ between public authorities and private businesses. A lack of established common standards and frameworks, developed in partnership with relevant private sectors, is a common hindrance to implementing robust resilience measures (OECD, 2019; Melchiorre, 2018; Keele and Coenen, 2019; UNDRR, 2020).

The fact that so many partners are involved in the management of critical infrastructure poses challenges for efficient coordination, especially given that policies are developed by a number of different authorities at the national, regional and local levels within countries and across sectors. Gaps in information sharing and communication between local and national authorities are common, and often local authorities do not have an adequate awareness of risk, the necessary capacities, or the power to develop and enforce risk reduction policies. Often, there is a lack of a clear initial understanding of what critical infrastructure resilience entails among both the public bodies and private companies involved (UNDRR, May 2019; UNDRR, 2020).

Public authorities and regulators have the important task of overcoming these challenges and closing the gaps by engaging private companies in conversations on resilience and raising awareness of the benefits of investing in resilience or sanctioning businesses that lack compliance with established rules and standards. Such a responsibility might be new for regulators, who tend to focus predominantly on promoting competition and adjusting prices; however, their role in monitoring and approving financial resources puts them in an ideal position to mainstream resilience in infrastructure investments (UK NIC, October 2019).

PUBLIC-PRIVATE PARTNERSHIPS (PPPS)



A number of mechanisms exist for governments to engage with and regulate asset managers and private and semi-private companies, to ensure the resilience of critical infrastructure and services. A common practice is the use of public-private partnerships (PPPs), whereby the private sector usually provides the service and public bodies exercise oversight over the activities and provide some of the financing or incentives. Other possible measures employed by governments and regulators include risk disclosure in mandatory financial reporting for asset operators and the use of disaggregated data for understanding risks and needs. The increasing requirements linvked with climate change and other stresses has prompted the need for governments to revisit the various mechanisms and practices they have used until now, and to critically re-evaluate the ability and capacity of both public and private partners to manage risk (Hallegatte et al., 2019; Keele and Coenen, 2019).


Salivanchuk Semen/Shutterstock.com

Often, public bodies provide both targeted incentives and penalties for companies managing critical infrastructure, to encourage them to incorporate resilience measures in their practices. In Finland, for instance, a combination of incentives and penalties was used to govern the energy sector. The 2013 Energy Market Act provided price incentives for those operators who improve the resilience of their networks, while at the same time introducing additional fees for operators who cannot meet the resilience targets. Another strategy used in Finland has been to share the results of the annual assessments of business continuity plans for energy operators so that they can compare their performance and learn from each another. The peer-pressure within the sector encourages operators to enhance their resilience measures. However, it is important that authorities find a good balance between 'sticks' and 'carrots' so that policies do not lead to price burdens for the end users (OECD, 2019).

3 OVERVIEW AND ANALYSIS OF REGIONAL AND NATIONAL REGULATORY FRAMEWORKS AND POLICIES: ENERGY, WATER, TRANSPORT AND ICT

3.1 REGIONAL FRAMEWORKS AND INITIATIVE

3.2 NATIONAL REGULATORY FRAMEWORKS AND POLICIES AND INITIATIVES

ENERGY • WATER • TRANSPORT • ICT

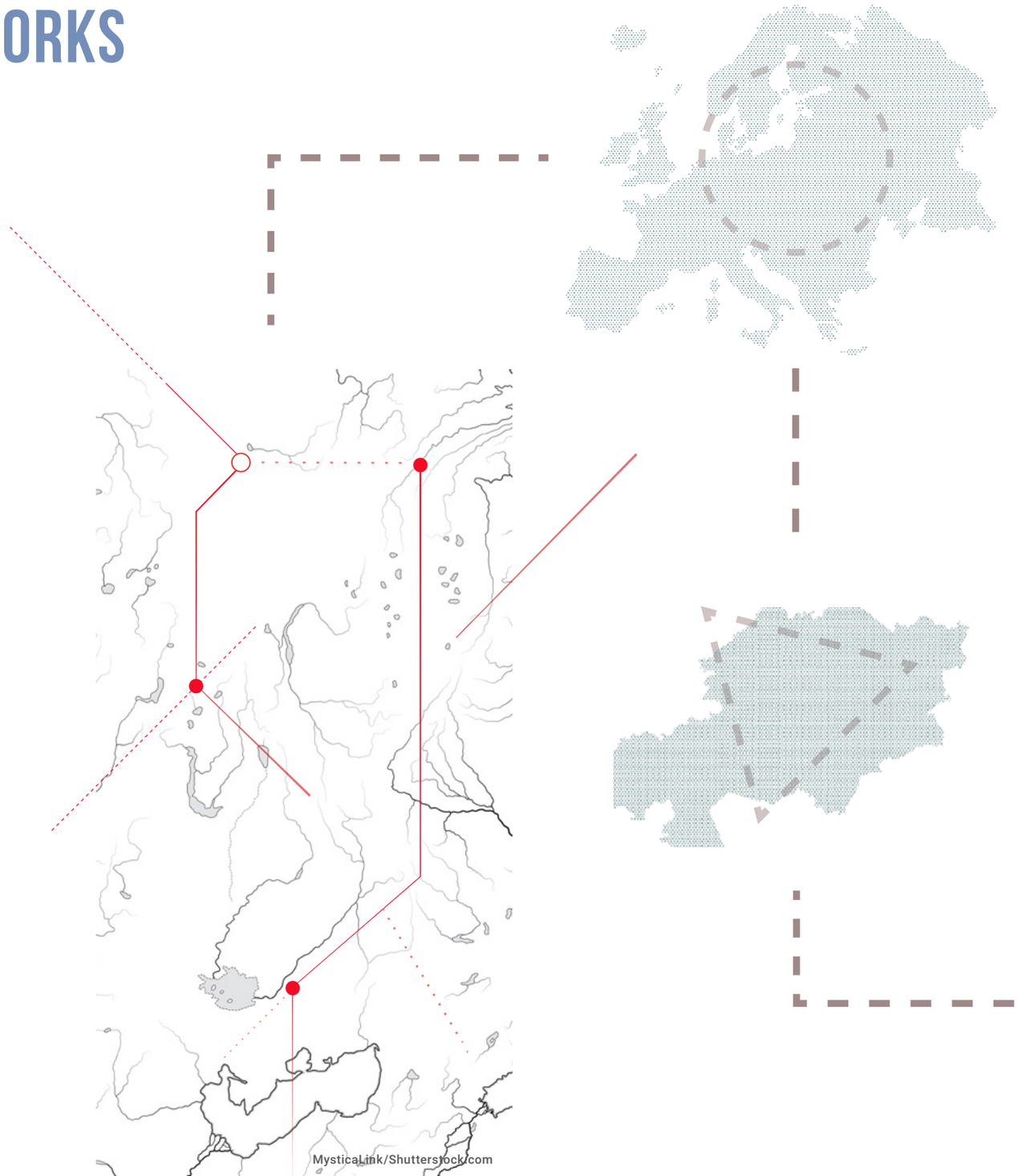
chekart/Shutterstock.com
Surapol USanakul r/Unsplash.com
Dan Smedley/Unsplash.com
Nguyen Quang Ngoc Tonkin/Unsplash.com

3.1 REGIONAL FRAMEWORKS AND INITIATIVES

The countries of Europe and Central Asia are part of a number of important regional frameworks that have an bearing on the development of national policies and procedures.

The EU has increasingly recognized the risk of natural and man-made hazards to critical assets, as well as the need to address interdependencies between sectors. This is reflected in the EU Civil Protection Mechanism – which extends to partner nations outside of the EU – that clearly states that the protection of critical infrastructure requires the development of mitigation and adaptation measures against disaster risks. The mechanism requires countries to conduct national risk assessments and provides emergency aid and assistance, on request, through the Emergency Response Coordination Centre (ERCC) (EC, May 2017).

The European Critical Infrastructure (ECI) Directive from 2008 establishes a set of key definitions, creates a procedure for the identification and designation of ECI, and lays the ground for a common approach in assessing the requirements for protecting critical assets (EC, July 2019). Even though the Directive was initiated as a response to an evolving terrorist threat across European countries after the 2001 9/11 attack in the US, natural and man-made hazards were also included in its scope. The Directive is applicable when the disruption of critical infrastructure affects two or more Member States or when the impact has the potential for trans-national disruptions.



MysticaLink/Shutterstock.com

The ECI Directive focuses only on the energy and transport sectors, but the EU has adopted a separate policy on Critical Information Infrastructure Protection (CIIP) aimed at securing the resilience of vital ICT assets. In regards to the water sector, EU Member States are subject to EU Directive 2000/60/EC – the Water Framework Directive (WFD) – which obliges Member States to implement improved EU water policies, based on the principles of integrated water management. Special attention is given to flood management in EU Directive 2007/60/EC (Floods Directive), which has been transposed into national legislation (Karagiannis et al., 2019); this is particularly relevant to the protection of critical infrastructure.

In January 2020, the EU published a new work programme that aims to update the ECI Directive, with the introduction of additional measures that reflect the interconnections between sectors. Provisions were made in light of the possible expansion of the Directive to cover other sectors aside from energy and transportation. The proposal is scheduled for adoption in the fourth quarter of 2020 (EP, 2020).

The intervention came after the EU conducted reviews of the 2008 ECI Directive in 2012 and 2019, which found that, even though countries transposed the Directive into their national legislation soon after it was adopted, its practical implementation still lagged behind. There were severe discrepancies in the way countries applied the policy and very little proof that the security of the energy and transport sectors had improved. **The review also found that very few European critical assets had been identified and designated as such** (EC, July 2019).

The fact that countries have defined what constitutes critical infrastructure in slightly different ways, and that the key partners in critical infrastructure policy (governments, experts, the private sector and sectoral regulators, among others) have different roles in each country, further contributes to discrepancies in coordination at the regional level and, at times, leads to overlapping frameworks. In fact, in its review, the EU argued that overlapping policies are not so much an issue at the national level as they are at the EU level, and noted the need to address this concern (CEPS, 2010; EC, July 2019). The 2019 review of the Directive also highlighted **the difficulties in addressing evolving risks due to the discrepancies in risk assessment methodologies and the lack of a single framework that addresses and manages all threats in a systemic manner. In addition, the document highlighted the lack of focus on resilience – in other words, the ability to 'bounce back' after emergencies and maintain minimal operational capability** (as opposed to developing robust infrastructure capable of withstanding all threats, a concept now deemed physically and financially impossible) (EC, 19 June 2020).

A common approach for critical infrastructure risk assessment is still lacking; however, the EU has made important steps towards creating a mechanism for identifying which investments qualify as resilient and which do not.

In March 2018, an action plan on sustainable finance was adopted by the EU Commission, envisaging a comprehensive strategy linking finance with sustainability. The action plan stipulates the establishment of an EU classification system or a taxonomy that sets screening criteria for 70 climate change mitigation and 68 climate change adaptation activities.

The EU has provided invaluable expertise and financial support through numerous projects across the Union as well as with partners from neighbouring regions. The Transport Corridor Europe-Caucasus-Asia (TRACERA) programme, for example, has been active since 1993. The initiative focuses on developing transportation corridors in 13 countries from Europe, Central Asia and the South Caucasus to improve trade and economic development. The programme recently released a new strategy, and a master plan was agreed for the 2016-2026 period. The master plan identifies sustainability and environmental considerations as crucial components of the initiative but does not give details on particular measures, nor does it include recommendations on managing disaster risks and climate change impacts (Russel, 2019; Egis International and Dornier Consulting, 2014).

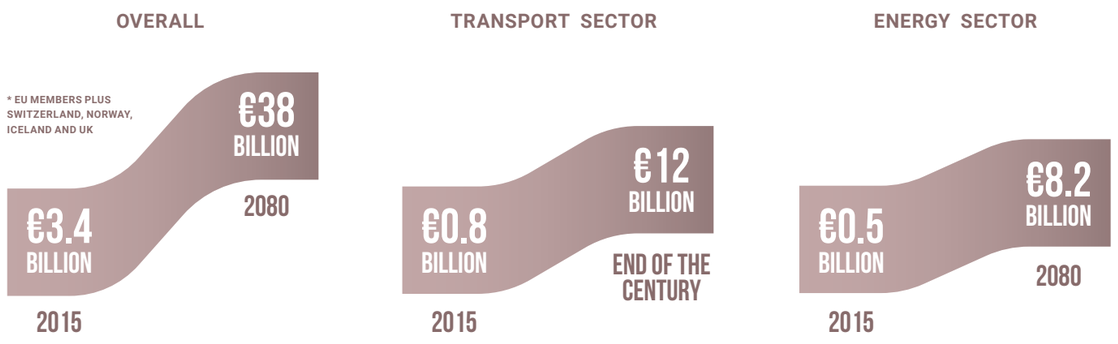
A number of other organizations and individual governments have also provided funds and assistance for developing infrastructure in Central Asia and the South Caucasus. ADB, for instance, has been working on a Central Asia Regional Economic Cooperation (CAREC) Program since 1997 and has recently issued a new CAREC Transport Strategy for the period up to 2030 – following on from its current strategy, which ends in 2020. The programme aims to develop key air, road and rail transportation corridors linking the countries between Europe, Russia, the Middle East and Asia, covering 7,800 kms of roads and 1,800 km of rail tracks. The 2030 strategy focuses on increasing the sustainability and quality of assets, including greener transport innovations (ADB, 2020). **The document notes the need for governments to shift towards longer-term strategies that take account of climate change impacts, in line with the 2030 Agenda for Sustainable Development. It does not, however, make a case for the importance of developing disaster-proof and resilient infrastructure and services.**

There are various programmes and projects in the region that focus on developing important transport corridors and improving energy and water services, which should last for decades. There is, however, a lack of long-term regional and national strategies and tangible commitments to resilience, hindering opportunities for integrating adequate disaster risk and climate impact measures (OECD, December 2019). In this sense, external partners could play a significant role in establishing resilience requirements and risk assessments. If resilience measures are not implemented this could undermine progress towards the Sustainable Development Goals. Given the number of organizations and countries with similar intentions of developing infrastructure in the region, especially along trade routes, there is a need for greater coordination between all parties to avoid conflicting interests. Resilience should become an integral part of these discussions.

3.2 NATIONAL REGULATORY FRAMEWORKS AND POLICIES

According to a 2015 report by the EU Joint Research Centre, Europe will experience a significant increase in multi-hazard, multi-sector damages in the next few decades: damages for EU Members plus Switzerland, Norway, Iceland and the UK are expected to increase from €3.4 billion annually in 2015 to 38 billion by 2080. The largest increase in multi-hazard damages is expected to be in the energy sector – from €0.5 billion annually in 2015 to €8.2 billion by 2080 – and the transport sector – from €0.8 billion in 2015 to €12 billion by the end of the century. Currently, climate hazards predominantly relate to river floods (44 per cent) and windstorms (27 per cent) but hazards due to droughts and heatwaves are projected to increase substantially; they could make up more than 70 per cent of climate hazard damages by the end of the century (Forzieri et al., 2015).

ESTIMATED MULTI-HAZARD ECONOMIC DAMAGES




Rawpixel.com/Shutterstock.com

As awareness of these emerging risks has increased, governments have developed and updated their national legislation and policies accordingly. For instance, 30 of the 34 countries participating in the EU Civil Protection Mechanism (the EU Member States plus Iceland, North Macedonia, Montenegro, Norway, Serbia and Turkey) have integrated floods in their national risk assessments (NRA); of these, ten have designated floods as a risk to critical infrastructure. Similarly, 20 nations have developed scenarios for long-term power outages in their NRAs (Karagiannis et al., 2017). However, there is more work to be done in this area. The decentralization of electricity networks and the multiplication of local grids, which brings with it new and emerging risks, may undermine earlier efforts. This calls for new strategies, practices and resilience measures to take account of these structural changes.

Both at the national and regional levels, gaps in the understanding of the links between climate change, disaster risk and infrastructure protection still exist. Attempts to address these issues through national mechanisms appear to be somewhat disparate. Nations have developed national sustainable development plans, climate change adaptation plans, national disaster risk reduction strategies, as well as legislation on the protection of critical infrastructure, but an understanding of how these different policies should interact in a coherent strategy is often missing, and coordination between bodies working on specific areas is limited. The current policies and regulatory systems of the majority of countries contain protection measures against known threats but provide little strategic direction on addressing issues such as limiting GHG emissions, managing increased disaster risks, tackling the negative impacts of climate change or responding to technological threats. This does not mean that existing systems need to become completely obsolete but that important updates are required to meet the new challenges (NIC UK, October 2019).

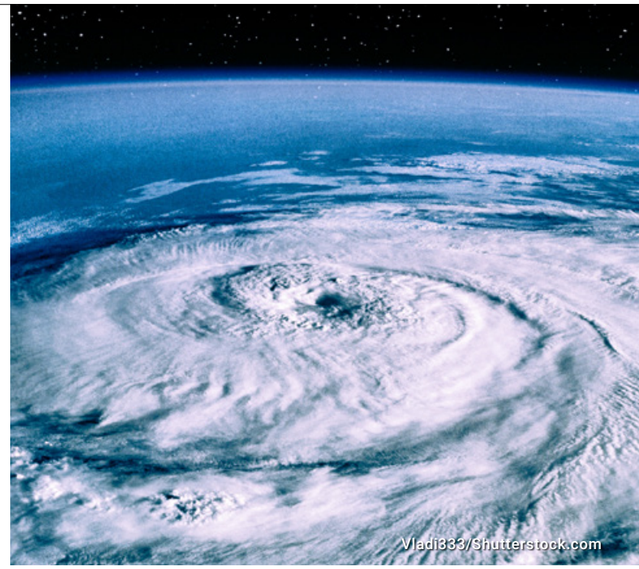
Countries in the region have adopted different approaches to the protection of critical infrastructure. The UK, for instance, employs a multi-agency approach and a mechanism for coordination between the public and the private sectors, while in France much of the responsibility lies with the public authorities. In the Netherlands, on the other hand, the private sector plays a more significant role within PPPs. Policies also vary across sectors. In the energy sector, for example, there is a need to simultaneously ensure security of supply, respond to concerns over climate change impacts and maintain an affordable price for end users; while in the ICT sector, rapid developments in technology pose new and evolving cyber risks that could impact assets in other sectors as well (CEPS, 2010). **This complex web of varying national mechanisms and sectoral specificities poses significant challenges, not only for cross-border and regional cooperation and standardization but also among domestic bodies and partners**. It also significantly complicates planning resilience measures across interlinked sectors as addressing risks in one sector could hamper efforts elsewhere.

A 2008 study by the Swiss Crisis and Risk Network on the development of critical infrastructure protection policies in 25 countries noted the emergence of three key trends. First, nations are increasingly instigating efforts to integrate resilience measures and adopt all-hazard approaches, taking stock of interdependencies and cascading failures. This is based on the understanding that the comprehensive protection of all assets is practically impossible and that prioritization is necessary; rather, the focus should be on enhancing the capacity to respond and bounce back. Second, as a consequence of adopting all-hazard approaches – which require improved coordination between partners and institutions – there has been a shift towards the centralization of responsibility for the protection of critical infrastructure in some countries (such as the UK and Switzerland). Finally, the growing concerns around the digitization of services and the dependence on ICT infrastructure has compelled countries to pay more attention to cyber security (CRN, 2009).

These developments, however, have come up against a number of challenges. Countries struggle to reconcile economic efficiency with the safety and security of interconnected assets and services; productive efficiency is usually achieved at the lowest possible cost. In many countries in Europe and Central Asia, private investments in infrastructure remain low due to a lack of incentives or excessive red tape, which often leads to compromising on the quality of materials or contractual obligations that fail to include measures for sustainability and resilience. Setting liability rules for faults or negligence is another major issue. Establishing causation in multiparty, multi-risk environments in connected systems is a difficult task; this is even more challenging in the absence of clear standards. **The lack of risk information – the basis for mitigation measures and setting standards – is a major concern** (CRN, 2009).

In most countries, risk assessments of critical infrastructure only take into account likely hazards and do not consider disaster risks, climate change impacts and interdependencies in a systematic way. This is true for all critical sectors, especially in countries that traditionally have not experienced many disasters. Different scenarios exploring a range of possible threats of varying likelihood and magnitude are rarely included in testing activities (UNDRR, 2020; OECD, 2019).

The following sections of the report look at some specific examples of national efforts in each of the four sectors. The aim is to provide an insight into the current status of the integration of disaster risk and climate change mitigation measures in national critical infrastructure protection policies.



The UK's National Infrastructure Commission has recently developed an approach that tracks 'functional dependencies' between different sector assets through network modelling techniques. The model tracks inter-linkages between the water, rail, road, electricity and digital sectors and aims to explore possible cascading faults. This model does not currently analyse dependencies between assets related to their physical proximity and does not take into account the possibility of human error, thus excluding man-made disasters. Still, the approach can make assumptions where information is not available (UK NIC, 2020). The model is still a work in progress but is a good example of efforts focused on addressing important gaps in infrastructure resilience mechanisms.

This links to the wider issue of the lack of comprehensive data on critical infrastructure protection. According to the UK's National Infrastructure Commission, Europe has a relatively high level of adaptation capacity compared to other regions of the world – although the impacts of climate change and the capacities to respond vary across countries. The Commission found that even though coping and adaptation strategies are developed at regional, national and local levels, there is a lack of systemic information on the actual effectiveness of implemented policies and measures, and limited evidence of adaptation planning (UK NIC, October 2019).

To add to this, a 2017 assessment on the readiness of all participating nations to report on the Sendai Framework targets showed that data related to targets A (on the number of deaths and missing persons) and B (on direct economic loss) was available for approximately 83 reporting countries, but data related to target D on reducing damage to critical infrastructure was available for only 60 per cent and is rarely complete. Data on infrastructure damage is often missing, or only takes account of large-scale crisis events, or is calculated in a different manner by different countries. Governments are required to make greater efforts to set appropriate mechanisms for the collection of detailed data in line with the reporting requirements of the Sendai Framework so that they can take more informed decisions to protect their critical assets (UNDRR, May 2019).

ENERGY SECTOR

An assessment report by the European Environment Agency (EEA), conducted among the members of the EU (plus Norway, Switzerland, Turkey and the UK), found that while the majority of countries include the energy sector (to varying degrees) in their Climate Change Impact, Vulnerability and Risk (CCIV) assessments, very few have included it in their national adaptation plans and strategies. Only Belgium, Finland, the Netherlands, Norway, Switzerland and the UK have implemented climate change adaptation measures in their energy sectors. Even though climate proofing of energy assets has been identified as a priority, important knowledge gaps still remain in this area (EEA, Dec 2019).

A 2017 report prepared for the European Commission indicated that there is a need for more detailed information on extreme weather events and their impacts on energy transmission and distribution networks, as well on how climate change will affect weather patterns in the long run. There are also gaps in the understanding of how disasters and climate change will impact renewable energy sources, as well as the potential environmental impacts of the increasing demand for water for cooling. The report includes a list of the most common structural and non-structural measures considered by governments for tackling these challenges; these include awareness-raising, building and improving dams and coastal and river defences, strengthening standards, training, installation of micro- and underground grids, and introducing green elements in water management. Countries have adopted different approaches to assessing climate and disaster impacts. The majority conduct vulnerability assessments, but risk assessments and a combination of the two approaches are also evident (Hendel-Blackford et al., 2017).

Jason Blackeye/Unsplash.com

COUNTRY EXAMPLES

THE NETHERLANDS

In the Netherlands, the Ministry of Infrastructure and Water Management has engaged a number of public and private stakeholders in conducting assessment studies and planning for adaptation strategies. As a result of the collaboration, vulnerabilities in the energy sector have been identified – namely, the potential adverse effects of extreme heat and droughts, as well as a rise in sea levels and subsequent flooding. Climate change is expected to create challenges for the operation of cooling systems for energy assets and the ICTs that support them. The Netherlands Environmental Assessment Agency has constructed an energy vulnerability matrix, which takes into consideration the cascading impacts of power disturbances (EEA, Dec 2019).

SPAIN & UK

Spain and the UK have also conducted assessment reviews. Spain concluded that water resources are of significant importance for the continued supply of energy in the country and a number of adaptation measures have been suggested. The leading body in this area, the Spanish Office of Climate Change (OECC), under the Ministry for Ecological Transition, collaborated with academia in conducting the assessment. The multisectoral review in the UK showed that the energy sector in the country is threatened by possible increases in strong winds, storms, high waves and flooding. The review is conducted every five years by the Department for Environment, Food and Rural Affairs, in accordance with the 2008 Climate Change Act (EEA, Dec 2019).

ROMANIA

Romania has released an Integrated National Energy and Climate Change Plan (2021-2030) that sets out a number of priority areas, taking into consideration man-made, natural and climate change-induced risks. In Romania's Energy Strategy for 2019-2030, the protection of critical infrastructure for energy in the event of natural disasters is designated as a medium-level priority. This includes monitoring and maintenance of the whole energy grid and performing upgrades to ensure adherence with safety standards for critical assets (lakes, dams, dykes, etc.). In its National Action Plan to Implement the National Strategy on Climate Change and Economic Growth Based on a Low-Carbon Economy for the Period 2016-2020, the government has designated developing capacities for monitoring potentially hazardous events and strengthening emergency management systems as high-priority operational objectives (Government of Romania, 2018).

MOLDOVA

In 2009, the Government of Moldova proposed working with Romania and Ukraine on a joint project to improve hazard prevention and crisis management policies in the shared Danube River Delta. The project was funded by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety in 2010. At the end of the project a Danube Delta joint contingency plan was developed, which included

procedures for mutual assistance and joint training of participants. Procedures for early detection and notification of hazardous events, as well as Safety Guidelines and Good Industry Practices for Oil Terminals were also established between the three countries. Policies and measures for the prevention of and preparedness for industrial accidents with national or transboundary impacts were also considered (UMWELTBUNDESAMT and UNECE, 2016).

GERMANY

Germany has a good record of ensuring the safety of energy supplies and has adopted legislation that obligates private companies to secure reliable and high-performance supply networks. In line with the Energy Industry Act, it carries out regular technical checks and monitoring reports (DE Federal Ministry of the Interior, 2009).

ESTONIA

Estonia is relatively unique in that it is among the biggest producers of oil shale in the world, which makes it the most energy independent country in the region. Energy production is operated by private companies, which are responsible for the management and safety of the assets and systems. For these companies, the major threats to uninterrupted operations are extreme weather conditions, strong winds and flooding, as well as cyber-attacks. To tackle these challenges some companies have installed protection devices and fences, as well as firewalls for their IT systems. Still, there are fears that if several technical failures occur consecutively, or in the event of a successful cyber-attack, the whole network could fail. In an emergency, national institutions could intervene. The Estonian Information System Authority (CERT) could respond in the event of cyber-attacks. Companies also need to coordinate with other State bodies, such as government-level crisis management teams, consisting of experts from different ministries (Melchiorre, 2018).

ITALY

Italy has installed smart grids across the country, incorporating new technologies capable of outage monitoring and detection. In 2004, the Italian Authority for Electricity and Gas approved a Grid Code, which can be applied in emergencies. The Code is subject to periodic update as per its provisions. Complex emergencies with cascading failures are also considered in the document. The sector is regulated by several ministerial bodies and public-private companies, each with specific responsibilities. Private operators work closely with the relevant public bodies. Interruptions to the operation of the supporting ICT systems have been identified as the biggest risk for the energy sector. A Security Operation Centre is responsible for managing cyber risks. Emergencies are dealt with on a case-by-case basis depending on the nature of the threat. In the event of a disaster, the civil protection authorities can intervene. There is, however, a need for clearer and less complex legislation to improve the speed and quality of PPP projects (Melchiorre, 2018).

Energy infrastructure in South-East and Eastern Europe, Central Asia and the South Caucasus is largely inherited from the Soviet era and is, in many instances, operating beyond its intended lifetime and designed purpose. The effects of this were seen, for example, in 2013, when Albania and Montenegro reported energy transmission and transportation losses of approximately 33 per cent and 21 per cent respectively. However, with the support of regional cooperation initiatives such as the Energy Community (established by the EU in cooperation with Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, Serbia, Moldova, Ukraine and Georgia) these countries and territories have made steps towards developing National Energy and Climate Plans and have committed to transposing EU energy-related regulations into national legislation (Nabiyeva, 2018).

In Central Asia, the much-needed development and upgrading of energy infrastructure is hampered by a lack of resources and the prevalence of limited, inadequate or out-dated standards for protection and maintenance. In 2003, in an endeavour to improve the safety of assets, NATO's Disaster Response Coordination Centre organized and conducted a civil protection exercise in the Fergana Valley with partner nations in the region. The exercise included a simulated response to a combined earthquake, flooding and landslide scenario. However, investments and efforts at the policy and strategy levels are still lacking (Arteaga, 2010).

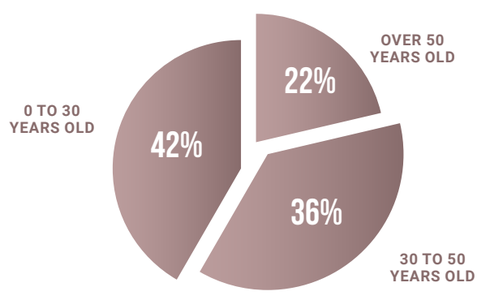
Peter Gudella/Shutterstock.com

WATER SECTOR

Water networks are usually natural monopolies with a single operator as construction costs are very high and the duplication of services is not economically viable. In the majority of EU Member States, water infrastructure is managed by the State and is operated by public or public-private bodies (EC, 2016). In some countries, private or semi-private companies participate in certain services, often in wastewater treatment (Smart Water Magazine, January 2020).

Water is not considered a critical asset in Greece, Israel, Italy, Portugal, Slovenia, Sweden and Turkey; however, dams and flood defences are considered critical infrastructure in Austria, the Czech Republic, France, Israel, Italy, the Netherlands, Norway, Slovenia and Turkey (OECD, 2019).
In May 2020, the EU Commission urged Sweden, Belgium and Greece to fully comply with Directive 91/271/EEC on the management of urban wastewater (which has been transposed into the national legislation of these countries) as assessments showed that parts of their territories were not collecting and treating wastewater properly before discharging it into the environment (Smart Water Magazine, 2020). A 2015 official document of the European Commission reported that, while the majority of EU Member States have developed new preliminary flood risk assessments, only about one third have explicitly taken into consideration the long-term impacts of climate change or socioeconomic pressures in their assessments (EC, 2015). That said, all EU Member States and Norway have adopted River Basin Management Plans in line with EU regulations (EC, 2019).

Studies have found that about 25 per cent of water supplied to the grid in London is lost in the water network. In Norway, this figure is as high as 32 per cent and is even higher in Italy. The high losses in Italy are, to a large extent, due to the ageing infrastructure: of the approximately 337,453 kms of water networks, 74,240 kms are more than 50 years-old, and 121,483 kms are 30 to 50 years-old. The monitoring of water losses is only done over a limited area of the network. In 2019, the Italian Government allocated €400 million for a ten-year period for water infrastructure projects to improve the technical quality of the networks (Toso, 2019).



COUNTRY EXAMPLES

MOLDOVA

In a 2013 report, the European Investment Bank noted that only 45 per cent of Moldova's population had access to clean drinking water and that wastewater was discharged into the environment without any prior treatment. The EU has funded projects to improve the quality of drinking and wastewater in the country, as well as to replace ageing water pumps and equipment (EIB, 2013). In 2019, Romania received €135 million from the EU to invest in improving the quality of drinking water and the operation of its waste management system, which will benefit close to 380,000 people living in the Timiș County area (Smart Water Magazine, 2019).

GREECE

In Greece, Drought and Water Scarcity Management Plans were developed to accompany their River Basin Management Plans. The country, however, reported that the River Basin Management Plans were often based on unclear or out-dated assessment techniques, and the approaches in the different plans varied. Water management was the responsibility of a number of different bodies, each focusing on a specific aspect of the process, with little coordination of their activities. Some of these bodies are understaffed and lack the capacity to execute their responsibilities. The risk of flooding is lacking in the plans but some targeted measures have been envisaged, relating predominantly to dam infrastructure. The potential adverse impacts of climate change have also not been properly reflected in the plans. In 2016, Greece adopted a National Climate Change Adaptation Strategy, which it hoped will improve the development of adaptation measures and their implementation (EC, 2018)

NORTH MACEDONIA

North Macedonia has experienced a number of breakdowns and leakages in its wastewater infrastructure due to its ageing assets. This has resulted in the contamination of rivers and water sources, impacting the environment and the daily lives of residents in the affected areas. New sewage systems and the construction of several wastewater treatment facilities have been planned and are being executed (NIRAS, 2020). The ageing water pipes are also affecting the drinking water supply systems, and increasing temperatures could undermine water availability. That said, currently North Macedonia is one of the few countries in the world that has the capacity to meet the water and sanitation needs of its entire urban population (Khalid, 2017).

BELGIUM

In 2015, Belgium reported that one of its major outstanding issues was the lack of coordination between its different regions. The regions are expected to consult and report to each other but, at times, communication is slow and local regulations can differ from one region to another. A more positive approach was adopted in the Flanders region with an initiative to engage the public and interested parties in the process of planning and drafting their River Basin Management Plan (as per EU requirements). The information was shared in newspaper articles and via radio and television and was made available in town halls with opportunities for residents to leave comments. In the Brussels and Walloon regions similar information was shared via posters and news outlets. Water scarcity and droughts as a result of climate change are touched upon in the local management plans but clear measures are lacking. All regions, however, have adopted regulations in relation to flood risk management (EC, March 2015).

GERMANY & AUSTRIA

Under German legislation, water suppliers are obliged to take measures in response to crisis situations in order to protect water networks. The Water Security Act and the 2016 Concept for Civil Defence of Germany also include clauses for the protection of water supplies in the event of civil emergencies. In Austria, a set of recommendations for water supply management in times of crises was developed in 2017 by the Austrian Association for Gas and Water. However, preliminary planning and preparedness measures appear to be lacking. Even though water supply services in Germany and Austria are considered very reliable and of a high standard, an incident in 2016 in Simbach am Inn on the border between the two countries showed how a lack of preparedness measures can lead to disastrous results. Heavy rainfall on the first day of June lead to a clogged pipe and the bursting of a dam. The resulting wave flooded large areas, causing an electricity blackout that affected 8,000 households, as well as disruptions to the drinking water supply (Bross et al., 2019).

GERMANY

In 2017, the German Federal Office for Information Security (BSI) introduced Germany's first security standard for operating water supply and waste management critical infrastructure, linking obligations under its IT Security Act of 2015 with the water sector (OneTrust DataGuidance, 2017). Indeed, ensuring cyber security for the continued operation of water systems and networks is now a priority for the majority of countries in the region.

Central Asia and areas of the Caucasus are highly dependent on snow and glacier melt for freshwater supplies. Changes in the water supply triggered by a warming climate could have significant implications for irrigation and hydropower energy generation. It is possible that by 2080 a reduction in the amount of rainfall could lead to insufficient quantities of water for consumption and services in the Caucasus. In 2016, the Centre for Emergency Situations and Disaster Risk Reduction (CESDRR) for Central Asia and the South Caucasus was established to facilitate coordinated planning and efforts in developing preparedness and response measures. At the national level, the countries of the region have all recognized the need to modernize their policies and infrastructure, as well as to incorporate climate change mitigation measures in policy and planning. Kazakhstan has adopted a water resources management strategy up to 2020, an Integrated Water Resources Management and Water Efficiency programme for 2008-2025, and, most recently, a Water Management Programme for 2020-2030. In Armenia, Water User Associations, established in 2002, have helped to improve the efficiency of irrigation networks in the country (SDC, 2019).

ErichFend/Shutterstock.com

TRANSPORT SECTOR

The UN Economic Commission for Europe (UNECE) has warned that rising sea levels, coastal flooding, storm surges and high waves could have significant negative consequences for transport infrastructure in north-western Europe and along the Baltic Sea. Coastal flooding could also damage ports and cargo areas, impacting supply chains for long periods of time. It is estimated that by 2100, in a 1-metre sea level rise scenario, over 60 per cent of seaports in coastal EU countries could be at risk of inundation. In fact, by as early as 2030, about 50 per cent of EU seaports (particularly along the North Sea coast) could be at risk and by 2080 seaports in Greece, the UK and Denmark may be severely impacted (UNECE, 2020).

However, there is still a lack of data on how climate change induced disasters and sudden events could impact the transport sector in the future. For example, flash floods in mountainous regions represent a serious threat to transportation, especially in less-developed areas, but an understanding of the changing nature of climate hazards is still at an early stage. There is also a need for a better understanding of the use of intermodal shifts as a coping mechanism in the event of an emergency. This means, for instance, increasing the capacity of railway networks when road infrastructure is damaged or inaccessible due to a weather event. Research has shown that the potential for integrating disaster risk reduction and climate change considerations into existing policies, regulations, training and maintenance procedures has not been thoroughly realized. The role of governments is particularly important as setting standards and requirements in legislation can lead to important improvements. In France, following a vulnerability review requested by the government, 800 standards for roads alone were scheduled for revision (Hendel-Blackford et. al., 2017).

After the economic crisis of 2008, much needed investment in transport infrastructure has been largely lacking across the region. Road and rail transport in most of Europe continues to degrade due to a lack of maintenance. Against this background, the increasing need for upgrading existing and developing new infrastructure to accommodate the emergence of alternative fuels poses an additional challenge. Recent innovative models for transport sharing are also creating new threats for the safety and security of passengers and goods in times of crisis (Pastori et al., 2018).

In Eastern Europe, roads and railways still suffer from a lack of timely interventions, or in places infrastructure is missing. In Greece, Spain, France, Italy and Portugal upgrades and improvements in port facilities and services, as well as in port connections by rail and inland waterways, have been identified as a pressing need. Spain and Portugal have prioritized the development and upgrading of railways and freight rail transport. Inland waterway transportation in Germany, Belgium, France and the Netherlands is in need of modernization. The EU is considering shifting about 30 per cent of road freight to greener types of transport such as railways, but currently the freight railway infrastructure is, to a large extent, inadequate; cross-border interoperability is also an ongoing issue (Pastori et al., 2018).

COUNTRY EXAMPLES

AUSTRIA

In Austria, 1,500 km of the 6,000 km of railway tracks have been assessed as vulnerable to disasters. Over a period of 21 years, between 1990 and 2011, approximately 1,200 weather-related events adversely affected transport infrastructure in the country. As set out in legislation, ÖBB – the national railway operator – is responsible for the construction and management of the railway network. Since 2005, ÖBB has had a special department dealing with disaster management (initially the Department of Natural Hazard Management and, since 2015, the Geotechnics and Natural Hazard Management Department), which produces hazard maps and develops preventative measures. The operator also has its own meteorological stations and has established a weather warning system. ÖBB has been used as an example of good practice for other operators in Europe. However, despite these efforts, several disasters have caused significant damage, such as the flooding and landslides in June 2013 in the northern Alps following heavy rainfall. Travel in several areas was temporarily halted because of damaged tracks. The subsequent reconstruction of the railway system cost approximately €75 million (Otto et al., 2018).

ITALY

In August 2018, a large section of the Morandi Bridge in Genoa collapsed, killing 43 people and causing damage to vehicles and buildings below and nearby. The area was hit by a storm and, according to witnesses, lightning struck the bridge; however, none of these events would normally be a reason for such a structure to collapse. Following an investigation it became clear that the disaster was the result of a combination of elements – from poor engineering and design in the first place, to the poor quality of materials used for the construction of the bridge, the age of the structure, and the lack of maintenance by the private company operating this section of the road. The authorities had been aware of problems with the bridge for years before the incident occurred and repairs had been carried out but these were unable to fix the underlying issues. Between 2007 and 2015, Italy (together with Spain) had the lowest levels of infrastructure spending among the major European countries. Around 300 bridges in the country are at a risk of collapse but a lack of centralized information makes it difficult to estimate the total amount of infrastructure at risk. A report by the EU also noted that underinvestment and a weak competitive framework also hamper improvements in railways and ports (Pollock, 2018; Drzik, 2019; EC, March 2019).

Luca Rei/Shutterstock.com

SERBIA

Droughts in 2012 and severe floods in 2014 illustrated the vulnerability of infrastructure in Serbia. An assessment of the country's policies for disaster management and climate change adaptation in the transport sector noted that climate change adaptation is only sporadically referred to (and only by a few experts working for infrastructure operators) and that there was no clear mechanism for investment planning for critical locations. Guidelines for tackling geo-hazards affecting road networks have been set out in legislation and have recently been updated to comply with EU standards but the implementation of measures is hampered by a lack of funding. The lack of coordination and cooperation between central and local levels of administration has also been identified as an issue. The Global Facility for Disaster Reduction and Recovery (GFDRR) has been assisting Serbia in mainstreaming climate change adaptation in road transport and in improving the capacities of relevant stakeholders (World Bank, 2018).

POLAND

In Poland, road networks have improved but continuous changes in the construction programmes and funding have been problematic. Most notably, the northern regions of the country have been somewhat neglected even though traffic needs have soared. In the railway sector, planned investment projects were not expected to meet the original targets set for 2023, even prior to the COVID 19 pandemic. However, Poland has paid some attention to the impacts of climate change on transport infrastructure, in line with the Polish National Strategy for Adaptation to Climate Change, adopted in 2013. It has conducted sensitivity, vulnerability and risk analyses to identify areas at risk of flooding, compiling the results on GIS maps. The Ministry of Environment has also been working with local authorities in 44 cities with more than 100,000 residents to develop climate change adaptation strategies, within the framework of the 'Development of Urban Adaptation Plans for cities' project (EC, March 2019; UNECE, 2020).

GERMANY

A 2019 EU report concluded that, while the quality of the transport system in Germany is generally high, there are a number of risks to the sector. Rising traffic congestion (Germany is a major transit country) and the lack of long-term political and financial commitment to upgrade cross-border infrastructure (especially railways) could undermine the ability to upgrade assets to meet future needs in line with climate change commitments. Germany has, however, put a great deal of effort into researching the potential impacts of climate change on the different types of transport infrastructure, in line with the German Strategy for Adaptation to Climate Change, released in 2008. The Strategy envisages adaptation measures to tackle both the adverse impacts of climate change and the increase in the number of extreme events. Since 2016, experts from seven departmental research institutes have joined forces to work on an 'Adapting transport and infrastructure to climate change and extreme weather events' programme, covering railway, waterways and roads. The integrated climate impact assessments are used as a basis for the development and adjustment of policies, regulations and standards for the country (EC, March 2019; UNECE, 2020).

ROMANIA

In Romania, the general condition and reliability of road and train infrastructure in the country is poor. The implementation of plans and strategies for upgrading road infrastructure remains slow, even though investment has been made available. In Hungary, the general quality of roads and railway infrastructure was assessed as high but regulations for inland water navigation on the Danube river have resulted in delays in transportation and increased operational costs (EC, March 2019).

Unlike other EU Member States, Estonia does not consider transportation as critical infrastructure (OECD, 2019).

Avigator Fortuner/Shutterstock.com

ICT SECTOR

In the past, telecom services were largely divided among various platforms or operators – for instance, voice telephony and online computer connections were often operated by different business systems and were therefore regulated under different legislation and by different regulators. However, with the development of Internet technologies and AI, services have become inseparable and companies have started to provide the whole set of systems and enter new business markets (EC, 2009). Large private companies have taken over a significant portion of the sector and European legislators and regulators have been debating the required level of regulation. The choices are usually between full de-regulation or continued selective regulation. Under the second option, the question is which areas would benefit most from continued regulation (Serentschy, 2015). While discussions revolve primarily around requirements for market entry and cyber security, the coordinated protection of national and cross-border ICT assets and services against disasters and climate impacts remains an under-unexplored area. This, however, could be one of the areas that would benefit from continued regulation.

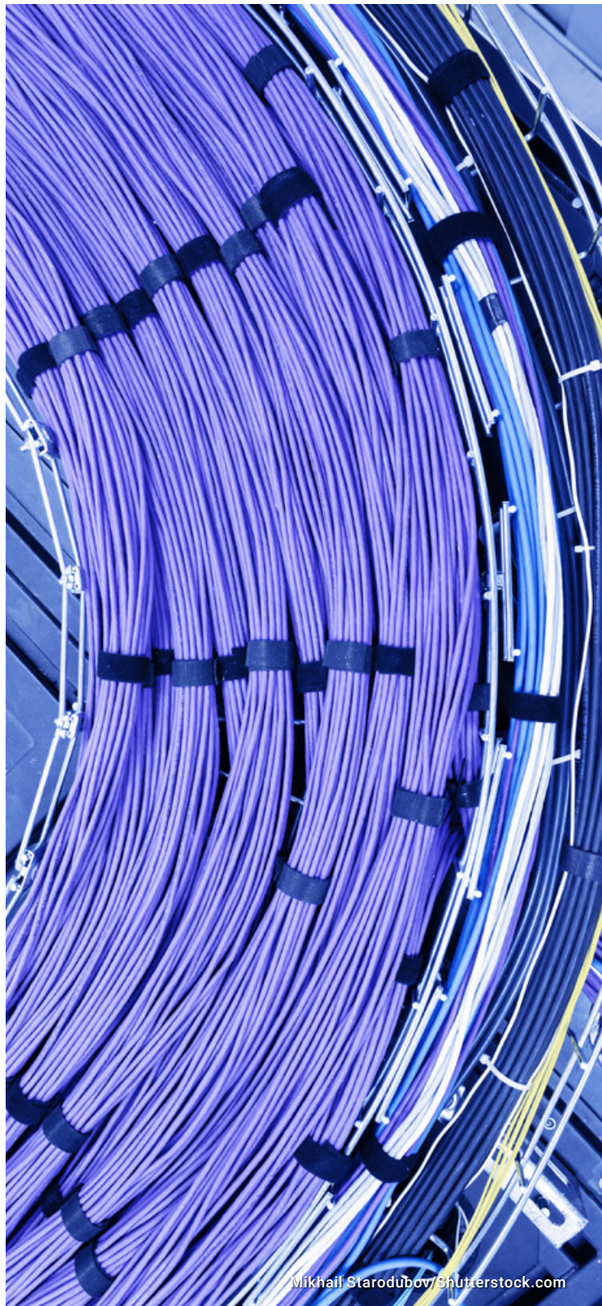
In terms of investment in the sector, a recent report by the European Telecommunications Network Operators' Association (ETNO) noted that per capita investments in European networks are much lower than their large international peers (Japan, US and South Korea): €89 per person in Europe compared to €177 in the others. That said, ETNO member companies invest heavily in infrastructure and, in the past two years, significant investments have shifted towards building fixed assets. The introduction of 5G is expected to require more infrastructure across the region and the sharing of assets among operators to avoid duplication of costs. This means that the approach to legal frameworks and contracts for such agreements will be of great importance to the way infrastructure operates and responds to emergencies (ETNO, 2020).

One positive development in the ICT sector is that European networks are steadily becoming greener, with overall carbon emissions decreasing in line with efforts to meet climate targets. The energy demand from the telecom sector has been increasing by approximately 5 per cent per year; however, by 2019, close to 50 per cent of the energy used by ETNO companies was derived from renewable sources. The Swedish Telia Company, which operates in both Europe and Central Asia, has pledged to reach carbon neutrality by 2030, not only in its operations but also in its supply chain. The Norwegian Telenor, which is a multinational provider, has dedicated 110,000 person-hours for training for supply chain sustainability (ETNO, 2020).

In the area of cyber security, majority of countries in Europe and Central Asia have established designated bodies and national computer emergency response teams (CERTs) or national computer security incident response teams (CSIRTs). EU Member States are also part of a network, which supports national cyber-security teams and facilitates cooperation between country teams within the Union. The CSIRT network cooperates closely with the EU energy sector and the Industrial Control Systems (ICSs) community. ICSs, including SCADA (Supervisory Control and Data Acquisition) systems, are used in the energy, water treatment, transportation, chemical and other industries. Since 2017, all EU Member States have published national cyber-security strategies (ENISA website, 2020). The majority of EU Members have also opted for an all-hazards approach in designing their national cyber-security strategies (ENISA, 2016).

Cyber security predominantly falls under the provisions of the national security legislation of individual countries and is increasingly being linked to the protection of critical infrastructure. That said, even though the Sendai Framework calls for protection from man-made and technological threats, cyber risks are still not considered in the national disaster risk reduction strategies of a number of countries. There is, as yet, little understanding of the linkages between cyber risks, critical infrastructure protection, climate change impacts and disaster management (UNDRR (cyber), 2020).

The majority of countries have developed National Cyber Security Strategies but gaps relating to national capabilities, cross-border and regional coordination, and the definition of terms for private sector involvement still remain (ENISA, 2015). Even though governments have the primary responsibility for ICT infrastructure, it is often the case that public administrations lack the expertise, resources and/or authority to perform ICT oversight functions to the required level. Information sharing on vulnerabilities is also obstructed by issues of trust or because it may go against the commercial interests of the private businesses involved (Melchiorre, 2018; ENISA, 2016).


Mikhail Starodubov/Shutterstock.com

COUNTRY EXAMPLES

FINLAND

Levels of progress in the ICT sector vary across countries in the region. Finland's ICT sector is relatively large compared to other European nations, and the country has pioneered a number of breakthroughs in both the Internet and mobile technology domains (Millar, 2015). The majority of critical assets in the country are managed by private companies and have equal responsibility. National legislation obliges operators of critical infrastructure to take risk protection measures, to conduct risk assessments and notify the authorities of security incidents but there are still some gaps in the mechanisms for protecting critical information infrastructure. Private businesses are also largely responsible for providing cyber security services and technical expertise. The 2019 Cyber Security Strategy of Finland states that cyber security should be the prerogative of all public authorities and organizations, as well as the private businesses operating critical infrastructure. The Strategy aims to support coordination between the various parties. It envisages the establishment of a Cyber Security Director within the Ministry of Transport and Communications responsible for coordinating the development of cyber security measures. A 24/7 Cyber Security Centre provides situational analyses to designated authorities and private companies to improve readiness and preparedness against cyber threats. (Finland Security Committee, 2019; ENISA, 2015; Gjesvik, 2019).

UK

In contrast with Finland's 'all-of-society' approach, the UK follows a more centralized approach. The lead body in this area is the Office of Cyber Security, a body within the UK Government Cabinet Office. It is responsible for developing the national strategy and policies, while the National Cyber Security Centre provides oversight for the activities of the different infrastructure operators and serves as a 'one-stop-shop' for cyber incidents within civilian networks (Gjesvik, 2019). Compliance with the UK's Sector Resilience Plans and industry-specific infrastructure design standards ensures the resilience of communications infrastructure. The plans and standards, which are updated regularly, take account of natural hazards and climate change impacts. Telecoms and broadcasting are regulated by economic regulators, who support the inclusion of resilience measures and build response capacities in the sector. ICT providers are not economically regulated; cooperation and coordination with governmental bodies in advance of emergencies is encouraged on a voluntary basis. In 2011, the Cabinet Office issued guidelines to improve the resilience of critical infrastructure and services in the UK but cyber threats were not included in the guidance. Instead, cyber risks are outlined in the National Risk Register (Cabinet Office, 2011).

FRANCE

France aims has adopted a number of legislations and laws defining its role in ensuring safe international digital spaces; this includes the International Digital Strategy from 2017, as well as guidelines and best practices, which it shares with its partners. The French Network and Information Security Agency (ANSSI), established in 2009 under the General Secretariat for Defence and National Security, is the lead body for coordinating cyber security efforts. The Agency sets minimum cyber security standards and requirements for both public and private operators, who are obliged to report cyber security incidents to the Agency and undergo cyber security audits, conducted either by ANSSI or by service providers accredited by ANSSI. The Agency is also responsible for categorizing assets by level of criticality and for developing sector-specific cyber security standards and guidelines. France is among the few countries in the region to adopt such a detailed and targeted approach. In 2013, ANSSI proposed a Critical Information Infrastructure Protection law, which establishes a common minimal level of cyber security for 12 critical infrastructure sectors and which links with the nation's critical infrastructure protection plan (CIP) (Instruction générale interministérielle relative à la sécurité des activités d'importance vitale). The CIP identifies critical sectors in the country and recognizes the threats posed by natural and man-made hazards (ENISA, 2015; BSA, 2015; ANSSI, 2020; UNIDIR, 2020).

BULGARIA

Bulgaria has a stable and growing ICT sector, with more than 10,000 ICT companies, of which 70 per cent export their services outside of the country (US Department of Commerce website, 2019). In its National Cyber Security Strategy, adopted in 2016, Bulgaria has underlined the need for periodic risk assessments to improve coordination, preparedness and response to different threats, as well as the need for developing a coherent vision and strategy for comprehensive cyber resilience. The Strategy also recognizes that the regulatory framework and mechanisms require further improvements in order to attain a higher level of security. The document notes that policies and measures should take into consideration not only known but also unknown and unpredictable threats and be flexible enough to adapt to sudden emergencies (Bulgarian Council of Ministers, 2016). A 2015 assessment noted that the cyber security regulatory framework was still limited and that there were no formalized PPPs (BSA, 2015). The full implementation of the strategy is yet to be realized. In 2018, a Cyber Security Act was adopted, which sets requirements for all operators of critical infrastructure to implement basic cyber security and standards in line with transposed EU legislation. Failure to comply could result in penalties (Kinstellar, 2018).

LATVIA

The cyber security strategy for Latvia, adopted in 2014, includes clear objectives and implementation timelines, and is backed up by a strong legal framework. The 2010 Law on Security of Information Technology defines the roles and responsibilities of Latvia's National Computer Emergency Response Team (CERT.LV). The 2014-2018 Cyber Security Strategy envisages an 'all-of-society' approach, where all ICT users, managers and legislators have an understanding of the basic principles of cyber security. The Strategy also identifies three important dimensions: infrastructure, services and processes. As per the regulations, the Cabinet of Ministers has to review the status of information critical to infrastructure annually. Representatives of critical assets are regularly involved in training, organized by CERT.LV. The protection of information infrastructure falls under the regulations for the protection of all national critical infrastructure, as detailed in the National Security Law (the law does not designate specific sectors as critical but rather considers any infrastructure that meets the criteria for criticality), and under the 2011 Law on the Security of Information Technologies. There is no explicit acknowledgement of the threats posed by climate change or disasters but a rather broad mention of 'dangers' (BSA, 2015; UNIDIR, 2020; ENISA, 2015; MoD Latvia, 2014).

In recent years, the main focus in the sector has been on cyber security but the current COVID-19 health crisis has reminded countries of the importance of other ICT assets. The crisis has revealed the vulnerabilities of telecommunication networks and the need for resilient telecom services and digital infrastructure. User demands have outpaced network capacities, prompting telecom operators and private companies to reduce their services to prevent outages and secure the operation of lifeline services such as emergency phone numbers. Vodafone has reported a 50 per cent increase in mobile traffic, BT 60 per cent and Nokia a 40 per cent increase. These developments have prompted a number of governments to classify electronic communications services as critical assets (CMS Law-Now, 2020).

Some governments have taken measures to respond to the pandemic. The Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) has recommended that certain online services run at a lower speed to preserve traffic speed for essential information outlets such as government information portals. However, operators have the final decision on whether they follow the recommendation or not. In Spain, special emergency measures oblige telecom providers to continue services for all end users for the duration of the crisis even if payments cease, thus protecting the public interest. The requirements have been extended to providers that were not previously considered critical but have now become essential. As a result of the health crisis, the planned introduction and installation of 5G infrastructure across Europe has been postponed (CMS Law Now, 2020).

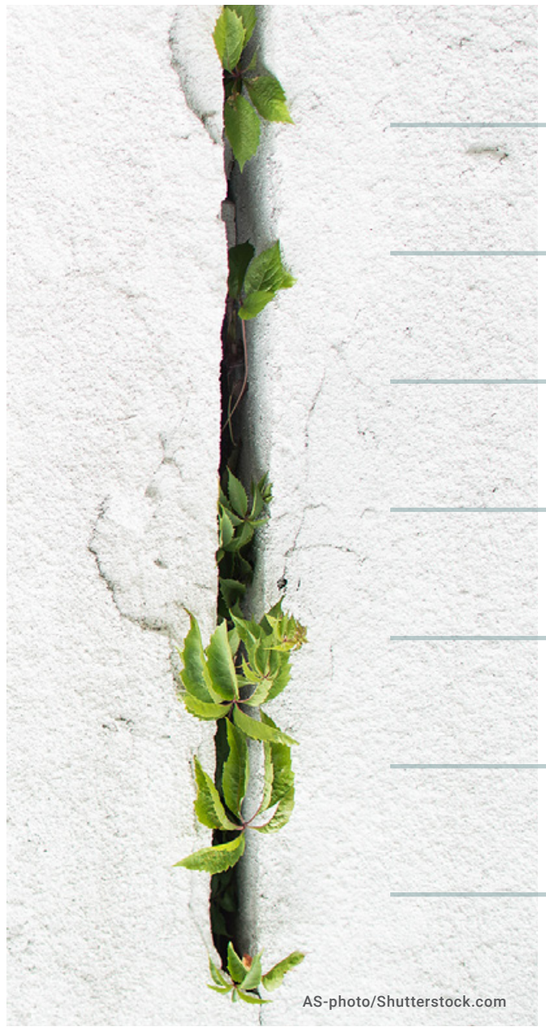
4 RECOMMENDATIONS AND THE WAY FORWARD

Kristopher Roller/Unsplash.com

4
RECOMMENDATIONS AND THE WAY FORWARD

The sections above detail a number of important steps that countries in Europe and Central Asia have taken to include resilience in their critical infrastructure protection policies.

At the same time, the desk review highlights areas that require immediate action by infrastructure regulators and policymakers:


AS-photo/Shutterstock.com

- **ESTABLISH** a national definition for 'resilient infrastructure'.
- **INCORPORATE AND LINK** infrastructure resilience in national and local disaster risk reduction strategies.
- **DEVELOP** a better understanding of inter-dependencies, interaction and connectedness of infrastructure systems.
- **IMPROVE** coordination at different levels and among all relevant parties.
- **ACTIVELY ENGAGE AND CREATE** incentives for private sector participation supported by risk-based performance.
- **FACILITATE** the collection of risk data and make disclosure of information on climate disaster risks mandatory.
- **ENHANCE** knowledge and build capacity.

ESTABLISH A NATIONAL DEFINITION FOR 'RESILIENT INFRASTRUCTURE'. Such a definition should include critical, essential, digital, distributed and natural forms of infrastructure, should be based on multi-hazard understanding allowing inclusion of new and evolving risks, and should institute climate change adaptation and disaster risk resilience as a baseline requirement. For infrastructure to be classified as resilient, climate change and disaster risk reduction measures should be an explicit requirement for investors and owners/operators.

At the regional level there is the need for establishing common approaches for risk assessment and management, and standardized procedures among countries in the region, based on data produced at the national-local level. Assessments should be conducted to delineate areas where regional action is preferred and where national competence is more appropriate, reflecting differences in the scale of risks and specificities of the different sectors (CEPS, 2010).

INCORPORATE AND LINK INFRASTRUCTURE RESILIENCE IN NATIONAL AND LOCAL DISASTER RISK REDUCTION STRATEGIES. At the national and local level, governments need to devise long-term strategies, in coordination with regulators, asset owners and other relevant parties, and develop resilience standards for a common framework. Risk assessments and stress tests should be conducted at regular intervals to ensure that assets and services meet established resilience standards. Such exercises will test the vulnerability of systems and inform and improve decision-making processes. For instance, standards could be updated at regular intervals

Critical infrastructure usually undergoes load testing. Procurement contracts, tenders and its technical specifications detail the methodologies for conducting these tests. To ensure that all essential infrastructure is operating appropriately, at all times and under all conditions, these test methodologies need to include potential shocks and stress factors that could be induced from both climate and geophysical hazards in their design, development, installation/construction, operation, maintenance and renewal. To this end, all financial instruments should incorporate a robust screening process to ensure that investments are resilient to future disaster and climate risk. (UNDRR 2020).

DEVELOP A BETTER UNDERSTANDING OF INTER-DEPENDENCIES, INTERACTION AND CONNECTEDNESS OF INFRASTRUCTURE SYSTEMS: Given the fluctuating and systematic nature of risk, there needs to be frequent assessment of what constitutes 'critical' infrastructure in any given locality or system. These assessments need to be based on an understanding of the inter-linkages between critical infrastructure assets, with a view, in particular, to potential cascading impacts.

One of the main challenges for critical infrastructure resilience is the connectivity and interdependence within and between systems, which makes them vulnerable to cascading failures (Heinimann and Hatfield, 2017). Some critical infrastructures are so interconnected and interdependent that disruption of one asset has the ability to impair the efficiency of numerous other critical assets.

Bilanol/Shutterstock.com

To increase the resilience of infrastructure investments it is essential to monitor and measure their vulnerability, sensi¬tivity, interdependency and exposure to risk. This shift requires investors, operators and decision makers to make sure that disaster and climate risks are considered in the location, design, construction and operation of planned infrastructure investments. Equally, in-frastructure regulators and operators need to develop and make use of indicators that encourage 'systems thinking' to take account of the complexity and interdependencies of global dyna¬mics and patterns of change (Lonsdale et al., 2015).

The absence of adequate detail on these linkages and interdependencies, largely due to the lack of prior experience and records of past events, is often highlighted as a major challenge in addressing the resilience of critical infrastructure (Chang et al., 2014). Understanding the nature of system interdependencies and evolving vulnerabilities will play a vital role in dealing with the likelihood and consequences of cascading failures in interdependent systems, particularly in the design of resilient infrastructure (Vespignani, 2010). The scale of systemic risk that stems from the increasing vulnerability of infrastructure systems at national or local levels is still not fully recognized (UNDRR, 2020). As suggested by Panda and Bower (2020), there is a need for holistic risk assessments that take into account all possible scenarios, hazards and vulnerabilities, their direct and indirect impacts, and the exposure to and awareness of potential sources as the basis for reducing risk from natural and technological hazards.

In 2020, the UK National Infrastructure Commission published a new framework for infrastructure resilience that aims to assist operators in improving their mechanisms for adaptation and recovery from shocks and climate change. The framework places great importance on resilience standards, which need to be "clear, proportionate and realistic". The development and monitoring of the implementation of the standards is the responsibility of the relevant or assigned public authority, to ensure that public and national interests are best served. The standards have to be transparent and based on a realistic assessment of the cost of response capacities for different systems.
The framework determines six key aspects of resilience for energy, water, digital, road and rail services: anticipate, resist, absorb, recover, adapt and transform. In the 'anticipate' phase, authorities should collect information on the condition of existing infrastructure and pinpoint gaps and weaknesses. The 'resist' phase involves taking preventative measures, while the 'absorb' phase looks at measures that would lessen the negative impacts of crises in cases where impacts cannot be avoided altogether. The 'transform' phase encourages operators to review and improve their assets and systems to meet new challenges and targets. The framework also recommends that governments publish a full list of resilience standards every five years after completing risk assessments and in discussion with regulators. Both short-term and long-term resilience strategies need to be in place (UK NIC, 2020).

IMPROVE COORDINATION AT DIFFERENT LEVELS AND AMONG ALL RELEVANT PARTIES: Policies and mechanisms need to be designed to suit local geographic and socioeconomic conditions. Disasters and climate change affect local areas in different ways and adaptation mechanisms have to be flexible enough to fit the specific conditions. Therefore, the coordination and cooperation between administrations at the central and local level, as well as with local private sectors, is essential in securing the continued operation of services (WB, 2008). A possible solution for improving the coordination among public authorities and with other stakeholders is the establishment of a multi-ministry body that would take the lead in information exchange and facilitating cooperation. As most countries have existing agencies for disaster risk management or civil protection, these bodies could also take on the responsibility for issues relating to critical infrastructure resilience, drawing expertise from other relevant agencies. Such structures, however, should not take over the responsibilities of the regulators (Hallegatte et al., 2019).

Coordination between different levels and stakeholders could also be improved through raising the risk awareness of local operators and private companies, as well as users; this could be done through targeted programmes and exercises. Such initiatives could also help improve the monitoring of the implementation of measures. For instance, where appropriate, residents could be engaged in community projects, such as developing platforms for reporting on damaged or ageing local infrastructure, or in developing hazard maps. Measures and projects need to set clear goals and be conducted in a transparent way to limit corruption and bad practices. Improving awareness and expertise in this area could be achieved through the development of university courses and investment in education (CEPS, 2010).

On a more strategic level, regulators and policies need to establish clear roles and responsibilities for the management and protection of critical infrastructure assets.

In Poland, a feasibility study was conducted before building a second cargo terminal at the Gdansk Deepwater Container Terminal (DCT). The study recommended that the height of the quay should be based on climate change projections and assessments. To this end, the DCT has been collaborating with the Port Authority in collating information on sea levels and high waves (GAR, 2019; Vallejo and Mullan, 2017).

In France, after repeated heat waves in 2003 and 2006, Électricité de France (EDF) (a predominantly State-owned electric utility company) initiated the 'Great Heats' programme for nuclear power plants, which urges operators to comply with the regulations governing river temperatures, and includes planning for different climate change scenarios. The programme ensured investments in improving cooling equipment and the monitoring of climate change impacts, as well as the periodic revision of safety standards (Vallejo and Mullan, 2017).

fran_kie/Shutterstock.com

ACTIVELY ENGAGE AND CREATE INCENTIVES FOR PRIVATE SECTOR PARTICIPATION SUPPORTED BY RISK-BASED PERFORMANCE.

Covering the costs of improving the resilience of infrastructure is not an easy task. A viable option for cost sharing would be to attract private companies to invest in resilience according to a standards of hazard resistance with pre-defined levels of acceptable risk (e.g. roads should be able to withstand a twenty-year period of heavy rainfall). Resilience beyond this level could be supported by the public sector (Hallegatte et al., 2019). Important public finance investments in resilience could assist in setting an example and a standard for all owners and operators (Melchiorre, 2018) – for example, France incorporated flood resilience measures that went beyond legal requirements as a part of a €30 billion investment project to upgrade the Paris public transport system (OECD, 2019).

Signing preliminary agreements delineating roles, responsibilities and costs could facilitate rapid response and recovery processes. For maintenance, performance-based contracts could oblige owners and operators to develop longer-term strategies and invest in resilience early on, as payments would be linked to the performance of assets (Hallegatte et al., 2019). Governments should also work with credit rating agencies to incorporate explicit resilience elements into assessments and withdraw from credit activities and sectors that cannot meet certain requirements or are highly exposed to climate and natural disaster risk (UNDRR, May 2019).

When discussing risk reduction and adaptation measures with businesses, public bodies need to make it clear that even though projections are constantly being updated, the time, frequency and magnitude of hazardous events cannot always be accurately predicted. This means that mechanisms need to be flexible and that operators should seek solutions that provide good results against as wide a range of potential threats as possible, rather than focus on an optimal solution against a single threat or scenario (Vallejo and Mullan, 2017).

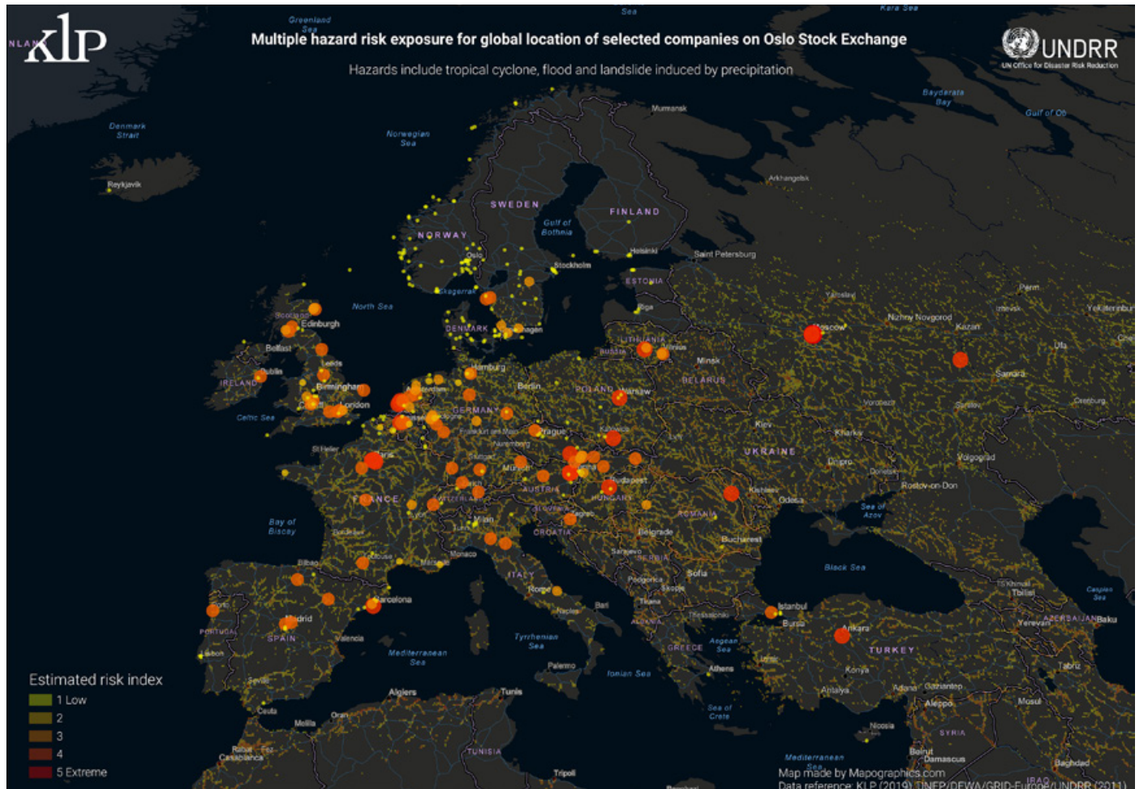
FACILITATE THE COLLECTION OF RISK DATA AND MAKE DISCLOSURE OF INFORMATION ON CLIMATE DISASTER RISKS MANDATORY.

Governments could support the collection of risk data (such as hazard maps) to inform investment decisions and ensure that public safety is taken into consideration. They could also require asset operators to report on physical risks and how they are managed. Public agencies could partner with the insurance sector and with national accounts statisticians to estimate infrastructure investments and capture claims data related to climate impacts and disaster events. Information from risk assessments and stress tests should also be systematically collated to allow for policy adjustments, improved sectoral cooperation and the sharing of best practices (Hallegatte et al., 2019; ADB, 2017; UNDRR, May 2019).

In 2019, UNDRR published a report on opportunities for integrating disaster risk reduction and climate resilience into sustainable finance, outlining 11 areas for consideration and a number of important recommendations. The report recommends that responsible authorities and regulators take measures to increase the transparency of risk data and establish disclosure requirements on disaster and climate risks for investors and assets managers. To ensure that investments are sustainable and account for the resilience of infrastructure, national and local disaster risk reduction and climate change adaptation strategies should be linked to national investment strategies (UNDRR, May 2019).

Governments can make use of a number of existing regional and international resilience guidelines and frameworks for information sharing. UNDRR provides a comprehensive overview of possible steps for integrating resilience into finance in the above-mentioned report and supports countries in fulfilling their commitments to report on the Sendai Framework targets – including target D on damages to critical infrastructure and disruption of services (UNDRR, May 2019).

In addition, regulators and policies need to ensure there are clear rules on liability for faults or negligence – an essential element for ensuring adequate maintenance and functioning of critical infrastructure.



ENHANCE KNOWLEDGE AND BUILD CAPACITY:

Infrastructure development involves multiple stakeholders, all of whom play a critical role. These include the public sector, investors, lenders, contractors, service providers/operators and end users. To attain 'true resilience', it is necessary to improve the knowledge and capacities of all stakeholders. To do this requires awareness-raising, advocacy and training programmes targeting each category of stakeholder across a range of national or local contexts.

Infrastructure development and maintenance will remain the primary responsibility of the State. As such, regulators and national authorities will have to play a role in setting the priorities and sharing these responsibilities with other stakeholders as part of efforts to adopt an 'all-of-society' approach. Capacity development is a central strategy for building resilience and adapting to the changing environment. Understanding the capabilities required for effectively implementing and enforcing standards for multi-hazard disaster risk reduction at national and local level is essential for building the ability of individuals, organizations and societies to successfully manage risks themselves.

This relies not only on training and specialized technical assistance, but also on strengthening the capacities of groups and individuals to recognize and reduce risks within their own communities. This includes sustainable technology transfers, information exchange, network development, management skills, professional linkages and other resources. Capacity development needs to be sustained through institutions that support capacity-building and capacity maintenance as permanent ongoing objectives.

CDRI
Coalition for Disaster Resilient Infrastructure

The Coalition for Disaster Resilient Infrastructure – established in 2019 under the lead of the Government of India – is a recent initiative to promote cooperation and the exchange of best practices between countries. The Coalition connects governments, international organizations, private businesses, academic bodies and development banks, and supports the development and improvement of national policy frameworks to limit disaster-related ecological and socioeconomic losses. As of March 2020, 15 countries have joined the Coalition, including Germany, Italy and the UK (CDRI website, 2020).

TO CONCLUDE

The combination of increasing demands for new and innovative infrastructure and services, on one hand, and the current reality of dangerously outdated assets in Europe and Central Asia, on the other, calls for resilient and more sustainable investment decisions while planning and realizing infrastructure projects. According to a study by the EU Joint Research Centre, damage to infrastructure as a result of disasters and climate change in Europe currently amounts to approximately €9.3 billion annually; this is expected to soar to €19.3 billion by 2050 and €37 billion by 2080 (EU Members, Switzerland, Norway and Iceland are included in the study). The energy and transport sectors will be the most affected, with annual expected damages of €8.2 billion by 2080 for the energy sector and €0.8 billion by the end of the century for the transport sector (EU Science Hub, 2017).

We are now at the stage where we must invest more in building resilience and sustainability into our infrastructure. It will take concentrated and continued efforts on behalf of all stakeholders to reduce the intensity and frequency of disasters caused by natural hazards, however with more resilient infrastructure, it is possible to change the way communities bounce back and recover from cascading disasters. For that a new approach to infrastructure, with increased focus on multi-hazard and co-benefits, will unlock new opportunities, reduce losses, prevent creation of new risk and spur significant economic, environmental and social benefits.

The protection of critical infrastructure and services, and the communities and economies that depend on them, is ultimately a matter of political will. The level of national commitment will determine the ability of countries and the region to 'bounce back from complex emergencies and, ultimately, build societies that are more resilient to future shocks.

The COVID-19 pandemic has demonstrated the consequences of the systematic underinvestment in resilience. The cascading nature of disaster risk, where one disaster can rapidly lead to another, coupled with insufficient investment in disaster risk reduction, means that the critical systems that we rely on for trade, food, energy, transportation and health, are increasingly vulnerable to hazards such as COVID-19.

This crisis is a wakeup call and an unprecedented opportunity to build back better, with a renewed focus on resilience. Alongside COVID-19, there is a more pressing crisis – the climate emergency. Climate change is occurring more rapidly and intensely than previously predicted. It poses a grave threat to our financial stability and has the potential to supersede the immense damage and loss caused by the COVID-19 pandemic. In the future, losses from climate-related disasters will increase dramatically if mitigation goals are not met and if we fail to ramp up resilience efforts. Recovery from this global pandemic and transformation towards a resilient Europe and Central Asia are intimately linked and must be pursued in a joined-up approach.

Jake Blucker/Unsplash.com

ABBREVIATIONS

ADB	Asian Development Bank
ANSSI	French Network and Information Security Agency
ASEAN	Association of Southeast Asian Nations
BRIGC	Belt and Road Initiative International Green Development Coalition
BSI	German Federal Office for Information Security
BT	British Telecom
CAREC	Central Asia Regional Economic Cooperation
CEPS	Centre for European Policy Studies
CERT	Computer Emergency Response Team
CERT.LV	Latvia's National Computer Emergency Response Team
CESDRR	Centre for Emergency Situations and Disaster Risk Reduction for Central Asia and South Caucasus
CCIV	Climate Change Impact, Vulnerability and Risk
CCPI	Climate Change Performance Index
CDRI	Coalition for Disaster Resilient Infrastructure
CH FOCP	Swiss Federal Office for Civil Protection
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CRN	Crisis and Risk Network
CSIRT	Computer Security Incident Response Team
DE	Germany
GFDRR	Global Facility for Disaster Reduction and Recovery
GIS	Geographic Information System
EC	European Union Commission
ECI	European Critical Infrastructure
EEA	European Environment Agency
EIB	European Investment Bank
ENISA	European Network and Information Security Agency
EP	European Union Parliament
ERCC	Emergency Response Coordination Centre
EU	European Union
EU TEG	European Union Technical Expert Group
GHG	Greenhouse Gas
ICAO	International Civil Aviation Organization
ICT	Information and Telecommunications
ICSs	Industrial Control Systems
IT	Information Technology
MoD	Ministry of Defence
NATO	The North Atlantic Treaty Organization
NRA	National Risk Assessment
ÖBB	The Austrian Federal Railways
OECD	Organization for Economic Co-operation and Development
OIEWG	Open-Ended Intergovernmental Expert Working Group
PPP	Public-Private Partnership
RO	Romania
RTR	Austrian Regulatory Authority for Broadcasting and Telecommunications
SCADA	Supervisory Control and Data Acquisition
SDGs	Sustainable Development Goals
SDC	Swiss Agency for Development and Cooperation
SFM	Sendai Framework Monitor
TRACERA	Transport Corridor Europe-Caucasus-Asia
UK	United Kingdom
UK NIC	United Kingdom National Infrastructure Commission
UMWELTBU–NDESAMT	German Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety
UN	United Nations
UN DESA	United Nations Department of Economic and Social Affairs
UNDP	United Nations Development Programme
UNDRR	United Nations Office for Disaster Risk Reduction
UNECE	United Nations Economic Commission for Europe
UNEP	United Nations Development Programme
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNGA	United Nations General Assembly
UNISDR	United Nations Office for Disaster Risk Reduction
UNSCR	United Nations Security Council Resolution
US	United States
WB	World Bank
WEF	World Economic Forum
WFD	Water Framework Directive

REFERENCES

1. Arteaga, F. (2010) Energy Security in Central Asia: Infrastructure and Risk (ARI). Elcanto Royal Institute. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/defense+security/ari1-2010 (accessed: 23.07.2020)
2. ACAPS (2014) Floods in Serbia, Bosnia and Herzegovina, and Croatia. Briefing Note. https://reliefweb.int/sites/reliefweb.int/files/resources/briefing_note_floods_in_serbia_bosnia_and_herzegovina_and_croatia_may_2014_update.pdf (accessed: 10.06.2020)
3. AP News (2019) Snow, flooding, mudslides in Austria kill 1, injure 2. https://apnews.com/d7de9952183d4f7298fa54ec6418918b (accessed: 30.05.2020)
4. Asian Development Bank (ADB) (2011) Armenia's Transport Outlook. Transport Sector Master Plan. https://www.adb.org/sites/default/files/publication/28298/armenia-transport-outlook.pdf (accessed: 05.06.2020)
5. Asian Development Bank (ADB) (2020) CAREC Transport Strategy 2030. Asian Development Bank, Manila, the Philippines, January 2020. DOI: DOI: http://dx.doi.org/10.22617/SPR200024-2
6. Asian Development Bank (ADB) (2017). Meeting Asia's Infrastructure Needs. Asian Development Bank, Manila. https://www.adb.org/sites/default/files/publication/227496/special-report-infrastructure.pdf (accessed: 11.07.2020)
7. BBC (2019) Albania hit by deadly 6.4 magnitude earthquake. https://www.bbc.com/news/world-europe-50555776 (accessed: 30.05.2020)
8. BBVA (2020) What is taxonomy for sustainable finance? https://www.bbva.com/en/what-is-the-taxonomy-for-sustainable-finance/ (accessed: 17.06.2020)
9. Black, J. (2002) Critical reflections on regulation. Australian Journal of Legal Philosophy 27: 1-35
10. Bross, L.; Krause, S.; Wannewitz, M.; Stock, E.; Sandholz, S.; Wienand, I. (2019) Insecure Security: Emergency Water Supply and Minimum Standards in Countries with a High Supply Reliability. Water 2019, 11, 732. DOI: 10.3390/w11040732
11. BSA The Software Alliance (2015) EU Cybersecurity Dashboard - Country: Romania. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_romania.pdf (accessed: 18.04.2020)
12. BSA (2015) EU Cybersecurity Dashboard: Country Profiles. http://cybersecurity.bsa.org/countries.html (accessed: 07.06.2020)
13. Bulgarian Council of Ministers (2016) National Cyber Security Strategy "Cyber-resilient Bulgaria 2020" (in Bulgarian). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-6 (accessed: 07.06.2020)
14. Centre for European Policy Studies (CEPS) (2010) Protecting critical infrastructure in the EU. CEPS task force report. Centre for European Policy Studies, Brussels. https://iris.luiss.it/retrieve/handle/11385/36860/860/Critical_Infrastructure_Protection_Final_A4.pdf (accessed: 12.07.2020)
15. Christidis, P.; Rivas, J. N. I. (2012) Measuring road congestion. European Commission Joint Research Centre Scientific and Policy Reports. Luxembourg: Publications Office of the European Union. DOI: 10.2791/15282
16. Climate Change Performance Index (CCPI) (2020) Index statistics. Germanwatch. https://www.climate-change-performance-index.org/ (accessed: 01.06.2020)
17. ClimateChangePost (2020) Coastal flood risk in The Netherlands. https://www.climatechangepost.com/netherlands/coastal-floods/ (accessed: 29.05.2020)
18. CMS Law Now (2020) Network resilience and telecommunications as essential service during Coronavirus (COVID-19). https://www.cms-lawnow.com/ealerts/2020/04/network-resilience-and-telecommunications-as-essential-service (accessed: 16.07.2020)
19. Coalition for Disaster Resilient Infrastructure website (CDRI) (2020) https://cdri.world/ (accessed: 10.06.2020)
20. Crisis and Risk Network (CRN) (2009) Focal Report 2: Critical Infrastructure Protection. Center for Security Studies (CSS), ETH Zürich, March 2009. https://www.files.ethz.ch/isn/105865/CRN-Report-Focal-Report2-Critical-Infrastructure-def.pdf (accessed: 16.07.2020)
21. Deloitte (2020) COVID-19: The impact of cyber on critical infrastructure in the next normal. https://www2.deloitte.com/global/en/pages/risk/covid-19/covid-19-the-impact-of-cyber-on-critical-infrastructure-in-the-next-normal.html# (accessed: 29.05.2020)
22. DE Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety (UMWELTBUNDESAMT) & United Nations Economic Commission for Europe (UNECE) (2016) Hazard prevention and Crisis Management in the Danube River Delta. http://www.unece.org/fileadmin/DAM/env/documents/2016/TEIA/AssistanceProgramme/doku_03_2016_hazard_prevention_and_crisis_management_in_the_danube_river_delta.pdf (accessed: 18.04.2020)
23. DE Federal Ministry of the Interior (2009) National Strategy for Critical Infrastructure Protection (CIP Strategy. Berlin, 17th June 2009. https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile (accessed: 18.04.2020)
24. Deutsche Welle (DW) (2019) Deadly floods in France, Spain cause disruption. https://www.dw.com/en/deadly-floods-in-france-spain-cause-disruption/a-50957967 (accessed: 30.05.2020)
25. Drzik, J. P. (2019) Infrastructure Around the World is Failing. Here's How to Make It More Resilient. World Economic Forum. https://www.weforum.org/agenda/2019/01/infrastructure-around-the-world-failing-heres-how-to-make-it-more-resilient/ (accessed: 25.05.2020)
26. Egis International & Dornier Consulting (2014) Logistics Processes and Motorways of the Sea II in Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Ukraine, Uzbekistan. LOGMOS Master Plan - TRECERA. ENPI 2011 / 264 459. http://www.traceca-org.org/fileadmin/fm-dam/TAREP/65ta/Master_Plan/MP.pdf (accessed: 14.07.2020)
27. Escritt, T. (2015) Power returns to Amsterdam after outage hits a million homes. Reuters. https://www.reuters.com/article/us-dutch-power-outages/power-returns-to-amsterdam-after-outage-hits-a-million-homes-idUSKBN0MN0UJ20150327 (accessed: 10.06.2020)
28. European Environment Agency (EEA) (2019) Adaptation challenges and opportunities for the European energy system. Building a climate-resilient low-carbon energy system. EEA Report No 01/2019. DOI: 10.2800/227321.

https://www.eea.europa.eu/publications/adaptation-in-energy-system (accessed: 27.05.2020)
29. European Environment Agency (EEA) (December, 2019) Renewable energy in Europe: key for climate objectives, but air pollution needs attention. Briefing no. 13/2019. DOI: 10.2800/926977. https://www.eea.europa.eu/publications/renewable-energy-in-europe-key (accessed: 27.05.2020)
30. European Investment Bank (EIB) (2013) Water sector: financing water supply, sanitation and flood protection https://www.eib.org/attachments/thematic/water_en.pdf (accessed: 02.06.2020)
31. European Network and Information Security Agency (ENISA) (2015) Critical Information Infrastructures Protection approaches in EU. Final Document | Version 1 | TLP: Green. https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf (accessed: 07.06.2020)
32. European Network and Information Security Agency (ENISA) (2016) NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. https://www.enisa.europa.eu/publications/ncss-good-practice-guide (accessed: 08.06.2020)
33. European Network and Information Security Agency (ENISA) website (2020) https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/scada (accessed: 07.06.2020)
34. European Telecommunications Network Operators' Association (ETNO) (2020) The State of Digital Communications 2020. Annual Economic Report. https://etno.eu//downloads/reports/etno%20state%20of%20digital%20communications%20report%202020.pdf (accessed: 04.08.2020)
35. Eurostat (2019) Population structure and aging. https://ec.europa.eu/eurostat/statistics-explained/index.php/Population_structure_and_ageing#Past_and_future_population_ageing_trends_in_the_EU (accessed: 29.05.2020)
36. EU (2000) Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000L0060 (accessed: 18.04.2020)
37. EU-CIRCLE (2019) Impacts of Climate Change and Extreme Weather Events on Critical Infrastructure. http://www.eu-circle.eu/2019/03/19/impacts-of-climate-change/ (accessed: 29.06.2020)
38. EU Commision (EC) (2016) Analytical grids on state aid to Infrastructure 2016 - 2017. https://ec.europa.eu/competition/state_aid/modernisation/notice_aid_en.html (accessed: 02.06.2020)
39. EU Commission (EC) (2006) Communication from the Commission on a European Programme for Critical Infrastructure Protection /* COM/2006/0786 final */. Brussels, 12.12.2006. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (accessed: 19.04.2020)
40. EU Commission (EC) (Dec 2019) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. The European Green Deal. COM(2019) 640 final. https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf (accessed: 10.06.2020)
41. EU Commission (EC) (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The Water Framework Directive and the Floods Directive: Actions towards the 'good status' of EU water and to reduce flood risks /* COM/2015/0120 final */. 52015DC0120. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0120 (accessed: 02.06.2020)
42. EU Commission (EC) (July, 2019) COMMISSION STAFF WORKING DOCUMENT EVALUATION of COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION {SWD(2019) 310 final}. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf (accessed: 11.06.2020)
43. EU Commission (EC) (May 2017) COMMISSION STAFF WORKING DOCUMENT Overview of Natural and Man-made Disaster Risks the European Union may face. SWD(2017) 176 final. Brussels, 23.5.2017. https://ec.europa.eu/echo/sites/echo-site/files/swd_2017_176_overview_of_risks_2.pdf (accessed: 16.07.2020)
44. EU Commission (EC) (March 2015) COMMISSION STAFF WORKING DOCUMENT Report on the implementation of the Water Framework Directive River Basin Management Plans Member State: BELGIUM. SWD(2015) 52 final https://ec.europa.eu/environment/water/water-framework/pdf/4th_report/MS%20Annex%20-%20Belgium.pdf (accessed: 02.06.2020)
45. EU Commission (EC) (2018) COMMISSION STAFF WORKING DOCUMENT Report on the implementation of the Water Framework Directive River Basin Management Plans Member State: GREECE. CORRIGENDUM. SWD(2015) 54 final/2. https://ec.europa.eu/environment/water/water-framework/pdf/4th_report/Greece_CORRECTED_5_EN_autre_document_travail_service_part1_v5-1_FINAL.pdf (accessed: 02.06.2020)
46. EU Commission (EC) (19 June 2020) Inception Impact Assessment. Proposal for measures to enhance the protection and resilience of critical infrastructure. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection (accessed: 12.07.2020)
47. EU Commission (EC) INFORM (2019) INFORM Country Risk Profile: Romania. https://drmkc.jrc.ec.europa.eu/inform-index/Portals/0/InfoRM/2019/Country_Profiles/ROU.pdf (accessed: 18.04.2020)
48. EU Commission (EC) (2017) Romania - Disaster management structure. Vademecum - Civil Protection. https://ec.europa.eu/echo/files/civil_protection/vademecum/ro/2-ro-1.html (accessed: 18.04.2020)
49. EU Commission (EC) (2019) Status of implementation of the WFD in the Member States. https://ec.europa.eu/environment/water/participation/map_mc/map.htm (accessed: 02.06.2020)
50. EU Commission (EC) (March 2019) Transport in the European Union Current Trends and Issues. https://ec.europa.eu/transport/sites/transport/files/2019-transport-in-the-eu-current-trends-and-issues.pdf (accessed: 18.04.2020)
51. EU Commission (EC), executed by TNO Netherlands Organisation for Applied Scientific Research, SEOR Erasmus University Rotterdam & ZSI Centre for Social Innovation (2009) Telecommunication: Comprehensive sectoral analysis of emerging competences and economic activities in the European Union. DG EMPL project VC/2007/0866. https://ec.europa.eu/social/BlobServlet?docId=4148&langId=en (accessed:04.08.2020)
52. EU Commission (EC) website (2020) Critical Infrastructure. https://ec.europa.eu/home-affairs/tags/critical-infrastructure_en (accessed: 19.04.2020)
53. EU Commission (EC) website (2020) Critical Infrastructure Warning Information Network (CIWIN). https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (accessed: 03.06.2020)
54. EU Commission (EC) website (June, 2020) EU Taxonomy for sustainable activities. https://ec.europa.eu/info/publications/sustainable-finance-teg-taxonomy_en (accessed: 17.06.2020)
55. EU Commission (EC) website (2014) Regional policy: Priorities for 2014-2020. https://ec.europa.eu/regional_policy/en/policy/how/priorities (accessed: 10.06.2020)
56. EU Commission (EC) website (July, 2020) Sustainable finance: Overview. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance_en (accessed: 16.06.2020)
57. EU Parliament (EP) (2018) Investment in infrastructure in the EU Gaps, challenges, and opportunities. Briefing. http://www.iberglobal.com/files/2018-2/infrastructure_eu.pdf (accessed: 11.06.2020)
58. EU Parliament (EP) (2020) PROPOSAL FOR ADDITIONAL MEASURES ON CRITICAL INFRASTRUCTURE PROTECTION /

AFTER 2020-9. Legislative Train 05.2020. https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/promoting-our-european-way-of-life/file/critical-infrastructure-protection (accessed: 11.06.2020)

59. EU Science Hub (2017) Critical infrastructure to be hard hit by climate hazards. https://ec.europa.eu/jrc/en/news/critical-infrastructure-be-hard-hit-climate-hazards (accessed: 29.05.2020)
60. EU Technical Expert Group on Sustainable Finance (EU TEG) (2020) Taxonomy: Final report of the Technical Expert Group on Sustainable Finance. https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200309-sustainable-finance-teg-final-report-taxonomy_en.pdf (accessed: 17.06.2020)
61. Finland Security Committee (2019) Finland´s Cyber Security Strategy 2019. https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/ (accessed: 07.06.2020)
62. Forzieri, G.; Bianchi, A.; Marin Herrera, M.A.; Batista e Silva, F.; Feyen, L. and Lavalle, C. (2015) Resilience of large investments and critical infrastructures in Europe to climate change. EUR 27598 EN. Luxembourg (Luxembourg): Publications Office of the European Union. DOI: 10.2788/171858
63. French Network and Information Security Agency (ANSSI) (2020) The French CIIP Framework. https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/ (accessed: 08.06.2020)
64. Ganin, A.; Quach, P.; Panwar, M.; Collier, Z. A.; Keisler, J. M.; Marchese, D.; Linkov, D. (2017) Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis 40(4). DOI: 10.1111/risa.12891
65. Gjesvik, L. (2019) Comparing Cyber Security Critical Infrastructure protection in Norway, the UK and Finland. NUPI Report 5/2019. Norwegian Institute of International Affairs. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2598280/NUPI_Report_5_2019_Gjesvik.pdf?sequence=1&isAllowed=y (accessed: 07.06.2020)
66. Global Assessment Report (GAR) (2019), Global Assessment Report on Disaster Risk Reduction. United Nations Office for Disaster Risk Reduction (UNDRR), Geneva, Switzerland. https://gar.undrr.org/sites/default/files/reports/2019-05/full_gar_report.pdf (accessed: 09.06.2020)
67. Global Facility for Disaster Reduction and Recovery (GFDRR) (2009) Disaster Risk Reduction and Emergency Management in Armenia. Global Facility for Disaster Reduction and Recovery "Armenia: Institutional Arrangements for Disaster Risk Management and Reduction". https://www.preventionweb.net/files/12368_ReportArmeniaDisasterRiskReductiona.pdf (accessed: 05.06.2020)
68. Global Facility for Disaster Reduction and Recovery (GFDRR) & The World Bank (WB) (2019) Accelerating risk reduction through forward looking investments and policies in Romania. https://reliefweb.int/sites/reliefweb.int/files/resources/RomaniaRiskReduction2pagerOctober2019.pdf (accessed: 18.04.2020)
69. Government of Albania; European Union; UN Albania; The World Bank (2020) Albania: Post-Disaster Needs Assessment. Volume A Report. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/albania_post-disaster_recovery_a_v9.0.pdf (accessed: 30.05.2020)
70. Government of Romania (2010) Emergency Ordinance 98/2010 on the Identification, Designation and Protection of Critical Infrastructure 2010 (in Romanian). https://www.sts.ro/files/userfiles/DOCUMENTE/Cadru_legislativ/ordonanta-de-urgenta-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.pdf (accessed: 18.04.2020)
71. Government of Romania (2018) Integrated National Energy and Climate Change Plan 2021-2030. https://ec.europa.eu/energy/sites/ener/files/documents/romania_draftnecp_en.pdf (accessed: 18.04.2020)

72. Government of Romania (2013) National climate change strategy 2013-2020 (in Romanian). https://www.preventionweb.net/files/61769_20131001snsc.pdf (accessed: 18.04.2020)
73. Government of Romania (2017) Sendai Framework data readiness review report. https://www.preventionweb.net/files/53201_romaniarou.pdf (accessed: 18.04.2020)
74. Hallegatte, S.; Rentschler, J.; Rozenberg, J. (2019) Lifelines : The Resilient Infrastructure Opportunity. Sustainable Infrastructure. Washington, DC: World Bank. License: CC BY 3.0 IGO. https://openknowledge.worldbank.org/handle/10986/31805 (accessed: 01.07.2020)
75. Hendel-Blackford, S.; Brand, K.; Nierop, S.; Winkel, R.; Street, R. (2017) Assessing Adaptation Knowledge in Europe: Infrastructure Resilience in the Transport, Energy and Construction Sectors: Final Report. Ecofys 2016, UKCIP, SRUC by order of: the European Commission. https://ec.europa.eu/clima/sites/clima/files/adaptation/what/docs/infrastructure_resilience_en.pdf (accessed: 23.07.2020)
76. International Civil Aviation Organization (2020) Economic Impacts of COVID-19 on Civil Aviation. https://www.icao.int/sustainability/Pages/Economic-Impacts-of-COVID-19.aspx (accessed: 29.05.2020)
77. Karagiannis, G.M.; Turksezer, Z.I.; Alfieri, L.; Feyen, L.; Krausmann, E. (2019) Climate change and critical infrastructure – floods, EUR 28855 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-09552-1. DOI:10.7260/007069, JRC109015
78. Keele, S., Coenen, L. (2019) Policy for critical infrastructure resilience. Melbourne, 2019. Workshop Summary. Arup and Resilience Shift, UK. https://www.resilienceshift.org/wp-content/uploads/2019/04/ResilienceShift-Role-of-Public-Policy-FINAL-1.pdf (accessed: 03.06.2020)
79. Khalid, M. (2017) Urban success for water quality in Macedonia. The Borgen Project. https://borgenproject.org/urban-water-quality-in-macedonia/ (accessed: 02.06.2020)
80. Kinstellar (2018) Mandatory cyber security standards apply to operators of critical infrastructure, digital and public service providers in Bulgaria. https://www.kinstellar.com/locations/news-deals-insights/detail/sofia-bulgaria/822/mandatory-cyber-security-standards-apply-to-operators-of-critical-infrastructure-digital-and-public-service-providers-in-bulgaria (accessed: 07.06.2020)
81. Koop, C.; Lodge, M. (2015) What is regulation? An interdisciplinary concept analysis. Regulation and Governance, Wiley Publishing Asia Pty Ltd. ISSN 1748-5983. DOI: 10.1111/rego.12094
82. Kornejew, M.; Rentschler, J.; Hallegatte, S. (2019) Well Spent : How Governance Determines the Effectiveness of Infrastructure Investments (English). Policy Research working paper no. WPS 8894. Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/414611560792300712/Well-Spent-How-Governance-Determines-the-Effectiveness-of-Infrastructure-Investments (accessed: 09.07.2020)
83. Lewis, L. P. and Petit, F. (2019) Critical infrastructure interdependency analysis: Operationalising resilience strategies. Contributing Paper to GAR 2019. https://www.undrr.org/publication/critical-infrastructure-interdependency-analysis-operationalising-resilience-strategies (accessed: 19.04.2020)
84. LSE (2020) Climate change laws of the world. Grantham Research Institute on Climate Change and the Environment, LSE. https://climate-laws.org/cclow/legislation_and_policies?type%5B%5D=legislative (accessed: 01.06.2020)
85. McLellan, A. (2019) Urgent Repairs Needed to Facilitate Project Moves. Breakbulk.

https://www.breakbulk.com/Articles/crisis-of-crumbling-infrastructure (accessed: 07.07.2020)

86. Melchiorre, T. (2018) Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. NATO Energy Security Centre of Excellence (NATO ENSEC COE). https://enseccoe.org/data/public/uploads/2018/04/d1_2018.04.23-recommendations-on-the-importance-of-critical-energy.pdf (accessed: 01.06.2020)
87. Millar, A. (2015) Finland is the place to be for ICT. ComputerWeekly.com. https://www.computerweekly.com/news/4500244666/Finland-is-the-place-to-be-for-ICT (accessed: 07.06.2020)
88. Ministry of Defence of Latvia (MoD Latvia) (2014) Cyber Security Strategy of Latvia 2014-2018. https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf (accessed: 08.06.2020)
89. Ministry of Transport of Romania (MoT) (2013) Sectoral Operational Programme Transport 2007 – 2013. http://old.fonduri-ue.ro/res/filepicker_users/cd25a597fd-62/Doc_prog/prog_op/5_POST/POST_versiunea_aprilie_2013.pdf (accessed: 18.04.2020)
90. Nabiyeva, K. (2018) Energy Transition in South East and Eastern Europe, South Caucasus and Central Asia Challenges. Opportunities and Best Practices on Renewable Energy and Energy Efficiency. Friedrich-Ebert-Stiftung. http://library.fes.de/pdf-files/id-moe/14922.pdf (accessed: 02.06.2020)
91. NIRAS (2020) More than 240,000 Macedonians benefit from the investments in wastewater treatment facilities. https://www.niras.com/projects/wastewater-treatment-in-macedonia/ (accessed: 02.06.2020)
92. OECD (2019) Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. OECD Publishing, Paris. DOI: https://doi.org/10.1787/02f0e5a0-en
93. OECD (2011) Regulatory Policy and Governance: Supporting Economic Growth and Serving the Public Interest. OECD Publishing. DOI: http://dx.doi.org/10.1787/9789264116573-en
94. OECD (December, 2019) Sustainable Infrastructure for Low-Carbon Development in Central Asia and the Caucasus: Hotspot Analysis and Needs Assessment. Green Finance and Investment, OECD Publishing, Paris. DOI: https://doi.org/10.1787/d1aa6ae9-en
95. OECD & UNECE (2016) Water Policy Reforms in Eastern Europe, the Caucasus and Central Asia Achievements of the European Union Water Initiative, 2006-16. https://www.oecd.org/env/outreach/EUWI%20Report%20layout%20English_W_Foreword_Edits_newPics_13.09.2016%20WEB.pdf (accessed: 02.06.2020)
96. OneTrust DataGuidance (2017) Germany: BSI recognises security standard for water supply and waste critical infrastructures. https://platform.dataguidance.com/news/germany-bsi-recognises-security-standard-water-supply-and-waste-critical-infrastructures (accessed: 18.04.2020)
97. Otto, A.; Kellermann, P.; Thieken, A. H.; Costa, M. M.; Carmona, M.; Bubeck, P. (2018) Risk reduction partnerships in railway transport infrastructure in an alpine environment. International Journal of Disaster Risk Reduction, Vol. 33, February 2019, Pages 385-397. DOI: https://doi.org/10.1016/j.ijdrr.2018.10.025
98. Panda, A. and Bower, A. (2020). Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, Vol. ahead-of-print No. ahead-of-print. DOI: https://doi.org/10.1108/IJDRBE-07-2019-0046
99. Pastori, E.; Brambilla, M.; Maffii, S.; Vergnani, R.; Gualandi, E.; Skinner, I. (2018) Research for TRAN Committee – Modal shift in European transport: a way forward. European Parliament, Policy Department for Structural and Cohesion Policies, Brussels. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/629182/IPOL_STU(2018)629182_EN.pdf (accessed: 04.06.2020)
100. Pollock, E. (2018) Italy's Morandi Bridge Collapse—What Do We Know? Engineering.com. https://www.engineering.com/BIM/ArticleID/17517/Italys-Morandi-Bridge-CollapseWhat-Do-We-Know.aspx#:~:text=On%20Aug.,not%20have%20felled%20the%20bridge (accessed: 05.06.2020)
101. Population Matters (2020) Population: The Numbers. https://populationmatters.org/the-facts/the-numbers?gclid=EAIaIQobChMI49_p2cbY6QIVVqaWCh10pQxEEAAYASAAEgJvA_D_BwE (accessed: 29.05.2020)
102. Ramm, K. (2018) Time to invest in Europe's water infrastructure. Euractiv. Available online: https://www.euractiv.com/section/energy-environment/opinion/time-to-invest-in-europes-water-infrastructure/ (accessed: 07.07.2020)
103. RO Ministry of Waters and Forests National Administration „Romanian Waters" (2016) National Management Plan Updated Related to Section from the International Hydrographic of Danube River Basin Which is Included in Romanian Territory 2016-2021. Available online: http://www.rowater.ro/TEST/Brochure_National%20Management%20Plan_EN.pdf (accessed: 18.04.2020)
104. Russel, M. (2019) Connectivity in Central Asia. Reconnecting the Silk Road. Briefing. European Parliamentary Research Service, European Parliament. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637891/EPRS_BRI(2019)637891_EN.pdf (accessed: 14.07.2020)
105. Serentschy, G. (2015) Why Europe's telecom sector needs regulatory modernization. Serentschy.com. Available online: https://www.serentschy.com/why-europes-telecom-sector-needs-regulatory-modernization/ (accessed: 04.08.2020)
106. Smart Water Magazine (January 2020) A tour of water management in Europe. Available online: https://smartwatermagazine.com/news/smart-water-magazine/a-tour-water-management-europe (accessed: 02.06.2020)
107. Smart Water Magazine (2019) Brussels adopts €4 billion investment package, including for water infrastructure projects. Available online: https://smartwatermagazine.com/news/european-commission/brussels-adopts-eu4-billion-investment-package-infrastructure-projects (accessed: 02.06.2020)
108. Smart Water Magazine (2020) EU warns Belgium, Greece and Sweden to comply with rules for treating urban waste water. Available online: https://smartwatermagazine.com/news/european-commission/eu-warns-belgium-greece-and-sweden-comply-rules-treating-urban-waste-water (accessed: 02.06.2020)
109. Statement of Romania to the 6th meeting of the Global Platform for Disaster Risk Reduction Delivered by H.E. Dr Raed ARAFAT, Secretary of State, Ministry of Internal Affairs, Head of the Emergency Situations Department (2019) Available online: https://www.preventionweb.net/english/policies/v.php?id=68436&cid=141 (accessed: 18.04.2020)
110. Swiss Agency for Development and Cooperation (SDC) (2019) Managing disaster risks and water under climate change in Central Asia and Caucasus. Available online: https://reliefweb.int/report/world/managing-disaster-risks-and-water-under-climate-change-central-asia-and-caucasus (accessed: 03.06.2020)
111. Swiss Federal Office for Civil Protection (CH FOCP) (2017) National CIP Strategy 2018-2022 (original in German: Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022). Available online: https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html (accessed: 29.06.2020)
112. The DEFENDER consortium partners (2017) Defending the European Energy Infrastructures. Project: H2020–CIP-01-2016–740898. Critical Energy Infrastructure. Security Stakeholder Group Manifest. Available online: https://defender-project.eu/wp-content/uploads/2019/06/DEFENDER_CEIS_SG-Manifest-V05.pdf (accessed: 12.07.2020)
113. The European Federation of National Associations of Water Services (2018) The governance of water services in Europe. Available online: http://www.eureau.org/resources/publications/150-report-on-the-governance-of-water-services-in-europe/file (accessed: 02.06.2020)
114. The World Bank (WB) (2008) Europe and Central Asia Region: How Resilient is the Energy Sector to Climate Change? Available online: http://documents.worldbank.org/curated/en/710881484809276842/pdf/111555-WP-PUBLIC.pdf (accessed: 10.06.2020)

115. The World Bank (2018) Second Technical Knowledge Exchange of Resilient Transport: Summary Report. Available online: http://documents.worldbank.org/curated/en/368251527152815053/pdf/126556-23-5-2018-15-26-58-FINALResilientTransportBelgradeTKXReportFinalDPforWebsite.pdf (accessed: 04.06.2020)
116. Toso, S. (2019) Briefing on European Construction: April 2019. Euroconstruct. Available online: https://www.euroconstruct.org/ec/blog/2019_04 (accessed: 02.06.2020)
117. Trading Economics (2018) Romania - Urban Population (% of Total). Available online: https://tradingeconomics.com/romania/urban-population-percent-of-total-wb-data.html (accessed: 18.04.2020)
118. United Nations (UN) (2020) A UN framework for the immediate socio-economic response to COVID-19. April 2020. Available online: https://unsdg.un.org/sites/default/files/2020-04/UN-framework-for-the-immediate-socio-economic-response-to-COVID-19.pdf (accessed: 07.07.2020)
119. United Nations (UN) (2015) Transforming Our World: The 2030 Agenda for Sustainable Development. A/RES/70/1. Available online: https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf (accessed: 11.06.2020)
120. UN DESA (2018) World Urbanization Prospects 2018. File 2: Percentage of Population at Mid-Year Residing in Urban Areas by region, subregion and country, 1950-2050. Available online: https://population.un.org/wup/Download/ (accessed: 29.05.2020)
121. UNDP (2020) BRIEF#2: Putting the UN Framework for Socio-Economic Response to COVID-19 Into Action: Insights: June 2020. Available online: https://www.undp.org/content/undp/en/home/coronavirus/socio-economic-impact-of-covid-19.html (accessed 01.07.2020)
122. UNDP (2001) Information Communications Technology for Development. Synthesis of Lessons Learned. Evaluation Office No. 5 September 2001. Available online: http://web.undp.org/evaluation/documents/essentials_5.pdf (accessed: 19.04.2020)
123. UNDP China (2018) Technology for Resilience along the Belt and Road. Available online: https://www.cn.undp.org/content/china/en/home/presscenter/pressreleases/2018/technology-for-resilience-along-the-belt-and-road.html (accessed: 15.07.2020)
124. UNDRR (2020) (cyber) Bridging Cybersecurity and Disaster Risk Reduction: Working Paper. Available online: https://www.undrr.org/publication/bridging-cybersecurity-and-disaster-risk-reduction-working-paper (accessed: 07.06.2020)
125. UNDRR (May 2019) Opportunities to Integrate Disaster Risk Reduction and Climate Resilience into Sustainable Finance. United Nations Office for Disaster Risk Reduction, Regional Office for Europe, Brussels, Belgium. Available online: https://www.undrr.org/publication/opportunities-integrate-disaster-reduction-risk-and-climate-resilience-sustainable (accessed: 10.06.2020)
126. UNDRR (2020) Options for Addressing Infrastructure Resilience. Working Paper. Available online: https://www.undrr.org/publication/working-paper-options-addressing-infrastructure-resilience (accessed: 03.06.2020)
127. UNDRR (UNDRR SFM report) (2020) Monitoring the Implementation of Sendai Framework for Disaster Risk Reduction 2015-2030: A Snapshot of Reporting for 2018. Available online: https://www.undrr.org/publication/monitoring-implementation-sendai-framework-disaster-risk-reduction-2015-2030-snapshot (accessed: 29.06.2020)
128. UN Economic Commission for Europe (UNECE) (2020) Climate Change Impacts and Adaptation for Transport Networks and Nodes. Available online: https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp5/ECE-TRANS-283e.pdf (accessed: 06.06.2020)
129. UNEP (2019) The Belt and Road Initiative International Green Development Coalition (BRIGC). Available online: https://www.unenvironment.org/regions/asia-and-pacific/regional-initiatives/belt-and-road-initiative-international-green (accessed: 15.07.2020)
130. UNESCAP (2020) Multi-Hazard Risk to Exposed Stock and Critical Infrastructure in Central Asia. Asia-Pacific Information Superhighway (AP-IS) Working Paper Series. Available online: https://www.unescap.org/sites/default/files/Multi_Hazard_Risk_Infrastructure_Central_Asia_ids.pdf (accessed: 10.06.2020)
131. UN General Assembly (UNGA) (2016) Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction. Seventy-first session Agenda item 19 (c) Sustainable development: disaster risk reduction. A/71/644. Available online: https://www.preventionweb.net/files/50683_oiewgreportenglish.pdf (accessed: 01.07.2020)
132. UNIDIR (2020) Cybersecurity Policy Portal: Country profies. Available online: https://cyberpolicyportal.org/en/ (accessed: 18.04.2020)
133. 133. UNISDR (2009) 2009 UNISDR Terminology on Disaster Risk Reduction. UN. Available online: https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf (accessed: 19.04.2020)
134. UK Cabinet Office (2011) Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf (accessed: 07.06.2020)
135. UK National Infrastructure Commission (UK NIC) (2020) Anticipate, React, Recover: Resilient Infrastructure Systems. Available online: https://www.nic.org.uk/wp-content/uploads/Anticipate-React-Recover-28-May-2020.pdf (accessed: 10.06.2020)
136. UK National Infrastructure Commission (UK NIC) (2019) Resilience Study. Scoping Report. Available online: https://www.nic.org.uk/wp-content/uploads/NIC_Resilience_Scoping_Report_September_2019-Final.pdf (accessed: 08.07.2020)
137. UK National Infrastructure Commission (UK NIC) (October 2019) Strategic Investment and Public Confidence. Available online: https://www.nic.org.uk/wp-content/uploads/NIC-Strategic-Investment-Public-Confidence-October-2019.pdf (accessed: 14.07.2020)
138. US Department of Commerce website (2019) Bulgaria - Information and Communications Technologies. Available online: https://www.privacyshield.gov/article?id=Bulgaria-Information-and-Communications-Technologies (accessed: 07.06.2020)
139. Vallejo, L. and M. Mullan (2017) Climate-resilient infrastructure: Getting the policies right. OECD Environment Working Papers, No. 121, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/02f74d61-en
140. Walker, J. J. (2012) Cyber Security Concerns for Emergency Management in Emergency Management, Dr. Burak E. (Ed.), ISBN: 978-953-307-989-9, InTech. DOI: 10.5772/34104
141. World Economic Forum (WEF) (2019) Global Risks Report 2019. World Economic Forum, Geneva. Available online: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (accessed: 25.05.2020)
142. UNDRR chief's 5-point plan for resilient infrastructure. Available online: https://iddrr.undrr.org/news/undrr-chiefs-5-point-plan-resilient-infrastructure (accessed: 05 October 2020)

UNDRR
UN Office for Disaster Risk Reduction

37 Bvd du Régent Brussels
1000, Belgium

www.undrr.org
www.preventionweb.net