
# Disaster Response

## Business Continuity Management
## Planning for disaster resilience in mobile networks

GSMA DISASTER RESPONSE

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Disaster Response

This report has benefited from contributions from Humanitarian Charter Signatories.

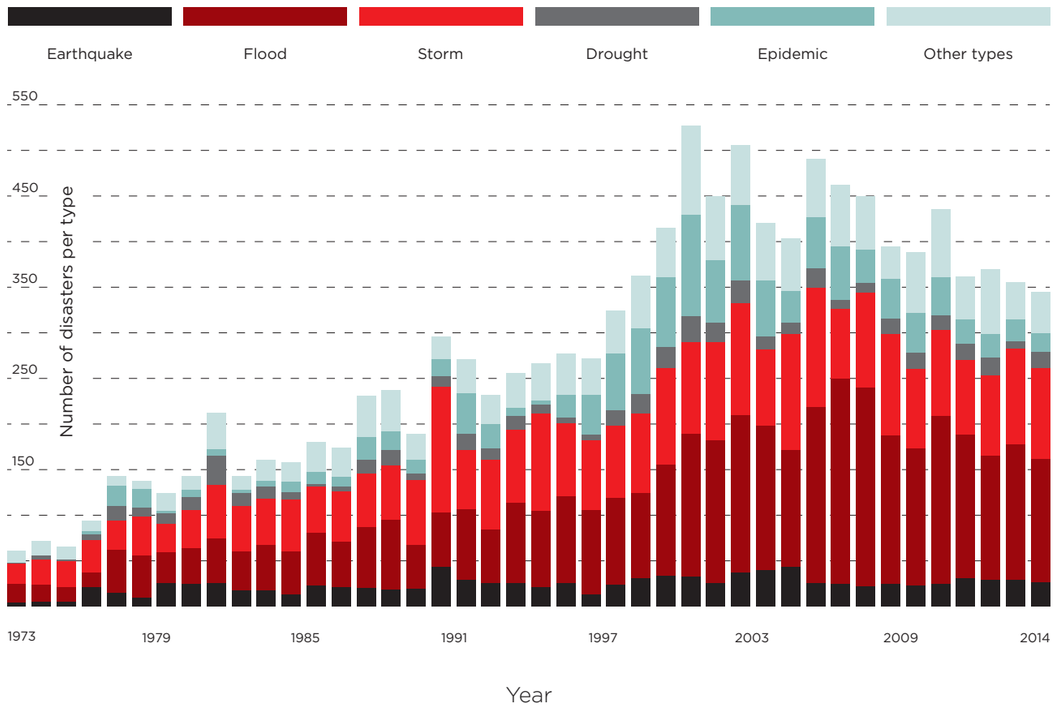
For more information, please get in touch:
web: www.gsma.com/disaster-response
email: disasterresponse@gsma.com

This publication was written by Martin Harris, GSMA.

# CONTENTS

# 1 Foreword

Since the birth of the mobile industry (around 1973) to date, there has been a marked increase in reported disasters affecting larger and larger populations;




Disasters by type since 1973 [1]

During that time mobile phone technology and usage has grown from being a niche market in developed markets to being the defacto communication channel for the majority of the worlds population, currently exceeding 3.5bn unique subscribers in 2015.

1. Centre for Research on the Epidemiology of Disasters (CRED) http://www.emdat.be/disaster_trends/index.html

In a disaster situation one of the first required resources is information (ideally verifiable information), so that both agencies tasked with response and the general populace can make informed decisions. The information during a disaster needs to be available, accessible and symmetric in order to be effective, this means that where possible and appropriate, all parties need to make relevant information available e.g. coverage maps, facility location, personnel location, etc. to each other. On top of this, MNOs can assist in making the information accessible to the population as needed.

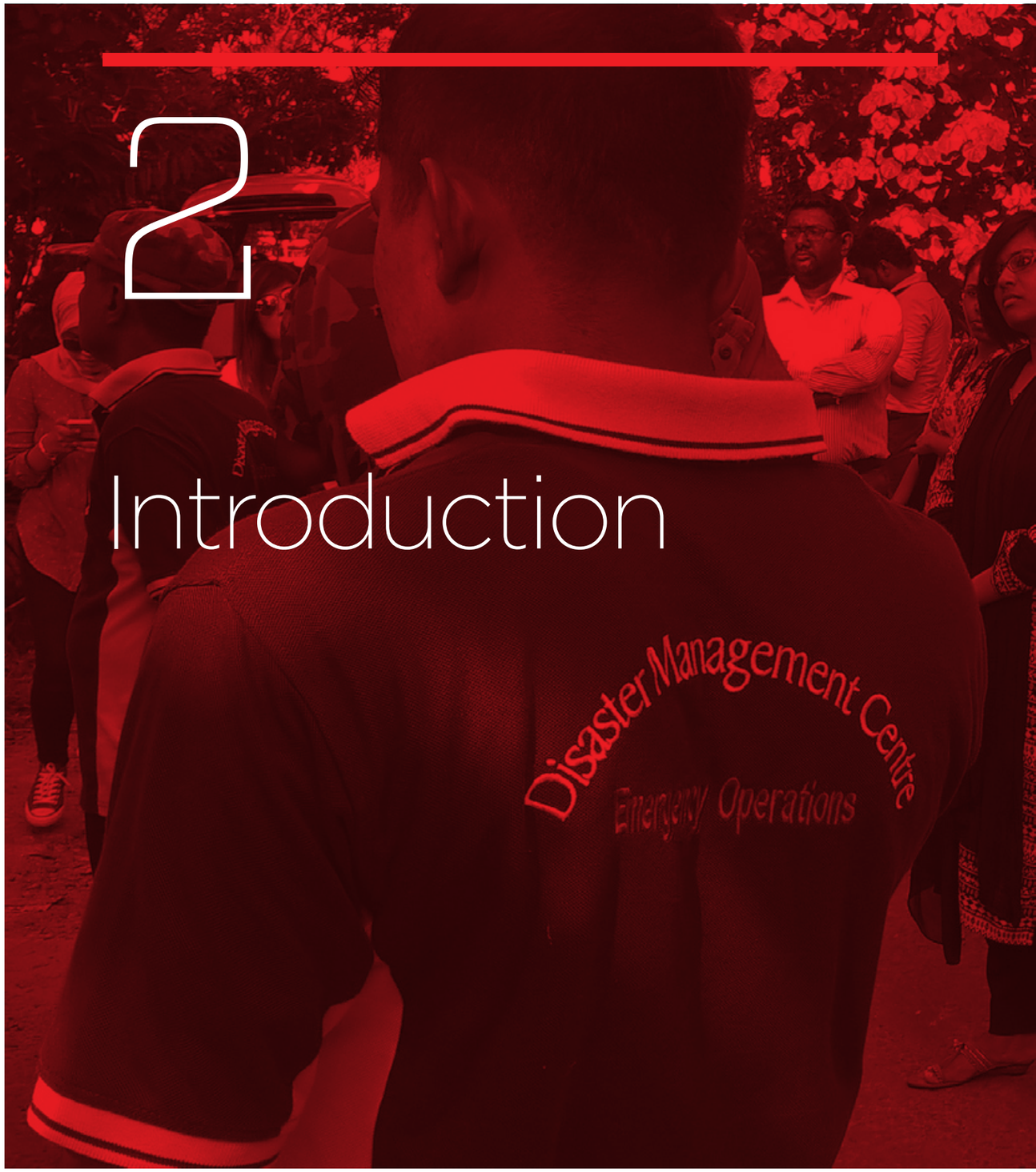
This has created a much greater expectation from subscribers, governments and international agencies that the mobile networks will help inform about ensuing disasters and provide the means for reaching out to families and friends caught up in disasters.

This on top of the need to provide support to emergency and relief services along with regulatory requirement compliance, means that building resilience of the mobile service and having robust business continuity plans is a key requirement for MNOs.

This is why one of the key activities linked to the Humanitarian Connectivity Charter (see page 48), is Planning, suggesting that "MNOs will work to develop a comprehensive disaster-preparedness and/or business continuity management (BCM) plan". The intention of this report is to explore this activity in greater depth and provide help to those looking to implement and improve existing plans.








# 2 Introduction

# 2.1 What does the report do?

The intention of this report is to highlight the business continuity planning and management (BCP&BCM) undertaken by Mobile Network Operators (MNO) in order to meet growing threats from national and regional disasters, plus the need for adapting and extending those plans to create much greater long term resilience for their business, services and support for the community they serve.

The intention of the report is to highlight what potential measures can be taken in order to help build resilience within mobile networks and their external dependencies through the use of Business Continuity measures. It is not intended to provide an exhaustive approach to BCM or BCP which is something undertaken by MNOs on a regular basis to such standards as ISO 22301. [2]

2. ISO 22301:2012 - Societal security -- Business continuity management systems --- Requirements http://www.iso.org/iso/catalogue_detail?csnumber=50038





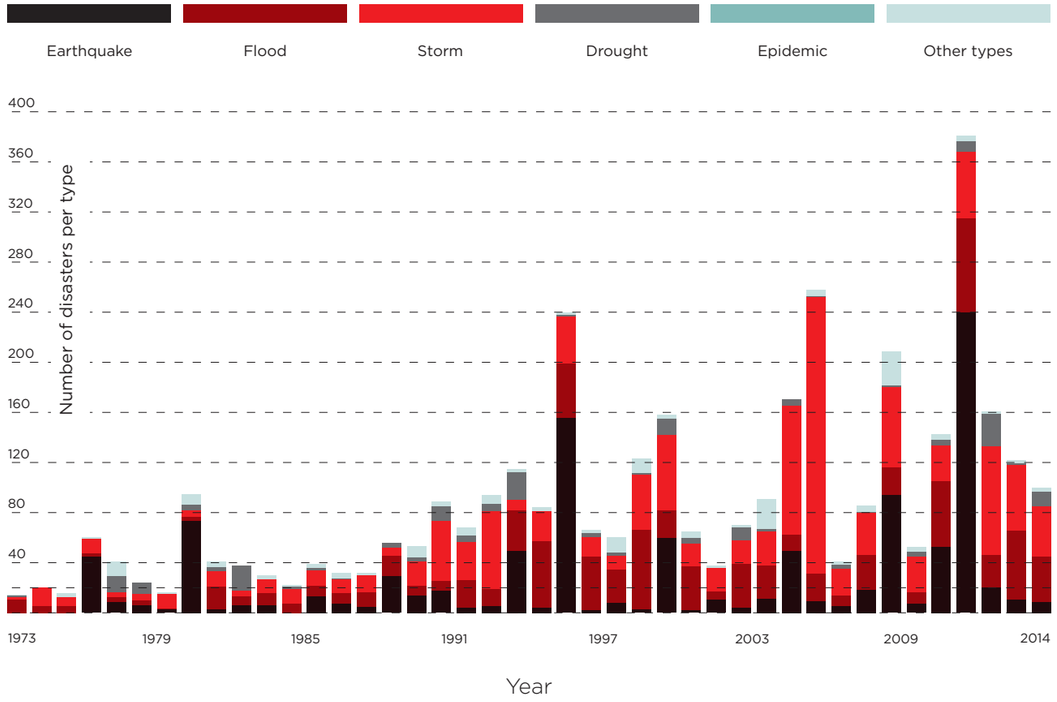



**Figure 2 Total Economic Damage of Disasters (scaled to 2014 USD)** [3]

# 2.2 Why build resilience into mobile networks?

As shown above the level of damage done by disasters, although very spikey by nature, has increased significantly over the last 40 years, probably through both and increase in frequency of disasters but also by population increase especially in vulnerable areas. Over the same period the mobile industry has developed into a nearly ubiquitous communication channel for the majority of the world's population. This combination has created a requirement not only for MNOs to protect their businesses in the face of such disasters but also a perceived responsibility to respond in supporting humanitarian needs during the disasters, especially in respect of communications.

3. http://www.emdat.be/disaster_trends/index.html

Whilst MNOs are creating and running BCPs to help protect their ongoing business against disruption both at a micro and macro levels, there is now considerably more at stake than just the MNO's business. It is now widely recognised that communication is a human right and the need is never more critical than during a disaster, where appropriate information and communications can help save lives, reduce suffering and advance recovery efforts.

One key aspect of BCM is building resilience into the network and the supporting business processes, so that over time the ability of the network to resist the depredations of disasters is increased. This in turn provides a better service for the subscribers and disaster responders, which should lead to better survival rates and reduced overall affect on the regional/national economy.

## 2.3 What is the current context for this report?

2015 saw international agreements being made on disaster risk reduction, climate change and sustainable development (UNWCDRR Sendai Framework, the launch of the UN Sustainable Development Goals (SDG) agenda, UNFCCC Paris agreement on climate change, etc.). Aspects of these agreements recognize the need that both public agencies and private industry will need to work together to help achieve the aims of these agreements and key part of this will in increasing resilience to disasters and supporting recovery efforts.

In the 18th century the regulations for building codes and zoning in the US came out of early insurers (like Benjamin Franklin) only insuring buildings against fire which complied to standards which they laid down. In the same way it is conceivable that the international agreements above and increasing pressure from insurers will mandate the adoption of increased regulation in resilience of businesses and public utilities.





# 3 Summary

# 3.1 Resilience for mobile networks

The definition of resilience is subject to the context to which it is applied to, for the purpose of this report it will be defined as the capacity of a mobile network (and its related business) to maintain and/or recover its ability to deliver mobile services to users, in the face of rapidly changing, wide scale disruption brought about by different types of disaster scenarios.

Whilst this contains a degree of robustness i.e. the ability to withstand disruption, it is more about the ability to recover to a point of stability and function sufficient to provide a sustainable service and business going forward. In order to do this the business needs plans and structures to be able to be resourceful and respond quickly to rapidly changing circumstances which in turn rely on built-in redundancy and robustness.

For this report we are considering that there are three aspects to resilience for mobile networks, the first is the effects on people and processes, the second is the recovery of the critical infrastructure, and third the building/recovery of ecosystems which support the business. All of these are interdependent and should be considered holistically as well as at individual levels. For example, providing BTS with backup power generators will help with infrastructure but it needs to be considered within the fuel supply chain ecosystem if it is to be deemed resilient.

Creating more resilient mobile networks to disaster scenarios will require the development of flexible processes which can adapt to the rapidly changing circumstances, the training of staff in these processes and their ability to respond to disaster scenarios.

Engineering robustness into the network infrastructure and providing effective monitoring and re-configuration abilities of the network to provide optimum capacity both during and after a disaster.

Working with external agencies to provide both support to key emergency services and to make sure essential resources can be sourced for the rebuilding and running of the network.

All above activities will help both protect the MNOs long term business and enable humanitarian assistance when it is most needed.

While the focus of this report is business continuity in the face of potential disasters for the MNO, it should be pointed out that as MNOs are “local” businesses which are directly impacted by the disaster and will be key to the long term recovery after the disaster by providing long term employment, key supplementary services such as mobile money, health services, micro-insurance, etc. on top of any CSR work they take on.





# 3.2 Recommendations

## 3.2.1 Recommendation 1 – Planning for resilience through BCM

Business Continuity Management is a key responsibility undertaken by an MNO, especially for those located in highly vulnerable (to disasters) areas of the World, in order to protect their business and provide essential services to support both short term help and longer term recovery for the affected community.

A component of this should be in developing, over time, an innate resilience in the people (staff), infrastructure and business processes to relevant disasters the MNO is potentially exposed to. There should be a balance between the cost of building resilience against the benefits to both the business and to the wider community in the face of a disaster.

## 3.2.2 Recommendation 2 – BCM needs to be a testing and iterative approach

BCM needs to be a constant iterative process which looks to improve resilience with every iteration, otherwise it runs the risk of becoming stale and ineffective in a constantly changing environment where vulnerabilities and the frequency of hazards are increasing.

In order for BCM to be effective it needs to be tested either by simulation or an actual event to see where plans work and where they do not and then to review and update them in order to increase the level of resilience.

### 3.2.3 Recommendation 3 – BCM need for reducing friction and increasing flexibility

In a disaster and its immediate aftermath, there is a high degree of disruption within a rapidly changing environment to be contended with, where even the best plans will never be sufficient to meet all eventualities. For that reason, plans need to allow for a degree of flexibility and room for people to innovate to find effective solutions to the problems they face without facing the burden of operational requirements which could slow down or render solutions ineffective.

This is important when working across different organisations (NGOs, Government, agencies, suppliers, etc.) whose own plans may not be as advanced or aligned to the MNOs. This is where a level of trust and discernment needs to be fostered in order to help find solutions to the issues being faced. This is a key component in establishing resilience across organisations.

### 3.2.4 Recommendation 4 – BCM actions and considerations for disaster scenarios

BCM considerations for specific disaster types are listed in section 7 of this report. BCPs should be created with specific disaster types in mind, as well as for varying levels of severity.






# 4 Business Continuity

# 4 Business continuity planning for disaster response

"Plans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of "emergency" is that it is unexpected, therefore it is not going to happen the way you are planning."

Dwight D. Eisenhower

Business continuity planning (BCP) as the name suggests is about making plans to keep a business going and/or re-constituting the business within an acceptable period of time without doing irreparable harm to the business in the long term, in the aftermath of a disaster (localised or national).

BCP is a constituent process of almost all major businesses such as MNOs and take into account all relevant potential risks (see definition in section 7) facing the organisation (based on initial assessments) from localised disruption e.g. fire in a key facility, up to national and regional wide scale disasters such as earthquakes.

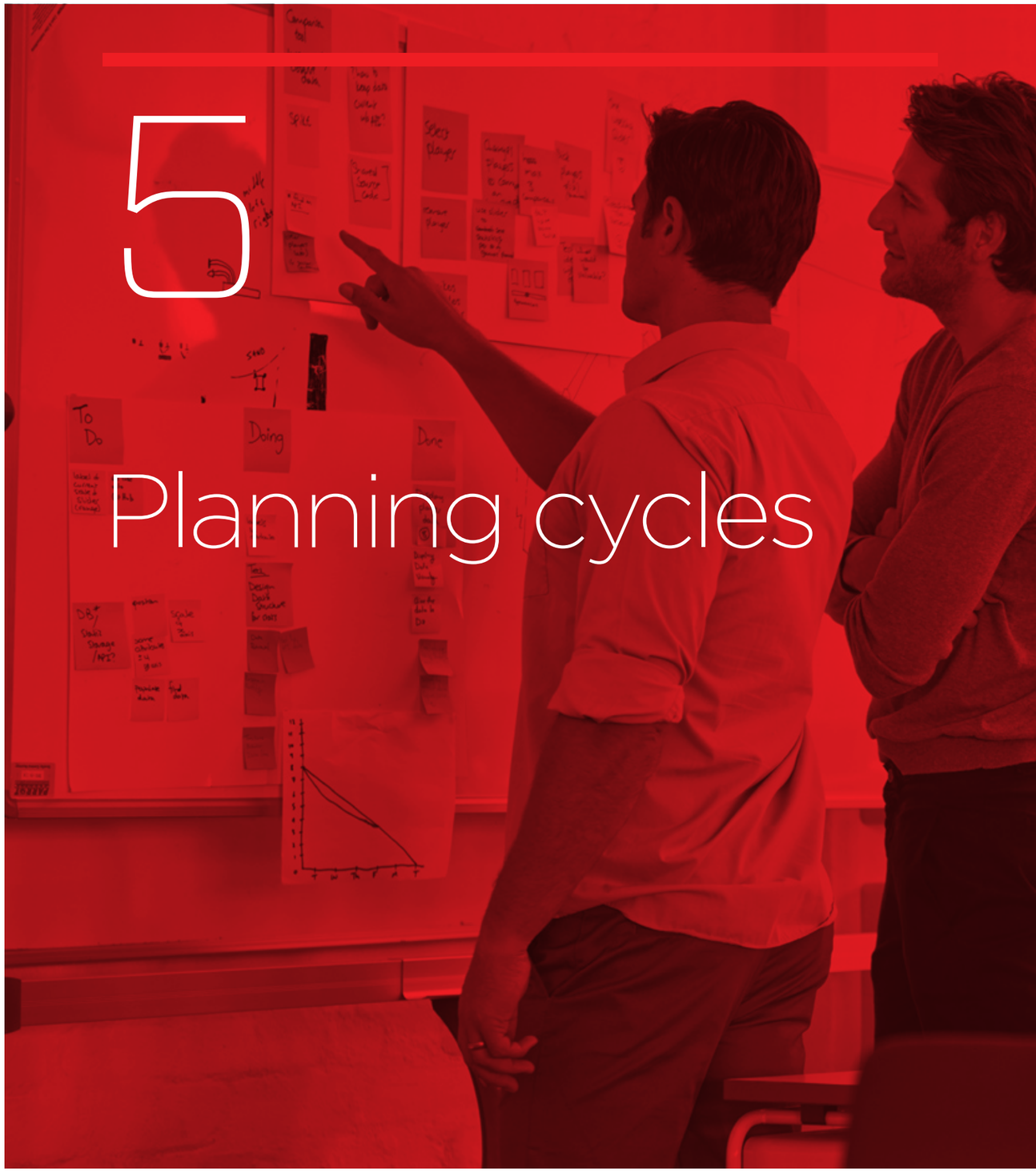
This report covers why and how these BCPs should be extended to incorporate resilience building, in order to also support humanitarian efforts in disaster response.

Mobile telecoms is no longer a "niche" luxury/business service but has grown into the most widespread communication medium across the world. In effect it has become the primary communication channel for much of the worlds population and as such is now deemed as a key or critical resource in times of disaster.

It is routinely relied on by the general populace and key workers (emergency services, government, humanitarian agencies) as a means of communication, information source and point of co-ordination. Hence, the need to restore and make networks and the services they depend upon more resilient in disaster situations. This goes beyond the need for pure business continuity for the MNO. Consequently, there is a much wider need for co-ordination and support to and from the MNO with national authorities, international agencies and NGOs.



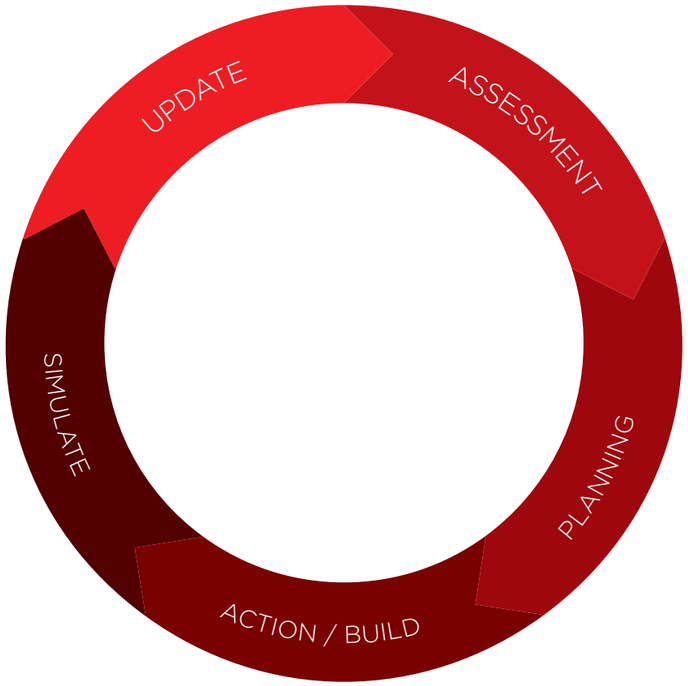





# 5 Planning cycles

# 5.1 Business continuity management (BCM) cycle

This section gives a high level view of the typical planning cycles gone through in BCM and Disaster Risk Reduction. Generally the Business Continuity Process is divided into key five parts usually arranged in a cyclical in nature;




**Business Continuity Cycle**

**Assessment -** This can include risk, vulnerability, hazard and capacity assessments, impact evaluation and criticality determination, in order to provide a clear assessment for the focus areas for the planning and resourcing.

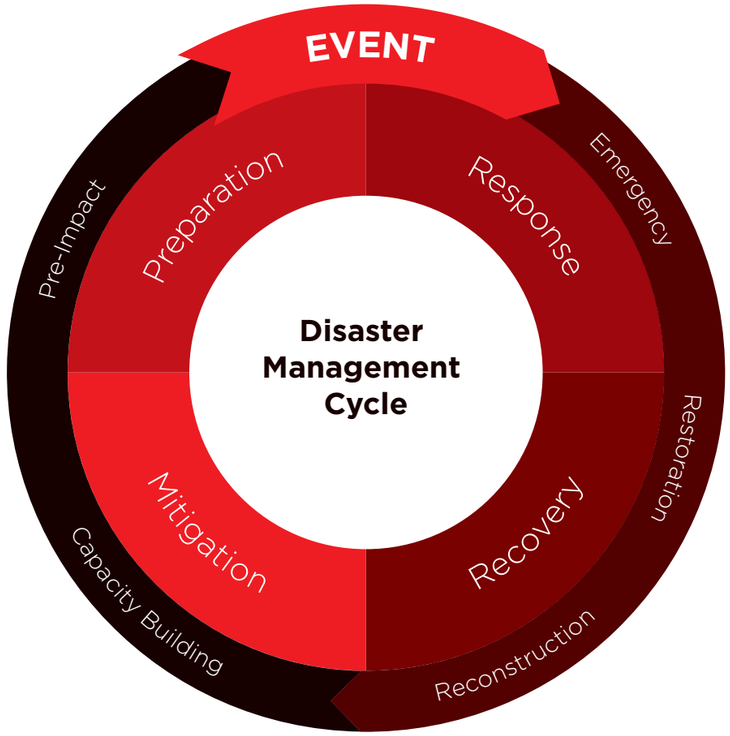
**Planning -** Based on the output of the assessment(s) a core BCM team (reflecting the key sections of the business also known as the Crisis Management Team - CMT) will need to create a BCP which reflects the requirements brought out in the assessments especially in meeting required objectives in order to restore and/or maintain the business (and by inference the network). If the organisation is going through this for the first time it may be expedient to run the BCP creation in parallel with the Assessments and adjust the BCP once the assessments are complete, this way at least a rudimentary BCP will be in place as soon as possible.

**Action/Build -** This part of the cycle focuses on implementing the BCP throughout the organisation and the dependencies identified as critical e.g. power supply from external companies and suppliers. This will involve identifying and training key staff, bringing processes and components up to a required standard, contracting supply chain vendors to comply with the BCP requirements, etc.

**Simulate/Test -** Once the BCP is in place regular simulations should be run based on identified scenarios in the assessments. Ideally these tests should be a mixture of internal simulations and external simulations i.e. working with key dependencies and government level simulations for wide scale disasters. Apart from an actual disaster this will be the most effective way of identifying issues in BCP and rectifying them, plus issues in co-ordination with partners and agencies.

**Update -** BCP should be reviewed on a regular basis and updated accordingly as a result of learnings from simulations, changing standards, business needs and as assessment updates become available.

# 5.2 Disaster response and resilience or disaster risk reduction cycle




**Disaster Response and Resilience Cycle**

A number of models for general Disaster Risk Reduction (DRR) have been researched and published, most of which follow a similar pattern of cyclical phases which fit within three main states of pre-disaster, disaster/impact and post disaster. Although there are other non-cyclical models, as some disasters are not cyclical or regular in nature, this model probably lends itself well to the planning of BCM given its parallels to the BCM cycle.

The key turning point between these states is the disaster itself which in most scenarios is relatively short in nature (two obvious exceptions being disease epidemics and war, in these protracted situations, aspects of the BCP should be incorporated into the everyday operations). During these different states the following phases exist;

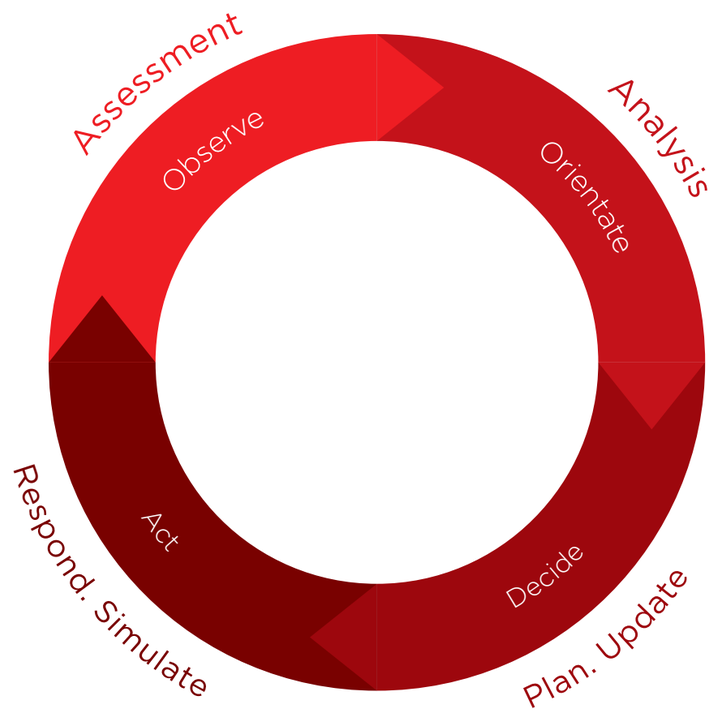
**Preparation (pre-disaster) -** This is where data concerning identified disaster scenarios is gathered and based on the output of the analysis of the data relevant plans are drawn up (such as BCP). Part of this (also shared with mitigation) will be building up relevant capacity in order to provide a degree of resilience to a particular disaster scenario. For example, for an MNO this may be using data analysis on historic CDR (Call Detail Record) data to help determine critical cell sites which can be highlighted in BCP as priority sites and to undergo engineering updates in order to make them more resilient.

**Response (post-disaster) -** This is triggered by the disaster, the conditions for triggering a response are one of the areas which need to be pre-agreed in the preparation along with degrees of severity so that affected organisations like MNOs can map and initiate the relevant action plans (from the BCP) to the scenario and severity. There needs to be a clear chain of authority and communications channel(s) for triggering the response both at a national level and within affected organisations such as MNOs. The response itself will be largely dictated for the MNO by existing BCPs and the directives of the CMT and should be adapted to conditions on the ground.

**Recovery (post-disaster) -** This phase follows on from the initial response phase and looks to re-build any damage to infrastructure, capacity, processes, skills etc. back to the point they were prior to the disaster (or better). It is often hard to define an obvious transition point from response to recovery. The response objective is to recover a pre-determined level and quality (which may be subject to regulation) of service within a time limit (RTO), this may mean taking temporary measures e.g. deploying a COW (Cell on Wheels), whereas recovery looks at the complete restoration of the business.

**Mitigation (post/pre-disaster) -** This is where learnings from the disaster are taken to update infrastructure, processes, etc. to not just improve the business but also increase resilience to future disasters thus adding to a higher level of protection for the business. This will often be tied to national objectives, programs and regulation looking to improve resilience to future events. In some schemas mitigation is defined within recovery and/or preparation phases, so that it is built into the work carried out during the recovery/preparation phases and therefore being more cost effective than more expensive retrofitting. It is important for MNOs to consider this during the recovery phase so any improvements can be tied into the re-investment being made during recovery and indeed during normal operational updates and infrastructure investments.

Both the BCM and DRR cycles have parallels with the OODA loop concept (see below), designed to reduce the time needed to respond to a situation and improve the response to subsequent situations. This is important to MNOs for a number of reasons amongst which is the reputation they have with their subscriber base. For example Turkcell saw the importance of subscribers seeing their service as the “gold standard” during disasters, which is a key influence as to which mobile network users subscribe to.




**John Boyd’s OODA loop**

The Disaster Response and Resilience cycle has a lot of parallels to Boyd’s OODA loop (Observation, Orientation, Decision and Action) which was developed originally for military engagement. Where observation phase collected data about the operational environment, orientation was the analysis phase of the collected data which then led to a decision and the resultant action. This cycle was then repeated as inevitably the action taken would change the environment requiring a re-assessment.

Boyd saw the parallel in engineering, where the loop can be viewed as a self-correcting process of observation, design and test. Consequently, the best outcome for the DRR and BCM processes outlined above is to lead to a self-correcting process.

In the “Resilience Imperative” Andrew Zolli and Ann Marie Healy[4] identified that one of the key aspect to resilient systems was the use of tight feedback loops, such as OODA in order to identify critical thresholds or abrupt change. Consequently, embedding these loops into the business and BCPs is key to providing a degree of resilience.

4. “Resilience: Why Things Bounce Back”, Apr 2013 by Andrew Zolli, Ann Marie Healy





# 5.3 Preparation and process

The first question often asked is why should we go through all this preparation and work for an event, which may or may not happen and if it does, it will never be completely as we plan for?

A disaster by it’s very nature will create a set of circumstances with a great deal of ambiguity about what is actually going on. This along with its unfamiliarity, transience and disruptive nature will combine to disorientate and overload people, systems and processes designed for “normal” or even “peak” operations.

By preparing for disasters and running simulations we help negate these symptoms, which could otherwise paralyze the business’ ability to respond and ultimately its ability to recover. It allows the organisation to help take the initiative, be adaptable to the situation and work more in harmony with suppliers, agencies and the State. All of which will help counteract the impression of danger, uncertainties and mistrust which such circumstances tend to generate.

Operators should aim to build a “command and control” system for use during disasters (BCM), which diminishes both internal and external friction and compresses the time needed to respond on key processes, thereby gaining speed and in turn increasing the organisation's resilience to the disaster. This should allow for staff and suppliers to innovate both in the process and in what is needed which may be able to be constructed from the limited resources available. A good example of this is during the 2015 earthquake in Nepal staff at NCell were able to build a number of COWs from existing telecoms kit, generators and some pickup trucks. [5]


**Innovating with existing resources**

5. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/12/GSMA_Disaster-Response_Nepal_Workshop.pdf

We use the term “command and control”, however the reality is in order to achieve the above the foundation of this is a much higher level of trust both within parties in the organisation and with external agents. This can only be effectively fostered prior to the impact of a disaster.

Whilst the majority of this report looks at the need to build resilience to counteract disaster scenarios to the network and the business, it should also be recognised that not all hazards come directly from the actual disaster but also from pressures external to the MNO such as government regulation, priorities, organisational change, political instability, suppliers, etc. For example, the hazard from flooding will be exacerbated by measures not taken by authorities to build flood defences thereby effectively putting the onus on the MNO to make key infrastructure resilient to flooding.

Ideally resilience efforts for the entailed risks should be shared between the public and private sectors through agreed funding, incentives and where necessary regulation but the latter should be not be used for pushing unreasonable costs onto the private sector. Pragmatically, MNOs will need to focus on those areas which they can reasonably influence, whilst being aware of the effects of those they cannot. For example, the MNO will typically work closely with the telecom regulator(s), to ensure pragmatic regulation during disaster situations but they are unlikely to be able to affect political instability in a region.

In order to avoid a “Groundhog Day” approach, where with each disaster the same vulnerabilities are built back in, at the same or escalating cost, the aim ultimately of any BCM and BCP is to allow the business to “bounce back”, when you take into account the need to improve resilience in the longer term, it would be more accurate to use the term “bounce forward” or “build back better” the intent being not just that the network and business is recovered to where it was before the disaster but that it is recovered to point which is more resilient than before the disaster struck. For example, when NTT DoCoMo rebuilt their cell towers after the 2011 Tsunami they planned in around 100 large-radio-zone base stations which (when needed) could provide coverage over 360° for 7 km radius and compensate for damage caused to regular base stations. [6]

6. NTT DoCoMo Technical Journal, Volume 13, No. 4 “Measures for Recovery from the Great East Japan Earthquake”

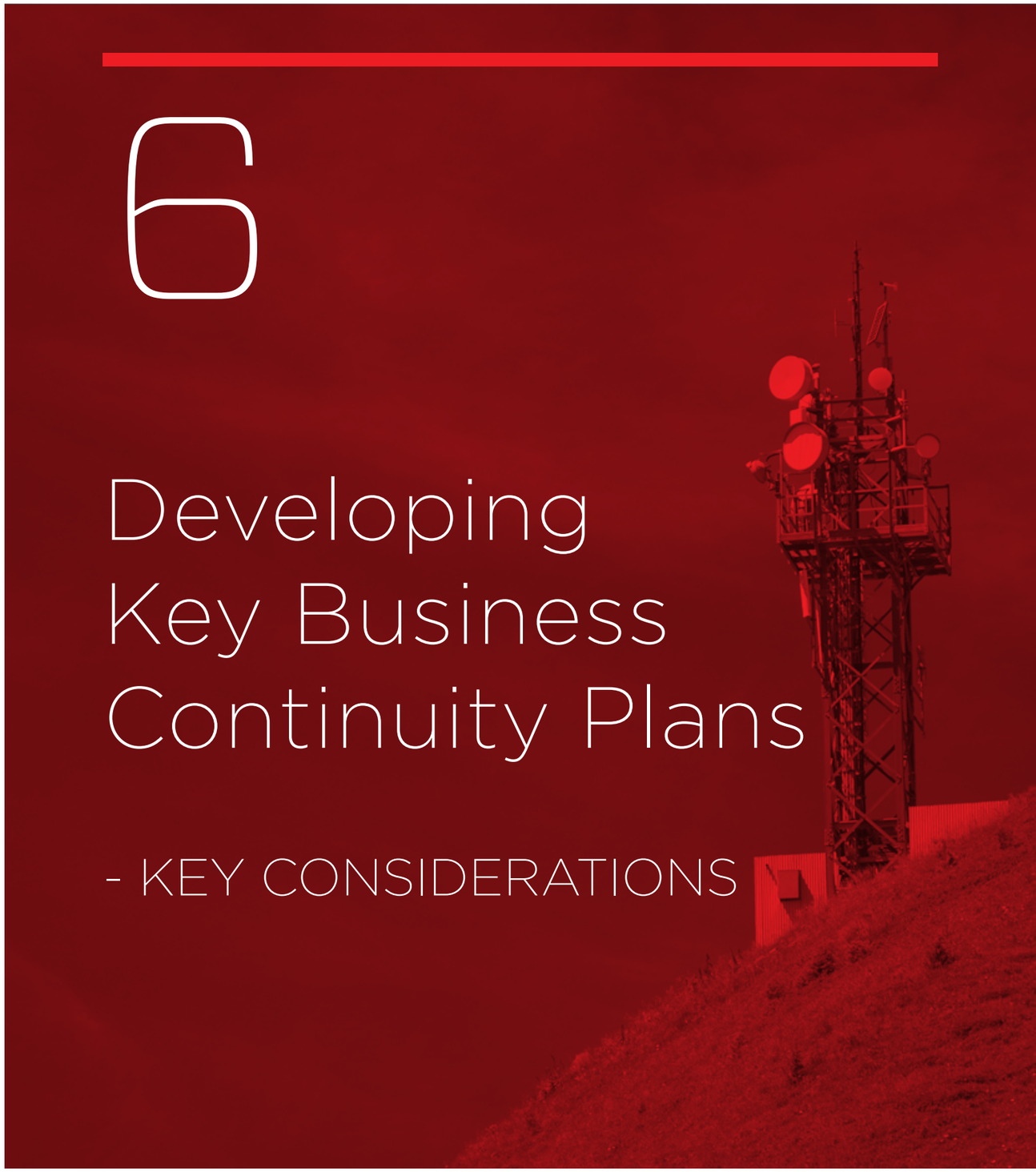




# 6

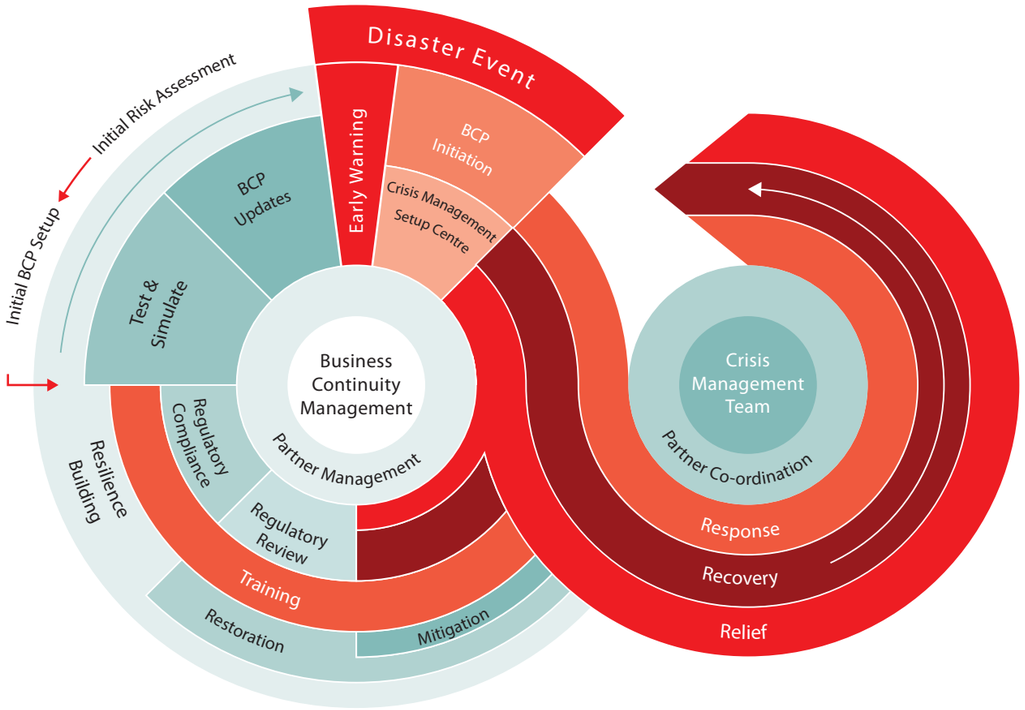
# Developing Key Business Continuity Plans

## - KEY CONSIDERATIONS



# 6.1 Introduction

This section is intended to be a reference section on actions and considerations to be taken into account when developing BCPs. It will show the overall actions and plans which should be considered for all disaster scenarios. Figure 1 provides an overview of a potential BCP development cycle.



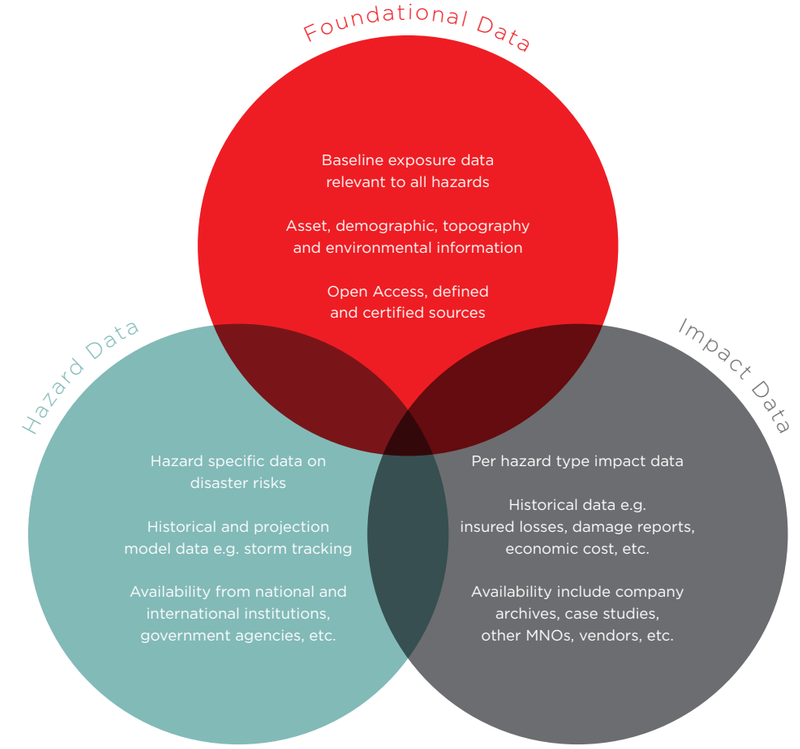

**Detailed example of a potential BCP cycle**





# 6.2 Disaster data

A basic requirement to any planning and decision making in disaster risk reduction and business continuity planning is the available source data. Data sources can be seen as three main intersecting sources as shown below.




**Data for DRR and BCP**

All too often these data sources are either not available, inconsistent, or expensive to use (licensing costs, research time). Ideally government agencies, institutions, and private companies should make such data available as far as they are able (given commercial and privacy sensitivities), to enable more accurate risk assessment and resilience planning.

# 6.3 Common to disasters

This section highlights some of the key actions and plans to be considered by MNOs for all types of disasters. Below this in the specific scenarios anything specific to those disasters will be highlighted, in all these cases the generic tasks below should be considered as part of those scenarios.



## 6.3.1 Data

### Foundation data

| Category | Data requirements | Data sources |
|---|---|---|
| Assets | Asset types<br>Asset location<br>Asset data | MNO, Vendor, Local and national government. |
| Demographics | Population maps and densities<br>Socio-economic status | National government, research institutions, MNO marketing dept. |
| Topography | Elevation<br>Land surface<br>Geological | Governments, international agencies, institutions, etc. |
| Environmental | Rainfall, wind speed/direction, temperature, tides, cloud coverage, atc. | Government metrological agencies, international institutions and commercial info sources. |

### Impact data

| Category | Data requirements | Data sources |
|---|---|---|
| Economic | Insured losses | MNO, insurance companies, government |
| | Buildings and structural damage | National emergency agency, Professional Associations |
| | Infrastructure damage – network, ICT, utility, transport, etc. | MNO, Utilities, Government. |
| | Human fatalities, injuries, migration, displacement, evacuations | Government, NGO, MNO (data analytics) |
| | Response and recovery costs | MNO, Insurer, Vendors, NGO, Emergency services |

# 6.3.2 Operations

## Staff

This section outlines the actions and plans which should be considered in terms of access and transportation in the management of a disaster response and in managing staff during a disaster.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **All** | • Setup BCM roles and responsibilities<br>• Construct asset register<br>• Set up and test staff call chains<br>• Plan staff evacuations<br>• Run internal staff simulations/drills<br>• Notify staff of plans<br>• Setup Disaster Management Committee<br>• Setup strategic corporate BCP<br>• Setup departmental BCM teams and responsibilities<br>• Maintenance function staff plans for disaster recovery<br>• Setup funding plans<br>• Identify key staff<br>• Setup expedited immigration plans for key support staff<br>• Setup corporate communications plan<br>• Setup tactical departmental BCPs<br>• Setup funds release processes<br>• Setup reporting processes<br>• Setup disaster fund management and processes | • Initiate Disaster Response Centre<br>• Open up communications with National Emergency Operation Centres | • Assess effectiveness of staffing plans and adjust<br>• Incentivise key staff to increase availability e.g. structural compliance for homes , etc.<br>• Refresh PoCs<br>• Refresh existing plans Update simulations |
| **Damaging** | • Plan damage assessment roster with damage assessment plans | • Initiate departmental responsibilities and plans<br>• Activate relevant response teams<br>• Initiate damage assessment roster<br>• Initiate temporary evacuations for affected sites<br>• Carry out damage rectification<br>• Initiate departmental reporting<br>• Initiate data gathering plans<br>• Initiate local funding mechanisms | • Improve structural resilience of infrastructure and housing facilities. |
| **Destructive** | • Staff risk assessment<br>• Staff contact and evacuation plan<br>• Staff training<br>• Medical and family support plan<br>• External staff resourcing plan<br>• Establish internal PoC<br>• Establish external PoC<br>• “Work from home” plans for non-key onsite staff<br>• Emergency medical assistance plan and communicate<br>• HR Disaster plan<br>• Run internal and external staff simulations/drills<br>• Setup CSR plans and partnerships | • Initiate evacuation plans<br>• Initiate Emergency medical assistance as needed<br>• Secure core team and key staff<br>• Convene Disaster Management Committee (Internal)<br>• Initiate funding plans and processes<br>• Initiate representation at national DR committees (External)<br>• Convene departmental BCM teams<br>• Initiate staff plans<br>• Assess need for external staffing and initiate accordingly<br>• Initiate facility safety assessments<br>• Initiate group communication plans<br>• Initiate internal reporting processes<br>• Initiate external reporting processes/systems.<br>• Initiate CSR plans & partner contacts<br>• Deploy emergency communications for emergency services and critical supply chain partners.<br>• Release emergency funding as required. | • Assess any funding gaps for future planning<br>• Asset management improvement programme |
| **Devastating** | • Update PoC for international and governmental organisations. | • Initiate staffing requests to external bodies | • Improve structural resilience of infrastructure and housing facilities. |

# Access & Transportation

This section outlines the actions and plans which should be considered for MNO staff and BCM both in the management of a disaster response and in managing staff during a disaster.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Update site security plans for disaster scenarios<br>• Transport procurement plans, specific to air and all terrain needs<br>• Site and facility monitoring and contact plans<br>• Key access routes monitoring plans<br>• Migration (subscriber) monitoring plans | • Initiate Disaster Response Centre<br>• Open up communications with National Emergency Operation Centres | • Assess effectiveness of staffing plans and adjust<br>• Incentivise key staff to increase availability e.g. structural compliance for homes , etc.<br>• Refresh PoCs<br>• Refresh existing plans Update simulations |
| **Damaging** | • Site access contact and check procedure | • Initiate transport procurement plans<br>• Monitor and disseminate information and transport links | |
| **Destructive** | • Alternative transport plans<br>• Distribution plan of COWs, COLTs, etc. | • Initiate COW and equipment distribution plans | |
| **Devastating** | • Transport co-ordination plans with state and international agencies<br>• Transport information sharing plans with international agencies | • Initiate state and agency transport co-ordination plans | |





# Supply Chain

This section outlines the actions and plans which should be considered to recover and keep key supply chains up and running both within the MNO and with external suppliers, agencies and governmental departments.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Plan geo-redundant emergency procurement plans<br>• Internal supply chain review<br>• External supply chain review<br>• Supply chain re-configuration for resilience | • Initiate Disaster Response Centre<br>• Open up communications with National Emergency Operation Centres | • Assess effectiveness of staffing plans and adjust<br>• Incentivise key staff to increase availability e.g. structural compliance for homes , etc.<br>• Refresh PoCs<br>• Refresh existing plans Update simulations |
| **Damaging** | • Plan geo-redundant emergency procurement plans<br>• Internal supply chain review<br>• External supply chain review<br>• Supply chain re-configuration for resilience | • Initiate local supply chain plans as required | • Review local supply chain effectiveness |
| **Destructive** | • External party inventory review and allocation | • Initiate supply chain plans, internal and external. | • Review internal and external supply chain effectiveness |
| **Devastating** | • Import supply chain planning<br>• Regulatory approval process for importing | • Initiate import processes | • Review out of country import processes and response.<br>• Update governmental agencies on issues found. |

# 6.3.3 Infrastructure

## Edge

This section outlines the actions and plans which should be considered from an infrastructure and technology point of view.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Prepare equipment sourcing plans<br>• Setup vendor expedited supply chain plan<br>• Plan and implement power reserve for BTS, to meet any regulatory requirement<br>• Setup fuel and consumables replenishment supply chain plans.<br>• Prepare extended coverage plan.<br>- CoW placement<br>- Spectrum reallocation<br>- Overlay cell coverage<br>• Plan for temporary /permanent large-radio-zone BTS and siting.<br>• Gain regulatory approvals and agreements on RTO.<br>• Identify critical cell site placements and BTS siting agreements with regulator, permanent and/or temporary. | • Monitor equipment availability and status | • Post disaster review of plans and effectivenes |
| **Damaging** | • Prepare damage assessment training and plans<br>• Identify critical base station locations and prioritised recovery plans | • Initiate damage assessment plans<br>• Initiate damage rectification plans | • Compile and analyse equipment damage reports |
| **Destructive** | • Alternative transport plans<br>• Distribution plan of COWs, COLTs, etc. | • Initiate equipment procurement plans<br>• Initiate extended coverage plans<br>• Update regulatory authorities | • Review out of country import processes and response<br>• Update governmental agencies on issues found |
| **Devastating** | • Plan for information sharing on coverage with external agencies | • Initiate coverage and damage assessment sharing plans | • Assess information sharing effectiveness and security |



GSMA DISASTER RESPONSE

# Network

This section outlines the actions and plans which should be considered to monitor, assess, maintain and repair transmission equipment and lines which enable the backhaul of communications in the network e.g. fibre, VSAT, Microwave/LOS, network topolgy, etc.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Input into network topology changes and upgrades in order increase resilience.<br>• Network link monitoring plans<br>• Prepare network link cut repair and access plans<br>• Keep network plans up-to-date and provide accessibility to BCM team<br>• Network Virtualization plans.<br>• Short term replacement equipment testing (e.g. CoWs, VSAT, High performance antennas, etc.)<br>• Contingency plans with satellite companies for backhaul bandwidth increases during emergencies. | • Monitor line availability and performance | • Post disaster review of plans and effectiveness |
| **Damaging** | • Prepare network link damage assessment training and plans<br>• Plan emergency break (fibre, cable, etc.) repair capabilities and equipment. | • Initiate damage assessment plans<br>• Initiate damage rectification plans | • Compile and analyse network damage reports |
| **Destructive** | • Simulate network disruption with different types of cut scenarios | • Initiate equipment/capacity procurement plans<br>• Update regulatory authorities | • Assess network channel disruption and re-assess repair and design plans<br>• Plan-in fibre/backbone improvements in restoration plans. |





# Core

This section outlines the actions and plans which should be considered to monitor, assess, maintain and repair equipment at the core of the network e.g. data centres, NOC, OSS/BSS, etc.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • ICT disaster recovery plans<br>- Redundancy and automated switch over plans for NE and OSS<br>• NE OSS monitoring plans<br>• ICT resilience plans (bracing, building codes adherence, etc.) | • Monitor NE availability and performance<br>• Monitor OSS failure processing and availability. | • Post disaster review of plans and effectiveness |
| **Damaging** | • Prepare NE and OSS damage assessment training and plans | • Initiate NE damage assessment plans<br>• Initiate NE damage rectification plans | • Compile and analyse NE damage reports<br>• Compile and analyse OSS failure handling processes |
| **Destructive** | • Simulate NE and OSS disruption with different types of failure scenarios | • Initiate equipment/capacity procurement plans | • Assess NE and OSS disruption and re-assess repair and design plans |
| **Devastating** | • Provision of automated network availability information for external agencies. | • Initiate national disaster recovery plans for NE and OSS | • Assess external providers delivery and any related regulatory processes. |

## 6.3.4 Usage

## Demand

This section outlines the actions and plans which should be considered to help meet and mitigate the high levels of demand placed on the network during a disaster.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Emergency network congestion plan<br>- Capacity measures<br>- Coverage measures<br>• Regulatory agreements on spectrum re-use and cell adaptation<br>• Subscriber educational program<br>• Develop and test disaster comm's app | • Initiate congestion measures based on system alerts/warnings | • Review subscriber traffic patterns and congestion issues to improve network plans and subscriber communication updates |
| **Damaging** | | • Initiate local congestion plans | |
| **Destructive** | • Prioritisation plan for essential services | • Initiate national congestion plans | • Identify vulnerable (to congestion) cells and update capacity and shaping plans |
| **Devastating** | • External agency migration plans between autonomous comm's and MNO coverage | • Alert external agencies<br>• Alert regulator to actions taken. | • Correct temporary measures taken during emergency. |

One key consideration on demand may be external to the MNO, where operators in other countries with significant diasporas from the region, may setup zero-rated tariffs for people trying to call into the affected area, which inevitably will compound congestion issues within the affected area. Operators outside the affected region should consider this and where possible check with the local MNOs first and/or encourage their users to use alternative methods such as SMS or SNS which will not have the same level of affect on the local network as voice calls. Also the MNOs in the affected areas along with the incumbent landline teleco may want to upgrade international calling capacity in their switches.





## Subscribers

This section outlines the actions and plans which should be considered to help meet the needs of subscribers on the network to continue to use the network effectively during and in the immediate aftermath of the disaster.

| Severity | Pre-Disaster Actions | During & Post-Disaster Actions | Resilience Improvement |
|---|---|---|---|
| **General** | • Communications plan<br>- Subscriber mobile use effectiveness in DR<br>- Early warning notifications and drill<br>- Media handling<br>• Agent support plan | • Initiate early warning systems | • Review media and subscriber communications plan effectiveness and update. |
| **Damaging** | • Early warning plans<br>• Early warning simulations | | |
| **Destructive** | • Subscriber credit plans<br>• Phone charging solution planning | • Initiate subscriber support plans for affected population | • Review credit and termination plans and update. |
| **Devastating** | • Subscriber termination suspension plans<br>• Roaming subscribers plans in-country and out of country<br>• Aid and Government agency staff support plan | • Initiate out-of-country roaming and agency support plans | • Review external agency support plans and update |

# 6.4 Technical considerations

This section looks at some technical issues and solutions for mobile networks in disasters. For more details, please our previous publication “Dealing with Disasters - Technical Challenges for Mobile Operators”.

## Warning systems

Early warning systems for disasters (or Public early Warning Systems -PWS) are a key tool in minimising the loss of life, and key in initiating BCPs effectively. A good system will by necessity have a multi channel approach (i.e. TV, Radio, Mobile, etc.), one of the key channels due to its reach will be over the mobile networks. This may take the form of Cell Broadcast (see detailed case study in “Mobile Network Public Warning Systems and the Rise of Cell-Broadcast”), SMS, IVR, Disaster alert app (see NTT DoCoMo “Area Mail” app[1] ), etc.

The effectiveness of PWS in combination with other DRR efforts (e.g. Cyclone shelters) in Bangladesh has seen casualties in comparable cyclones in 1970 of nearly 300,000, down to 139,000 in the 1991 Cyclone and most recently in 2007 Cyclone “SIDR” saw 3,363 casualties. Also see the GSMA Case Study on “DEWN – Dialog’s Disaster and Emergency Warning Network”,

7. NTT DoCoMo Technical Journal Volume 15, No. 1, “Delivering Tsunami warnings via “Area Mail” Early Warning System.





Another aspect is in the use of mobile networks both directly and indirectly to help provide detection of the early signs of impending disasters, through the likes of;

**Linking remote sensor networks** and linking them to national alert programs.

**Drawing data and analytics from crowd sourcing apps on smart phones,** an example being the MyShake Project being run by the University of California Berkeley, where the app uses the sensors in the phone to help detect potential earthquakes (current smartphone accelerometer technology is sufficient to detect 5.0+ earthquakes). Taking this approach helps them achieve an order of magnitude difference in the density of their sensor network, even though they are by nature less accurate than ground based dedicated sensors[8].

**Monitoring of SNS (Social Networking Services),** can also help detect and inform authorities of disaster issues. In Japan they have been pioneering this technology to monitor, filter, analyze and raise alarms accordingly.

8. http://myshake.berkeley.edu

Key to PWS working across multiple channels and partners is the use of standardized protocols, the key one for this being the Common Alerting Protocol (CAP), see box below;

### Common Alerting Protocol

The Common Alerting Protocol (CAP) is an XML-based data format that standardises and simplifies the exchange of data for public warnings and emergencies between alerting technology types. CAP allows a warning message to be consistently transmitted simultaneously over multiple warning systems to many different applications e.g. TV, radio, mobile phone, fixed phone or public signage.

CAP increases warning effectiveness and simplifies the task of activating a warning for those responsible for issuing them. However, like many protocols, CAP does not address any particular application or telecommunications method but rather addresses the message itself.

**Key benefits of CAP include:**

- Reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning system inputs/outputs.
- Message formats can be converted to and from the “native” formats of all kinds of sensor and alerting technologies.
- Formation of a basis for a technology-agnostic national and international “warning internet.” CAP forms the basis of emergency alert services run by many multi-agency bodies around the world including those in the US by the Dept. of Homeland Security/FEMA and by the National, State and Territory governments in Australia.





## Infrastructure Resilience

Infrastructure resilience will be decided by a number of factors, key amongst these will be power, backhaul and core infrastructure. A central capability to this is redundancy, this is a fundamental component in building resilience into mobile networks. The benefits of redundancy will always to be balanced against the cost to implement such measures. Below are a few of the key areas where redundancy can play a crucial role;

**Power** has a number of well proven backups from batteries to diesel generators and increasingly renewable power alternatives. One area of further research for backup power for disaster situations, where grid power could be disrupted for days, is in the use of fuel cell technology, which could have a longer “burn” time without being so susceptible to the effects of the disaster.

**Backhaul resilience** lies in a combination of redundant channels e.g. fibre, satellite, micro-wave, etc. available to each node and the design of the network, where a mesh based design will be more effective in reducing the chances of a complete outage for a node (or parts of the network) as it has more than one path available to it on the network. For example the re-routing of Inter-core signalling over a VSAT connection (2+ Mbps).

**Increasingly** the ability to “virtualise” the network (i.e. the move from a highly centralised to a distributed network concept) will help build resilience as this will allow for dynamic re-configuration of the network and virtual routers, etc.

| | Better | | | | | Worse |
|---|---|---|---|---|---|---|
| Criteria | Solar | Wind | Pico-hydro | Biodiesel | Fuel Cells | Fossil Diesel |
| Overall Ranking | | | | | | |
| CAPEX | | | | ** | *** | |
| OPEX | | | | | | |
| Reliability | | | | | | |
| Supplier Availability | | | ? | | | |
| Theft Resistance | | | | | | |
| Public Green Image | | | | | | |
| Opperational Supply Chain Predictability | | | | | | |
| Output Predictability * | | | | | | |
| Resource Ability | | | | | | |

| Key | Very Good | Good | Okay | Poor | Very Poor |
|---|---|---|---|---|---|

**Backup power "green" effectiveness**





The equipment on the edge of the network in most scenarios are the most susceptible to the effects of the disaster, the most obvious being the BTS/RNC and their masts/towers. Here a number strategies exist such as;

**Cells on Wheels (COW)** is a versatile solution for providing coverage for affected areas and cells. Both in geographical coverage and in covering increased traffic at key facilities e.g. refugee camps, hospitals, etc.

**Collapsible mast/tower,** in areas where there is a possibility of damage by severe weather e.g. wind, sufficient lead time in early warning can allow engineers to temporarily shutdown the cell and brace it against the effects of the disaster. This means that it is more likely that service can be restored quicker in the aftermath of the disaster. Although the cost of this is loss of coverage just prior to and during the disaster, which may not be acceptable for key emergency services which rely on the networks availability. However, this approach used selectively in combination with an umbrella coverage type approach may add resilience without dropping coverage entirely.

**Umbrella/large radio zone base stations,** this is where certain critical base stations in the network which have an advantageous geographical positioning are built to be able to cover wider areas, so they can continue coverage when adjacent cells are affected by the disaster (if at a lower capacity). These base stations are typically built to a higher standard of robustness and redundancy, so they can continue to function both during and in the aftermath of a disaster.

**Tower sharing,** may have a negative effect on resilience, whilst often encouraged by regulators for economic and civil disruption purposes, this may have a detrimental effect on overall network resilience as any destruction of a tower will affect all the MNOs coverage in an area not just one network, leading to an effective reduction in redundancy.

MNO systems, which comprise the core of the network and support both service provision and VAS are typically sited in centralised hubs such as Network Operation Centres (NOC) and ICT Data Centres. These centres can be vulnerable to both widespread (earthquake) and localised (fire) disasters, consequently are built to a high standard of resilience both in terms buildings and physical protection e.g. bracing, and in terms of systems failure e.g. server failure. Some of the methods employed include;

**Geo-redundancy,** this is where centres geographically separated from each other have the capacity to take over the load from another centre should it fail e.g. HLR.

**Service and BSS duplication,** this entails running systems which mirror each other (often in separate locations), so if one fails the other can pick up the load with immediate effect e.g. Data-core (SGSN, GGSN).

**Overload handling,** running redundant capacity so that if and when systems become overloaded extra capacity can be added to handle the traffic. This also requires a monitoring system which is configured to handle exceptional circumstances generated by the disaster, this is where simulation is an effective tool.

**MSC pool,** this is where several MSC are interconnected to form a pool which can share resources and logical connections to all the BTS being served. This can allow for real-time switching between MSCs, reduce the impact of handovers as populations move away from affected areas and help load sharing the traffic surge on the network which affects most networks during a disaster.

## Network congestion

Although not strictly a solution for congestion, allowing for national inter-operator roaming will allow users access to whichever network is available in their area after the disaster. This will need to be carefully negotiated and configured between MNOs and with the telecom regulator. On issues such as what should be the trigger points for opening up roaming (and closing), intermediation between MNOs on charging and a harmonisation of tariffs during a disaster e.g. if one MNO offers a zero rated approach versus a credit top up approach of another MNO.

One common method of attempting to alleviate call congestion on the network is by switching compression codecs for OTA interface (beyond the MSC/TRAU) from FR/EFR to Half-rate (HR) which effectively doubles the capacity (13 Kbit/s to 7 Kbit/s) at the cost of audio quality. Where available (UMTS/3G) it may also be worth considering an appropriately configured AMR codec which will give the same bandwidth saving with less of a hit on audio quality.

The other benefit of using HR/AMR is where the default backhaul from the BSC/RNC to the MSC is damaged or cut and the BSC/RNC has to switch to a lower bandwidth redundant backhaul channel e.g. VSAT, using HR/AMR will help make the best use of the lower bandwidth i.e. the number of simultaneous calls which can be supported.

The release of the 3GPP standards for 4G/LTE mobile networks has included Self Optimising Network capabilities especially in Release 9 onwards which covers coverage, capacity, mobility and load balancing optimizations with the aim of self configuring, optimizing and healing networks. This clearly would be advantageous to maximising mobile network availability during and post disaster and points the way to which mobile networks will become more resilient as they are upgraded in the future.

The constraints of opening up additional capacity to deal with (assuming the infrastructure is available), comes down to a number of items;

**Physical infrastructure constraints** e.g. capacity of the transmitters on the towers, backhaul capacity, etc.

**Licensing,** many of the software based systems in a mobile network work off licensing agreements with the relevant vendors, some of these licenses may be volume/capacity linked, where the amount paid to the vendor is linked to particular usage patterns. For a crisis situation MNOs should have agreements and processes in place to allow for additional temporary licensing. This may include manual overrides where dynamic licensing servers of the vendor cannot be reached to do any needed re-configuration.

**Available spectrum,** typically the MNOs spectrum license will cover certain bandwidth which have a finite capacity for calls, data, signalling for emergency scenarios. It may be worth exploring with the regulator and other MNOs the possibility of re-configuring the network during a crisis to make use of adjacent spectrum either for the radio network and/or capacity for micro-wave backhaul. This is a complex solution and would need to be agreed well in advance of any crisis, so technical solutions can be made ready and tested.

**In country roaming,** another potential solution to help congestion would be to allow users to roam to other networks “in country” so they can make use of whatever capacity was available in their area. This will need to be agreed in advance with both regulators and other MNOs in the region. Plus the necessary configuration tested and trigger points for opening and closing the service to be clearly defined and agreed by all parties.





## Mobile Apps

A number of agencies and MNOs have developed mobile apps to help assist both their staff and the general populace for disaster scenarios providing functionality such as;

Early warning of a disaster event

Informational services for specific events e.g. location of refuge centres, quarantine areas, preventative health information, etc.

Communication services e.g. family reuniting, offline messaging, voice messaging over IP, message board, etc.

Information upload of local situations, text, pictures, etc.

Staff specific functionality e.g. outage maps, hazard assessment methods, contact numbers, procurement processes, etc.Some example apps are;

NTT DoCoMo Disaster Kit App

Pacific Disaster Centre Disaster Alert App

Dialog’s DEWN disaster alert app

Federal Emergency Management Agency (FEMA) App

## Transportation

As a large part of MNO infrastructure is geographically spread over a large area, often encompassing remote areas not always easily accessible even in normal circumstances, transportation to key facilities during a disaster, to assess and restore physical network assets is critical. The BCP should take account for the use of transportation not used in normal operations, for example, all terrain vehicles or helicopters due to the disruption caused by the disaster, such as broken transport links, civil unrest, etc.

Some transport methods may also become restricted due to demand during a disaster, so having pre-arranged priority access agreed in advance with the relevant authorities and/or arrangements to share emergency transport facilities.

Transportation of equipment

Observation – damage assessment

Network augmentation (Wi-Fi)





# 7

# Disaster scenarios

## BCM considerations for specific disaster types

# 7.1 Introduction

In section 6 key actions and considerations to be taken into account when developing BCPs were outlined. This section of the report will focus on specific BCM actions to be considered when preparing for particular event types.

It is intended that the document will be updated on regular basis to increase the depth of knowledge for a specific scenario and to add coverage for more scenarios over time.

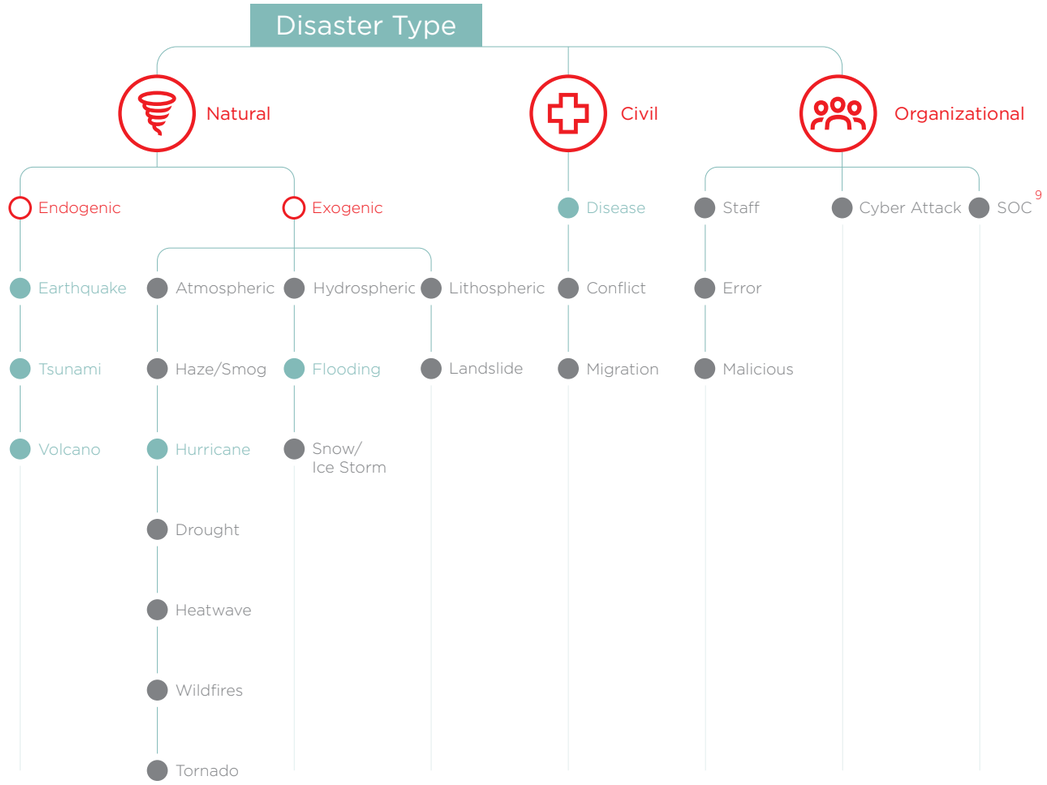
If you wish to submit additional information for a scenario or suggestions for other items you would like to see covered please contact us on **disasterresponse@gsma.com**

When considering BCP in respect of DR one consideration (most often in assessment) is the nature and causation of potential disasters which an organisation and region can be prone to. In order to do this, it can be useful to build up a taxonomy that applies to the organisation and region.





Below is an example taxonomy and the effects on the network by the variations;




**Disaster Type Taxonomy**

Initially this report will focus on the scenario's highlighted above i.e. Earthquake, Tsunami, Hurricane/Cyclone, Flooding and Disease. It is hoped that over time this document will be updated to expand on the information on each scenario and to extend the number of scenario's covered.

9. SOC stands for a Self-Organized Criticality, this is where a sequence of small and/or large events snowball into a major or catastrophic disaster for the network, possibly started by the initial effects of a disaster e.g. the Fuchashima nuclear plant in the Great East Japan Earthquake followed by the tsunami led to an unforeseen sequence of events which led to a catastrophic failure.

# 7.2 Tsunami

## 7.2.1 Onset

Whilst there is often little or no warning of the seismic activity responsible for the causation of Tsunami's, the likelihood of a Tsunami itself can be predicted based on the seismic activity and related (computer) modelling, along with early warning sensors (e.g. seabed pressure monitors), giving potential warning ranging from hours to minutes.

At best this will only give organisations the ability to execute the early part of the BCP e.g. warning staff, securing immediate facilities, initiate disaster monitoring systems, etc.

| Agency | Link | Region |
|---|---|---|
| NOAA (US) | http://www.noaa.govICG/ | Pacific/Atlantic |
| ICG/IOTWS | http://iotic.ioc-unesco.org | Indian Ocean |

## 7.2.2 Hazard data

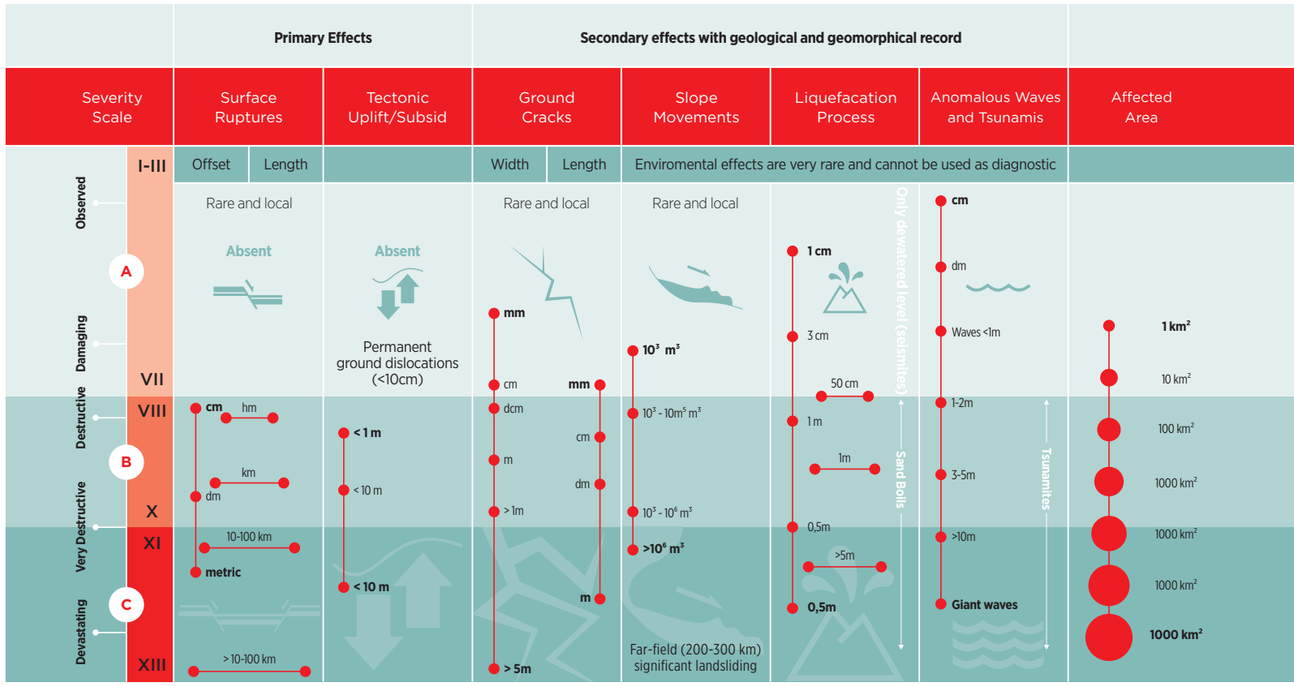
| Category | Data requirements | Data Sources |
|---|---|---|
| Tsunami | Mapping of wave height and velocity | Local governments, Meteorological Agency, private firms, researchers |
| | Tsunami prediction | Meteorological Agency, private firms, researcher |
| | Hazard maps | Local governments, private firms, researchers |





## 7.2.3 Crisis definitions

The definition of the level of effect of a Tsunami is most often linked to the ESI 2007[10] or European macroseismic scale (EMS)[11] definitions.




**ESI 2007 Seismic Activity Scale**

In most circumstances the business will need to plan for level VIII and above and any plans should be linked to the scale of the disaster e.g. for a level VIII event, there may only need to be checks initiated for low level damage assessment at identified vulnerable sites and facilities.

10. https://en.wikipedia.org/wiki/Environmental_Seismic_Intensity_scale

11. https://en.wikipedia.org/wiki/European_macroseismic_scale

# 7.2.4 Operations

## Staff

The effects on staffing from a Tsunami will be dependant on the scale of the disaster and the proximity of staff to coastal areas during both work and personal times.

Setup early warning feeds for staff where available (e.g. NTT App)

Plan damage assessment roster with specific water/flood damage assessment plans.

Water damage rectification

Re-route/site water sensitive equipment

## Access/transportation

During and immediately after a tsunami incident, routes to key infrastructure in the affected area will most likely be very difficult to get through due to flooding, damage and debris. Consequently transportation planning will need to account for modes of transport required e.g. all terrain vehicles, boats, helicopters, etc.

In order to secure availability of these resources may mean working with both private and state resources e.g. the army, both of which will require substantial planning and prioritisation with the third parties especially in the case of using state resources.

Transport procurement plans, specific to water and all terrain needs





## Supply Chain

Effective maintenance of the mobile network under normal working conditions is subject to numerous supply chains both internal and external to the MNO. During disasters these will be stressed significantly often beyond breaking point.

It is key that the critical supply chains are identified, tested and reinforced so they can withstand the likely scenario's which they will face during a disaster. An example would be Turkcell when reviewing their fuel supply chain (for BTS backup power generators) identified that their supplier's depots were centralised in a couple of key centres. This meant that where a disaster significantly disrupted key arterial routes into a region the fuel supply would not be able to meet the relevant RTO (Recovery Time Objective). The solution was to enforce the RTO through the supply chain and work with the supplier to re-configure their distribution network so the RTO could be met in various disaster scenarios.

Another key supply chain will be in the supply of replacement equipment damaged by the disaster both in terms of the equipment and the accompanying engineering resources. This may have at least two implications first the availability in-country inventory from the respective vendors and secondly the need to import inventory from outside the country affected. This will require careful planning to minimise issues with the supply chain, especially where equipment needs to be imported which under normal circumstances can be a lengthy procedure.

This will drive the need to create flexible expedited processes which can be implemented during disasters, plus post disaster rectification processes e.g. equipment brought in under emergency conditions are properly ratified post disaster, for example in the US during disasters the regulator will allow the MNO/Vendor to import restricted equipment under an "experimental license" which gives the MNO/vendor a window to complete the regular import certification processes once the immediate emergency situation has passed. Thereby minimising the RTO of the network.

## 7.2.5 Infrastructure

### Edge (BTS/SC)

Network edge infrastructure in low lying coastal areas affected by tsunami are the most likely to sustain damage and/or to be affected by power and communication outages in the network for example in the Great East Japan Earthquake and resulting Tsunami saw service interruptions across 5000 base stations. This damage can be from water getting into sensitive electronic equipment and damage from the initial impact and related debris. Even where the equipment survives the initial impact operationally, it may be affected by power outages. This may not be immediately obvious as UPS and backup systems kick in but as these run out of independent fuel sources it will become more of an issue if they can't be either re-connected to the grid or fuel supplies be renewed.





### Backhaul/network

Cabling, network links and transmission paths may be affected as follows;

**Fibre –** cuts in fibre in pipelines/underground where the infrastructure is destabilised e.g. a bridge is swept away with the attached pipeline. Above ground fibre cut by the effect of the wave and or debris. Damage to fibre nodes e.g. terminators, switches, etc.

**Wire line links –** as with fibre, plus water ingres to cabling.

**Microwave LOS/NLOS links –** loss of towers with links, alignment issues where transmitters and receivers are knocked out of alignment due to shift in tower or directly to the equipment. Water damage to equipment.

**VSAT –** physical and water damage to equipment. Alignment issues (less prevalent than MW). Increased attenuation from accompanying weather conditions.

Network topology design and redundancy is key to mitigating the effects of transmission path failures i.e. cuts in the network links and should be planned carefully with potential disasters in mind e.g. benefits of using loop or mesh v's point-to-point topologies.

## Core

The network "Core" here is defined as key network equipment (NE) used to handle the various operational and business capabilities of the network usually situated in centralised data centres or network operations centres. This will include key network components such as the VLR, HLR, GGSN, SMSC, etc. along with operational and business support systems. Key monitoring systems of the OSS should also be included here.

Initial network design would look to place these key data centres out of the path of a tsunami i.e. on higher ground, inland. Where this is not possible then flood precautions should be designed into the facility. Another key learning from the Great East Japan Earthquake and Tsunami was that the NE monitoring system became overloaded due to a combination of both localised NE failure alarms and congestion alarms across the whole network being generated. This requires careful management in the generation of alarms and the ability to process them in these large-scale real-time systems.





# 7.2.6 Usage

## Demand

One of the key issues during a disaster is the increased demand on the network as subscribers try to contact family, friends and information services, which far exceed the network's peak-time dimensioning. This more often than not is compounded by damage to the network reducing coverage and/or capacity. The resulting congestion is not just limited to the area where the disaster occurred but also across the region as news spreads and unaffected areas try to contact those in affected areas.

## Subscribers

During and immediately after a disaster there may be a number of issues subscribers face in using the mobile network (besides network coverage and congestion - see sections above). These can include;

- Warning notifications
- Damage or loss of phone
- Adequate power supply for charging phones
- Lack of PAYG credit balance
- Access to PAYG top-up mechanisms (e.g. prepay card availability, ATM access, etc.)
- SIM card registration availability
- Account termination
- Roaming access (tourists, international agency workers, etc.)





# 7.3 Earthquakes

## 7.3.1 Onset

Whilst the technology exists to detect earthquakes (seismographs, etc.), there is little in the way of being able to predict earthquakes with any accuracy. What early warning systems there are may be able to give a few seconds and at best minutes (depending on distance from the epicentre).

For example, preceding the Nepal Earthquake in April 2015, the regional authorities and international agencies were aware there was a high risk of seismic activity in the region within the next 80 years.

Consequently, from the perspective of a mobile network the most effective measures for earthquakes will be in preparation and building in resilience to the vulnerable systems.

This does raise the issue of how far should an MNO go given the increased costs in building resilience versus the potential damage to the business should an earthquake occur.[12]

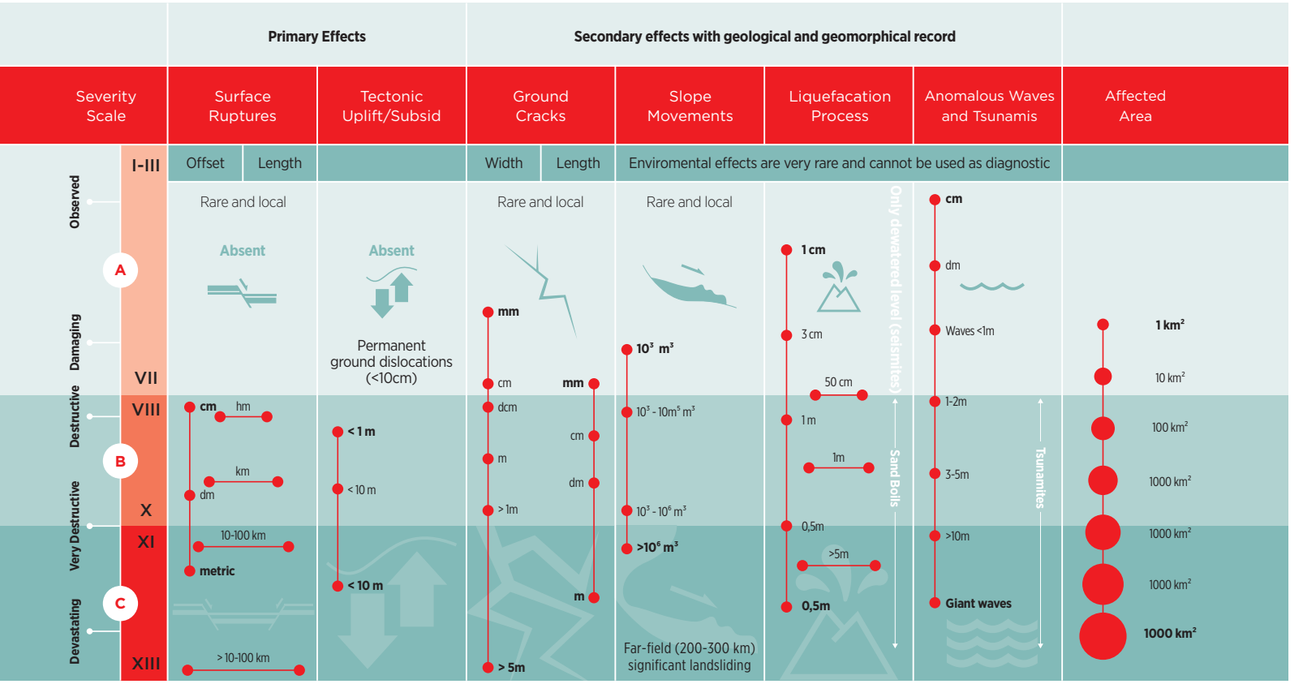
## 7.3.2 Hazard Data

| Category | Data requirements | Data sources |
|---|---|---|
| Earthquake | Historical earthquake characteristics | Government agencies, academic, researchers |
| | Interruption contingencies | Private firms, researchers |
| | Seismic characteristics | Government agencies, academic, researchers |
| | Event shake maps | Government agencies, academic, researchers |
| | Hazard maps | Government agencies, academic, researchers |

12. See “Implementing and maintaining BCM” in “Disaster scenarios for Business Continuity Planning In Mobile Networks” which outlines the need and approaches to building resilience into BCM and BCP.

# 7.3.3 Crisis definitions

The definition of the level of effect of an Earthquake is most often linked to the Richter scale and represented in the ESI 2007[13] or European macroseismic scale (EMS)[14] definitions.




**ESI 2007 Seismic Activity Scale**

In most circumstances the business will need to plan for level VII (5.0 Richter) and above and any plans should be linked to the scale of the disaster e.g. for a level VII event, there may only need to be checks initiated for low level damage assessment at identified vulnerable sites and facilities.

The level of crisis will also be dictated by the level of exposure and vulnerability of particular areas, for example a relatively "small" earthquake in a highly populated area were poor building stock is prevalent will have a much greater effect than a larger earthquake in a remote less populated area. As the network in the former will be reliant on rooftop BTS and subject to greater congestion issues than rural BTS which can be built to more exacting building codes and not reliant on the supporting building infrastructure.

13. https://en.wikipedia.org/wiki/Environmental_Seismic_Intensity_scale

14. https://en.wikipedia.org/wiki/European_macroseismic_scale





# 7.3.4 Operations

## Staff

Earthquakes are potentially very disruptive to staffing, through personal injury, family concerns, destruction of habitation, the availability of food and medical supplies and transport issues due to blocked roads, fuel supply etc.

## Access/transportation

During and immediately after an earthquake incident, routes to key infrastructure in the affected area will most likely be very difficult to get through due to damage (liquefaction, fault tears, etc.) and debris (from falling buildings). Consequently, transportation planning will need to account for the state of roads, tracks, airports, etc. and modes of transport required e.g. all terrain vehicles, helicopters, etc.

In order to secure availability, of these resources may mean working with both private and state resources e.g. the army, both of which will require substantial planning and prioritisation with the third parties especially in the case of using state resources.

Site access may be affected by unstable buildings and/or blocked access. Limited or no security on site may mean that access is denied to staff.

## Supply chain

Supply chains will suffer similar levels of disruption, although by their nature may have worse disruption e.g. fuel supply for generators may be disrupted due to transport links being down, vehicles being out of place, petro-chemical plants being shut down, etc.

To help reduce exposure in the supply chain MNOs can cascade BCPs and make sure that the providers plans meet the needs of their BCP. Reviewing supply chain providers for BCP compliance also has the side benefit of improving the general robustness of the supply chain which can be benefit normal operations as well.

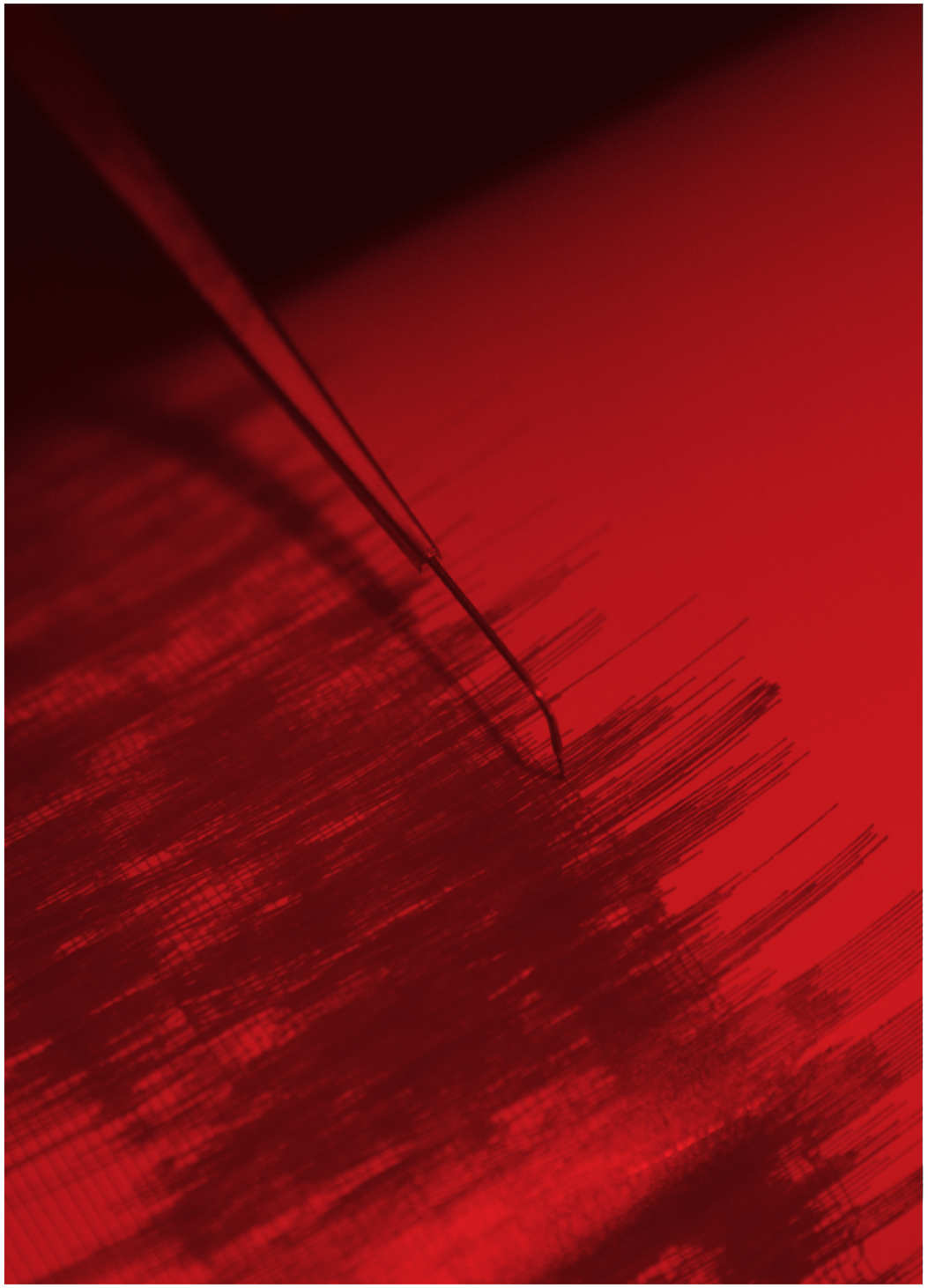
# 7.3.5 Infrastructure

## Edge (BTS/SC)

The level of damage to the infrastructure on the edge of the network will be dependent on factors such as the proximity to the epicentre, towers and housing design, dependant building design for rooftop BTS.

Even where the equipment survives the initial impact operationally, it may be affected by power outages.

This may not be immediately obvious as UPS and backup systems initially kick-in but as these run out of independent fuel sources it will become more of an issue if they can't be either re-connected to the grid or fuel supplies be renewed.



## Backhaul/network

Cabling, network links and transmission paths may be affected as follows;

**Fibre/Cable –** generally underground cabling is less prone to disruption, although in areas where liquefaction accompanies the earthquake they will still be at risk. Above ground cabling is at more risk of support/pole failures and breaks from objects falling on them (e.g. trees) but it is usually quicker to identify breaks and repair them than underground cables.

**Microwave LOS/NLOS links –** loss of towers due to structural failure, loss of alignment through disturbances to the towers may also be an issue.

**VSAT –** physical damage to equipment. Alignment issues (less prevalent than MW). Increased attenuation from accompanying weather conditions.

Network topology design and redundancy is key to mitigating the effects of transmission path failures i.e. cuts in the network links and should be planned carefully with potential disasters in mind e.g. benefits of using loop or mesh v's point-to-point topologies.





## Core

Larger core installations such as NOCs may be vulnerable depending location (distance from the epicentre), building code adherence, bracing and IT infrastructure. Again the implementation of redundant and mirrored sites will also affect the degree of resilience e.g. running parallel sites with some level of over capacity so operations can be switched easily in the case of failure.

# 7.3.6 Usage

## Demand

An earthquake will engender much higher use of the network leading to issues around congestion both during and in the aftermath of the tremors, which will probably be further compounded by disruption to the networks overall capacity (as above). Elements such redundancy, network configuration and user education will help alleviate such issues along with improved RTO.

## Subscribers

In relation to end user equipment impact will be relatively low as most devices are carried on the person or nearby, so other than loss damage is less likely. The key issue for the user's phone will be charging the device in the immediate aftermath when power supply from the grid may be limited and alternative sources oversubscribed and expensive. The other key issue for subscribers will be maintaining credit on their account. For pre-paid subscribers access to recharge mechanisms may be restricted as retailers/agents may not be able to provide the relevant mechanisms (e.g. pre-paid scratch cards). For post-paid customers the ability and mechanisms for settling accounts may be disrupted. Also for non-nationals roaming in the country to make sure they still have access even when the MSC can't confirm with their MNO's HLR due to network disruption, etc.

# 7.4 Volcano

## 7.4.1 Onset

Whilst it is almost impossible to predict a volcanic eruption, there are indicative activity which can give a degree of early warning based on seismic activity. Early warning of an eruption is based on probability and not on certainty and the signs are specific to each volcano.

Although the immediate effects will be fairly localised and the longer term effects e.g. ash plumes, flows, etc. will be more widespread and may be dependant on weather conditions.

Warnings are usually sourced from local governmental bodies tasked with tracking volcano activity e.g. PHIVOLCS (www.phivolcs.dost.gov.ph).

## 7.4.2 Hazard data

| Category | Data requirements | Data sources |
|---|---|---|
| Volcanic Activity | Historical volcanic characteristics | Government agencies, academic, researchers |
| | Interruption contingencies | Private firms, researchers |
| | Seismic characteristics | Government agencies, academic, researchers |
| | Eruption coverage maps | Government agencies, academic, researchers |
| | Hazard maps | Government agencies, academic, researchers |





## 7.4.3 Crisis definitions

Volcanic activity is typically measured on two scales the first being the probability of an eruption happening, this is usually a 4 or 5 point scale ranging from dormant through to probable eruption within 24 hours. Secondly once an eruption occurs the scale of the disaster is measured by the Volcanic explosivity index on a scale of 1 to 8 based on the volume of ejecta, for example the Mount St Helens eruption (1980) was a level 5 (Paroxysmic), with a greater than 10km plume.

### The level of crisis for the network will depend on a number of factors;

**Density of population in the effected area –** most volcanoes tend to be in sparsely populated areas so there is unlikely to be infrastructure, staff, etc. in the effected area. The exception being small island states.

Probably the largest area affected comes from the plume of ash which can drift for a number of kilometres. **Ash can affect mobile networks through;**

- Ash deposits which can clog equipment and affect ventilation systems. It is also very abrasive/corrosive and removal may cause further damage to equipment if not done correctly.
- There is also evidence that the electrically charged ash in the plume will disrupt local radio signals which may affect the OTA interfaces for the network as well as any microwave or satellite backhaul.

## 7.4.4 Operations

### Staff

The effects on staffing from a volcanic eruption will be dependant on the scale of the disaster and the proximity of staff to volcano and its fallout during both work and leisure times. What specific actions should be considered?

Setup early warning feeds for staff for eruption probability and eruption in progress, this could be refined to those in affected areas by staff location.

Plan damage assessment roster with specific ash, and related volcanic flow damage assessment plans.

Pre-emptive ash protection plans and clearing guidelines plans.

### Access/transportation

Localised transport may be disrupted in the area of the eruption, including air travel due to issues with ash. More remote BTS equipment especially on high ground may be difficult access.





### Supply Chain

Minimal impact on most supply chains other than those which need access to equipment in the affected area.

## 7.4.5 Infrastructure

### Edge (BTS/SC)

BTS situated near to the volcano or on high ground in the vicinity, along with those in the potential path of any fallout from an eruption, may be affected and the following considerations made;

Protective measures plan for vulnerable sites.

- Heat and projectile protection
- Ash protection plans – sealing sites, ash removal procedures and equipment.

Post eruption damage assessment and rectification plans.

- Facility cleaning, filters, antenna, dishes, etc.
- Backup power systems cleaning e.g. solar panels, DSG filters, etc.

## Backhaul/network

The main effects will depend on the type of eruption and network cabling/equipment being in the path of the eruption. In the majority of cases the effects will be marginal as most equipment/cabling will have been situated away from unstable volcanic environments. Things to consider and plan for are;

Cleaning OTA transmission equipment of ash, e.g. satellite dishes, microwave transmitters and receivers, etc.

Fibre cut repairs and re-routing (where debris, flows, etc. have made the original route unsustainable)

## Core

The effect on core network infrastructure should be marginal as most of the supporting data centre's would be situated well away from "at risk" areas surrounding volcanos. In the case off ash fallout considerations shown above for other telecom equipment should also apply here i.e. filter cleaning, etc.

If core network systems need to be placed within a vulnerable area (e.g. small volcanic island state), then running a redundant setup with a backup facility in a different area would limit the chances of both facilities being affected.





# 7.4.6 Usage

## Demand

As previously mentioned most volcanic activity is in sparsely populated areas and consequently demand for use in the affected area will be higher than normal, probably within the system dimensions' subject to equipment failure.

However, like any large "event" the network will be subject to congestion as usage spikes and plans should be in place to handle the congestion on the network as best as possible.

## Subscribers

Other than in a colossal eruption the majority of subscribers would not be affected by most eruptions, other than network congestion issues in the immediate aftermath of the event. Also as indicated above the majority of the systems in place for the day to day operations supporting subscribers would not be affected. So other than in a very large scale eruption, there are minimal specific needs for subscriber plans over and above normal operation will provide.

# 7.5 Hurricane/Typhoon

## 7.5.1 Onset

As hurricanes form out at sea over large bodies of warm water and typically take days to reach dangerous levels, they can be observed (satellite images), assessed and tracked prior to them moving into populated areas. This gives the possibility of warning often days in advance, although the strength and path of the hurricane may vary.

Hurricane typically form during specific seasons (typically July to November), which also means that pre-season activities can be planned e.g. asset assessment, public campaigns, etc.

Compared to most other natural disasters this gives the potential for more accurate early warnings both for the MNO in order to undertake preparatory work and to give warning to the population likely to be affected by the hurricane.

## 7.5.2 Hazard data

| Category | Data requirements | Data sources |
|---|---|---|
| Hurricane/ Typhoon/ Tropical Cyclone | Historical cyclone tracks and characteristics | Government meteorology bureau, Regional Specialized Meteorological Centers, Tropical Cyclone Warning Centres |
| | Wind hazard maps | Government emergency response dept, Government and specialist companies on building and facility codes |





# Below are some of the agencies providing hurricane/typhoon/ cyclone information;

| Agency | Link | Region |
|---|---|---|
| Japan Meteorology Agency | http://www.jma.go.jp/en/typh/ | Western North Pacific Ocean and South China Sea |
| NOAA (US) | http:// www.noaa.gov | Atlantic Ocean |
| PDC | http://www.pdc.org/weather/index.php/tag/joint-typhoon-warning center/ | Pacific & Indian Oceans |
| India Meteorological dept. | http://www.imd.gov.in | Bay of Bengal and the Arabian Sea |
| La Réunion-Tropical Cyclone Centre (Météo-France) | http://www.meteofrance.re/cyclone/activite-cyclonique-en-cours | South-West Indian Ocean |
| Fiji Meteorological Service | http://www.met.gov.fj/current_warnings.php | South-West Pacific Ocean |
| Localised metrological agencies | | |
| Indonesian Meteorological and Geophysical Agency | http://www.bmkg.go.id/BMKG_Pusat/Default.bmkg | Indonesia |
| Australian Bureau of Meteorology | http://www.bom.gov.au/cyclone/index.shtml | South-East Indian Ocean |

## 7.5.3 Crisis definitions

**Saffir-Simpson Hurricane Wind Scale** [15]

| Category | Sustained Winds | Types of Damage Due to Hurricane Winds |
|---|---|---|
| 1 | 74-95 mph<br>64-82 kt<br>119-153 km/h | **Very dangerous winds will produce some damage:** Well-constructed frame homes could have damage to roof, shingles, vinyl siding and gutters. Large branches of trees will snap and shallowly rooted trees may be toppled. Extensive damage to power lines and poles likely will result in power outages that could last a few to several days. |
| 2 | 96-110 mph<br>83-95 kt<br>154-177 km/h | **Extremely dangerous winds will cause extensive damage:** Well-constructed frame homes could sustain major roof and siding damage. Many shallowly rooted trees will be snapped or uprooted and block numerous roads. Near-total power loss is expected with outages that could last from several days to weeks. |
| 3 major | 111-129 mph<br>96-112 kt<br>178-208 km/h | **Devastating damage will occur:** Well-built framed homes may incur major damage or removal of roof decking and gable ends. Many trees will be snapped or uprooted, blocking numerous roads. Electricity and water will be unavailable for several days to weeks after the storm passes. |
| 4 major | 130-156 mph<br>113-136 kt<br>209-251 km/h | **Catastrophic damage will occur:** Well-built framed homes can sustain severe damage with loss of most of the roof structure and/or some exterior walls. Most trees will be snapped or uprooted and power poles downed. Fallen trees and power poles will isolate residential areas. Power outages will last weeks to possibly months. Most of the area will be uninhabitable for weeks or months. |
| 5 major | 157 mph or higher<br>137 kt or higher<br>252 km/h or higher | **Catastrophic damage will occur:** A high percentage of framed homes will be destroyed, with total roof failure and wall collapse. Fallen trees and power poles will isolate residential areas. Power outages will last for weeks to possibly months. Most of the area will be uninhabitable for weeks or months |

15. Taken from National Oceanic and Atmospheric Administration (US) http://www.nhc.noaa.gov/aboutsshws.php





# The level of crisis for the network will depend on a number of factors;

**Density of population in the effected area –** whilst tracking information may give the MNO an indication of the area which will be affected, it is not completely predictable and so there can be a variance according to area the hurricane finally makes landfall.

**Wind can affect mobile networks through;**
Damage and destruction of above ground infrastructure and properties from wind, rain and debris. For example, BTS and cell towers are vulnerable along with roofs of properties, where the combination of roof damage and heavy rain can affect susceptible equipment.

There may also be some disruption to satellite micro-wave communications due to high levels of attenuation (rain fade) caused by the storm.

## 7.5.4 Operations

### Staff

The effects on staffing from a hurricane will be dependant on the scale of the disaster and the proximity of staff to the affected area. Hurricanes can affect large areas, so transport and staffing will be a key consideration in planning. What specific actions should be considered?

Setup early warning feeds for staff for hurricane probability and tracking.

Plan staffing for pre-emptive infrastructure bracing and protection work.

Re-enforce transportation and field engineering plans for a large area of possible disruption.

Staff training health and safety assessment, for example, engineers called out to a defective roof top BTS, should be able to effectively assess whether the underlying building is safe to enter e.g. looking for signs of structural damage, etc.

### Access/transportation

Access to infrastructure may be impeded by debris around and damage to the relevant facility. Some consideration should be given to resource availability to help clear access to the site.

Transportation links by road, water and air will be affected during the hurricane and in the case of water and land links may persist for a while after the passing of the hurricane e.g. fallen trees, storm surge, etc. Transportation plans should take into account conditions under which the various transportation options will be effective, plus how working in conjunction with emergency services can help effective access to infrastructure for the repair teams.





### Supply Chain

Supply chains in and out of the area affected by the hurricane both during and in the aftermath of the hurricane. One key consideration (depending on the nature of the supply chain), is to have a more distributed approach to the supply chain, ensuring that the needed supplies are closer to the affected sites e.g. fuel dumps and equipment spares.

## 7.5.5 Infrastructure

### Edge (BTS/SC)

BTS situated in the path of the hurricane especially those in exposed areas e.g. hill tops, may be affected and the following considerations made;

**Protective measures plan for vulnerable sites.**

- Pre-emptive shutdown and bracing of vulnerable sites (see 5.B).
- Use of backup power not easily damaged by wind and debris e.g. batteries, diesel generators, fuel cells. Renewable sources such as wind turbines, solar arrays are susceptible to damage during hurricanes.

**Post hurricane damage assessment and rectification plans.**

- Facility access and debris removal.
- Re-establishing a site which has been pre-emptive shutdown to bring it back on-line.
- Backup power systems re-supply.

## Backhaul/network

Cabling, network links and transmission paths may be affected as follows;

**Fibre/Cable –** generally underground cabling is less prone to disruption, although in areas where flooding accompanies the hurricane (e.g. from precipitation, storm surge) they will still be at risk. Above ground cabling is at more risk of support/pole failures and breaks from debris and objects falling on them (e.g. trees) and breaks from tension caused by extreme wind speeds.

**Microwave LOS/NLOS links –** loss of towers due to structural failure, loss of alignment through disturbances or vibration to the towers may also be an issue.

**VSAT –** physical damage to equipment from wind or debris. Alignment issues from the force of the wind. Increased attenuation/rain fade from accompanying precipitation.

Network topology design and redundancy is key to mitigating the effects of transmission path failures i.e. cuts in the network links and should be planned carefully with potential disasters in mind e.g. benefits of using loop or mesh v's point-to-point topologies.

## Core

Larger core installations such as NOCs and ICT Data Centres are less likely to be vulnerable if siting and good building code adherence has been applied. Again the implementation of redundant and mirrored sites will also affect the degree of resilience e.g. running parallel sites with some level of over capacity so operations can be switched easily in the case of failure or the need for load balancing.





# 7.5.6 Usage

## Demand

A hurricane will engender much higher use of the network leading to issues around congestion both during and in the aftermath of the hurricane, which will probably be further compounded by disruption to the networks overall capacity (as above). Elements such redundancy, network configuration and user education will help alleviate such issues along with improved RTO.

## Subscribers

In relation to end user equipment impact could be relatively high to water ingress to the device from exposure to the weather conditions. Another issue for the user's phone will be charging the device in the immediate aftermath when power supply from the grid may be disrupted by fallen power lines, etc. and alternative sources hard to find and oversubscribed.

Access to credit for their account should not be a major issue as long as the renewal and top-up methods are still widely available shortly after the hurricane has passed. Where the severity of the storm has required external intervention by international relief agencies, then help with roaming for non-national workers in the country will need to be considered.

# 7.6 Flooding

## 7.6.1 Onset

Flooding does not typically happen in isolation but is linked to another disaster conditions e.g. precipitation from storms, storm surge, tsunami, dam failure, high tides, etc. Some of these disasters are predictable in their own right and alongside known measures e.g. rainfall levels from weather stations, rising river levels, this can give a degree warning of a flood event. This tied with a knowledge of equipment geographical positioning and vulnerability should in most cases give a degree of forewarning for MNOs. The use of water ingress sensors at key facilities may also help give advance warning to the MNOs monitoring facilities

## 7.6.2 Hazard data

| Category | Data requirements | Data sources |
|---|---|---|
| Flooding | Mapping of levees / retention basins | Local governments, private firms, researchers |
| | Hazard flood maps | Local governments, Geoscience Institues, state governments, Insurers |





## 7.6.3 Crisis definitions

The definition of the level of effect of a Flood is typically described in flood "stages". In the USA the National weather service define the following stages;

**Action Stage –** level at which mitigation actions should be activated e.g. when rivers at the top of their banks, coastal having elevated tides exceeding normal high tides levels.

**Flood Stage –** an established height for a given location above which a rise in water surface level begins to create a hazard to lives, property, or commerce. The issuance of flood advisories or warnings is linked to flood stage.

- Minor Flood - is defined to have minimal or no property damage, but possibly some public threat.
- Moderate Flood - is defined to have some inundation of structures and roads near the stream/coast. Some evacuations of people and/or transfer of property to higher elevations may be necessary.
- Major Flood - is defined to have extensive inundation of structures and roads. Significant evacuations of people and/or transfer of property to higher elevations are necessary.

In most circumstances the business will need to plan for Minor flooding and above and any plans should be linked to location specific information, there may only need to be checks initiated for low level damage assessment at identified vulnerable sites and facilities.

# 7.6.4 Operations

## Staff

The effects on staffing from flooding will be dependant on the scale of the disaster and the proximity of staff to areas prone to flooding during both work and personal times.

Setup early warning feeds for staff where available (e.g. Local weather Apps)

Plan damage assessment roster with specific water/flood damage assessment plans

Water damage rectification

Re-route/site water sensitive equipment

## Access/transportation

During and immediately after a flood incident, routes to key infrastructure in the affected area will most likely be very difficult to get through due to flooding and debris. Consequently transportation planning will need to account for modes of transport required e.g. all terrain vehicles, boats, helicopters, etc.

In order to secure transport availability of these resources, it may mean working with both private and state resources or bringing in the vehicles from outside of the affected area.





## Supply chain

During flooding supply chains may need to make use of alternative transportation, it should be checked that partners have taken this into account in their BCP.

Careful thought should be given to the siting of equipment and their potential for portability should it be required. For example, after the 9-11 disaster in New York, it was mandated that rooftop backup power generation facilities and their fuel supplies should be moved to the basements of the respective buildings. However with flooding which accompanied hurricane Sandy, this meant many of the power backups for these cells were compromised. This is where BCP assessment should take into account all the relevant scenarios as a whole and not just in separation.

# 7.6.5 Infrastructure

## Edge (BTS/SC)

Network edge infrastructure in low lying coastal and river areas affected by flooding are the most likely to sustain damage and/or to be affected by power and communication outages in the network. This damage can be from water getting into sensitive electronic equipment and damage from inundation e.g. silt, mud, etc. Use of COWs should be considered to help maintain coverage and located as close as is reasonable (subject to access and topography) to the affected cell site.

Recovery of affected sites will need to wait until the flood waters have receded and the facilities have been made safe, especially concerning power supplies and possible contamination from the flood waters and leakage e.g. diesel from fuel tanks.

## Backhaul/network

Cabling, network links and transmission paths may be affected as follows;

**Fibre –** cuts in fibre in pipelines/underground where the infrastructure is destabilised e.g. a bridge is swept away with the attached pipeline. Damage to fibre nodes e.g. terminators, switches, etc.

**Wire line links –** as with fibre, plus water ingres to cabling. In areas especially vulnerable to flooding routing cabling above ground may be preferable but will need to take into consideration other prevailing disasters and the primary factor for the flooding e.g. storms.

**VSAT –** physical and water damage to equipment. Alignment issues (less prevalent than MW). Increased attenuation from accompanying weather conditions

Network topology design and redundancy is key to mitigating the effects of transmission path failures i.e. cuts in the network links and should be planned carefully with potential disasters in mind e.g. benefits of using loop or mesh v's point-to-point topologies.





# 7.6.6 Usage

## Demand

One of the key issues during a disaster is the increased demand on the network as subscribers try to contact family, friends and information services, which may far exceed the network's peak-time dimensioning. This more often than not is compounded by damage to the network reducing coverage and/or capacity.

The resulting congestion is not just limited to the area where the disaster occurred but also across the region as news spreads and unaffected areas try to contact those in affected areas.

## Subscribers

During and immediately after a disaster there may be a number of issues subscribers face in using the mobile network (besides network coverage and congestion - see sections above). These can include;

- Warning notifications
- Water damage or loss of phone
- Adequate power supply for charging phones
- Lack of PAYG credit balance
- Access to PAYG top-up mechanisms (e.g. prepay card availability, ATM access, etc.)
- SIM card registration availability
- Account termination
- Roaming access (tourists, international agency workers, etc.)





# 7.7 Disease

## 7.7.1 Onset

Here we will consider the onset of an epidemic contagious disease which is not endemic to a country or region (endemic diseases should be considered under standard operational practices). In the case of infectious and contagious diseases, the nature of the onset will differ according to the nature of the disease and the method and speed of transmission. Whilst it is unlikely there will be any pre-warning of the initial cases of a disease, there will be various warning levels as the epidemic grows. The warnings will be released by recognised agencies such as government health bureaus and the WHO.

MNOs may be requested to provide alerts to their users about the spread of disease and preventative measures. Ideally these alerts should be created and distributed through agreed processes and channels between the relevant health agencies and the MNO. It is important that any messaging is co-ordinated and assessed by the appropriate agencies so the messages are timely, accurate and avoid panicking subscribers.

## 7.7.2 Hazard data

| Category | Data requirements | Data sources |
|---|---|---|
| Disease/ Epidemic | Health information and alerts | Government health bureaus, WHO,specialist NGO |
| | Epidemic coverage and quarantine maps | National and Local governments, NGOs |
| | Mobile coverage maps | MNO, Government regulator |
| | Employee health coverage | National health service, insurance providers |

## 7.7.3 Crisis definitions

The definition for diseases will depend a lot about the disease and the method(s) of transmission, including the degree of virulence. For example, the WHO outlined a 6 phase definition for the pandemic of the H1N1 flu virus;

1 **Phase 1 -** no viruses circulating among animals have been reported to cause infections in humans.

2 **Phase 2 -** an animal influenza virus circulating among domesticated or wild animals is known to have caused infection in humans.

3 **Phase 3 -** an animal or human-animal influenza virus has caused sporadic cases of disease in people, but has resulted only in limited human-to-human spread.

4 **Phase 4 -** is characterized by verified human-to-human transmission of an animal or human-animal influenza virus able to cause "community-level outbreaks." The ability to cause sustained disease outbreaks in a community marks a significant upwards shift in the risk for a pandemic.

5 **Phase 5 -** is characterized by human-to-human spread of the virus into at least two countries in a region.

6 **Phase 6 -** the pandemic phase, is characterized by community level outbreaks in at least one other country in a different region in addition to the criteria defined in Phase 5. Designation of this phase will indicate that a global pandemic is under way.

At which point various BCPs are triggered will be determined by requests from official bodies and the need to initiate provisioning and protection MNO staff and facilities. As stages and the progress of the disease will very widely the trigger points will need to be decided on a more dynamic basis by the CMT.





## 7.7.4 Operations

### Staff

The affect on staff may be considerable, especially for those in affected areas some actions which should be considered as part of a BCP;

Staff roster of affected people and families.

Home working capabilities

Staff evacuation plans

Decentralisation of key engineering staff

Increased health coverage for staff e.g. medical evac

Prescribed health facilities (e.g. hand sanitisers) and training

Remote payments/banking e.g. over mobile money

Support from specialist NGOs and health partners on risks and reduction practices.

## Access/transportation

Whilst an epidemic in its own right will not create access problems, the measures put in place by authorities may have an affect on access, especially where quarantine measures are taken. Some actions to be considered;

Decentralisation of key staff needed for site maintenance

Work with key health and NGO services to help support them and gain access to the affected areas

Vehicle and personnel protection and processes e.g. hazmat suits, cleansing processes and materials

Research possibilities around the use of unmanned maintenance and inspection technologies (e.g. drones)

## Supply Chain

As with MNO staff, vendors in the supply chain will face the similar challenges, so its important that vendor and supplier BCPs are harmonised with the MNOs. Some actions to be considered;

Decentralisation of supply depots and key supplier staff and transportation.

BCP alignment.





# 7.7.5 Infrastructure

## Edge

Disease will have little or no effect on existing infrastructure, other than access for maintenance and fuel supply restoration.

The key issue MNOs may find will be where the epidemic affects remote areas where there isn't current coverage by their network. In these cases they may come under pressure to provide both temporary cover and a long term coverage solution. The issue for a long term coverage solution is an economic one for example in order for an MNO to put the needed infrastructure in place (BTS, towers, backhaul, power, etc.) means for the population density covered and likely ARPU, they will be looking at a 20 – 30 year ROI. Some actions to consider;

Provision of COW coverage capability

VSAT support for remote COWs

Reduced cost options for increased remote coverage e.g. tower sharing, economic incentives, government support, grants, etc.

## Backhaul/network

No major affects anticipated over above maintenance access (as above) and remote area coverage demands.

For this the MNO may need to consider VSAT capacity plans for temporary coverage increases.

## Core

No major affects over and above any staffing affects and maintenance issues. For BCP purposes the MNO may want to consider improving remote monitoring and configuration capabilities for the network, which will help reduce the need for onsite maintenance.

Along with geo-redundancy of NOCs and Data Centres so that if one is in an affected area the network load and management can be handled from a centre out of the affected area.





# 7.7.6 Usage

## Demand

Demand on the network will not be at the same levels as a natural disaster which peaks at a specific point but rather there may be some increase in traffic during peak activity times e.g. when there are media news on the epidemic, etc. Also any traffic increase will tend to be more localised to cells where there are hotspots for the epidemic and/or new medical facilities put in place.

Probably the main demand will be for coverage in rural areas where the epidemic might be prevalent and secondly for increased capacity to help temporary medical and related services. Some considerations for BCP in these circumstances are;

Use of COWs to provide temporary coverage and/or capacity

Use of “Instant Networks” for rural coverage in specific areas e.g. medical facilities

Network sharing passive (towers) and active (RNC, etc.)

Targeted government support e.g. subsidies, USF grants, etc. for rural coverage to help reduce the ROI lead time.

GSMA is currently running a “Connected Society Programme” exploring various aspects of internet access over mobile and increasing adoption including options for rural coverage.[16] A recently published a report “Rural coverage: strategies for sustainability - Country case studies”[17] with GSMAi may be of interest.

16. http://www.gsma.com/mobilefordevelopment/programmes/connected-society/

17. http://www.gsma.com/mobilefordevelopment/programme/connected-society/rural-coverage-strategies-for-sustainability/

## Subscribers

The majority of subscribers would not be affected by the direct effects of most epidemics. Also as indicated above the majority of the systems in place for the day to day operations supporting subscribers would not be affected.

Subscriber needs will be more around being able to easily refresh credit, access financial services, along with health informational and diagnosis services. A key example during the recent Ebola epidemic in West Africa of mobile money uses covered:

Payment for the large numbers of Health workers / burial teams employed in response activities.

Helping to reduce impact from the closure of banks and other MFS.

Easier method of payment in times of reduced mobility and helping with the continuation of ‘normal’ business needs.

For health informational services consideration should be given to;

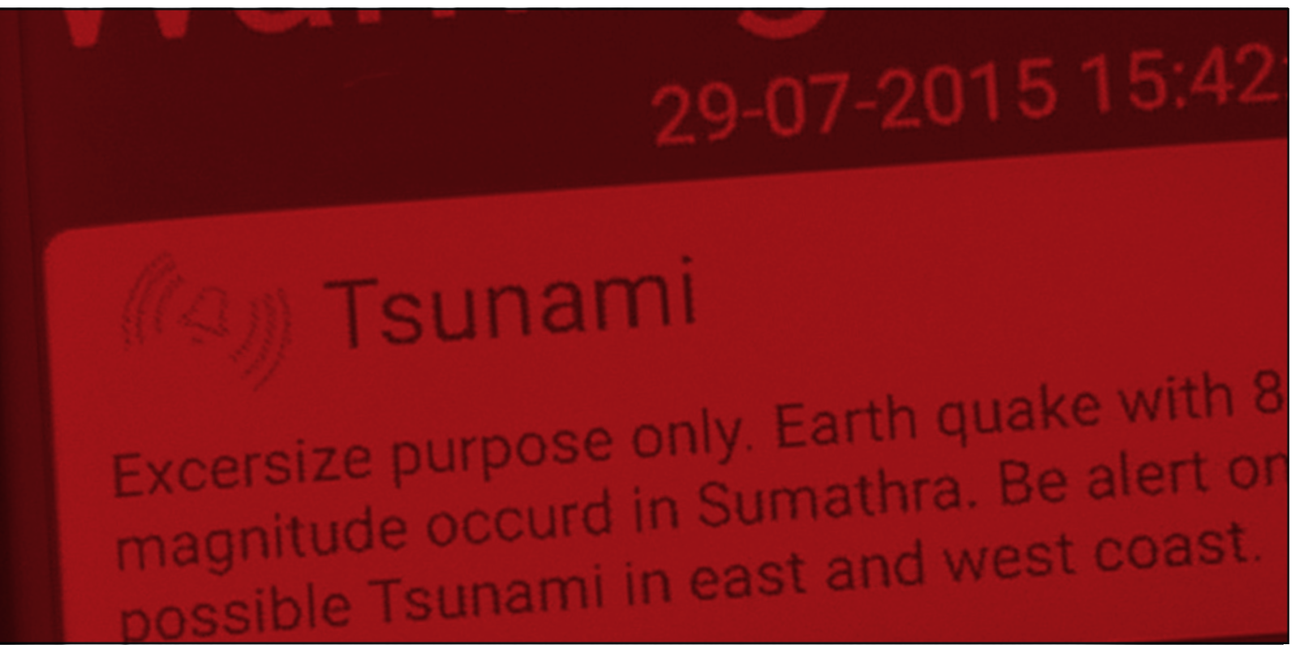
The use of common (cross MNO) resources such as short codes, ideally these need to be agreed prior to any outbreak.

Access to accredited health information and the relevant expertise in content creation and adaptation for mobile channels.

Approval processes for health content and services with Government health bureau, should be pre-defined and responsive within clear timeframes.








Ultimately BCP and DRR practices are looking to make mobile networks as resilient as possible to the effects of disasters to both minimise loss to the business and maximise support for agencies and the general populace during such events. In order to do that we need to consider what characteristics we are looking to develop as part of the BCP and DRR work.
The following are a few characteristics which may be helpful in planning, derived from a few sources [18]

18. See "The Resilience Dividend" by Judith Rodin and "City Resilience Framework" by the The Rockefeller Foundation and Arup





## 8.1 Assessment

As described above a key part of planning is assessing not just the risks presented to the business and populace by particular disaster scenarios but also an awareness of the capacity the business has to combat it. Assessing and being aware of the business's strengths and assets as well as vulnerabilities and liabilities will be key to creating effective plans to respond to disaster scenarios.

This also needs to be a continuous incremental process especially as the business develops, for example as networks move from 3G to LTE, in theory the pure IP nature of LTE should provide a greater degree of network robustness in the face of disruption, which should be accounted for in BCP as LTE is rolled out and the possibilities raised by a "Flexible Management Entity" (see "Enabling Disaster Resilient 4G Mobile Communication Networks" white paper[19]).

Also a COW (Cell on Wheels) could be seen as an asset, whereas a roof top BTS on building not up to the relevant building code for a scenario could be seen as a vulnerability.

## 8.2 Capacity & robustness

Key to resilience is not just having sufficient capacity for day-to-day needs but having sufficient capacity to be able to offer diverse solutions for rectification when a disaster strikes. For example, power for a BTS under normal operations would constitute a grid supply and sufficient local generation (e.g. diesel generator) to cover the level grid outages normally expected. However in disaster situations there is a potential for much longer outages/disruption, so capacity should look to cover longer periods and possibly alternative power supplies (e.g. solar power, fuel cells, etc.). Increasing redundancy will help create a higher level of robustness as will the ability to have flexibility around resources within the organisation so they can be re-purposed to cover changing needs and situations.

The intent here is to plan into the business and its elements a greater degree of robustness to the likely disaster scenarios facing the organisation.

Whilst increasing the resilience of a mobile network has a cost in terms of both capital expenditure and operational expenses, this should be weighed against the potential future cost to the business when a disaster strikes in terms of RTO, revenue loss, asset loss, reputational damage and regulatory compliance as well as the potential for lowering fiscal volatility for the MNO. The insurance industry is increasingly using Cat (catastrophe) modelling in order to insure against such events, this takes account exposure, hazard, vulnerability and financial data, this may be something which MNOs can work on in conjunction with their insurers to help understand the cost effectiveness of resilience work.

19. "Enabling Disaster Resilient 4G Mobile Communication Networks" by Karina Gomez, Leonardo Goratti, Tinku Rasheed and Laurent Reynaud.

## 8.3 Co-ordination

Support for co-ordination both within the MNO departments and externally to agencies through various channels human and machine-to-machine (e.g. API to provide coverage queries), will greatly increase the ability to help both the re-establishment of the network and business as well as supporting humanitarian efforts.

This is a key principle in the GSMA Humanitarian Connectivity Charter.[20]

For example, keeping the humanitarian agencies informed of network coverage and outages will help them direct efforts and make use of emergency telecom systems where its needed, inversely this may also help co-ordinate access to supply chains for needed transport, etc. for the MNO.

## 8.4 Regulation

The business needs to be able to regulate itself so it can deal with anomalous and irregular situations without creating a long term catastrophic fail for the business or avoid a cascade of failures to becoming systemic. The creation and implementation of a BCP will help to regulate the business when disasters strike. There also needs to be balance of external regulation (from government), which whilst supporting normal activities to an agreed standard, should also have the flexibility to allow for disaster situations. For example, a simplified and expedient importation of telecoms equipment process. Plus, incentives to help reduce the cost:benefit ratio for the MNOs to help them build resilience for the network.

GSMA has published an emergency mobile telecommunications regulatory best practice guideline.[21]

20. http://www.gsma.com/mobilefordevelopment/programmes/disaster-response/humanitarian-connectivity-charter

21. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/GSMA-Industry-Position_Emergency-Telecoms-Regulation.pdf





## 8.5 Agility

The need for agility and flexibility is key, by their very nature disasters can strike with little or no warning and rarely in the same way as before, plus during the response phase circumstances are frequently changing, indeed the speed of change can in itself generate ambiguity and what seems to be non-predictable behaviours. Consequently, flexibility in planning and action is essential, no one plan will be able to provide a complete solution to every eventuality. To paraphrase John Boyd[22], "those who can handle the quick rate of change have a better chance of surviving".

In order to create that flexibility, plans and processes need to be able to allow for innovation and initiative which can lead to adaptability in the face of an ever changing situation. For example, after the earthquake in Haiti both the housing and BTS equipment had been damaged, fixing and/or replacing the relevant telecoms equipment without appropriate shelter/housing meant an increased risk of damage from the environment, one solution Digicel staff came up with was to re-purpose shipping containers (used for bringing in AID) for housing BTS equipment by the installation of power and fans (for cooling).

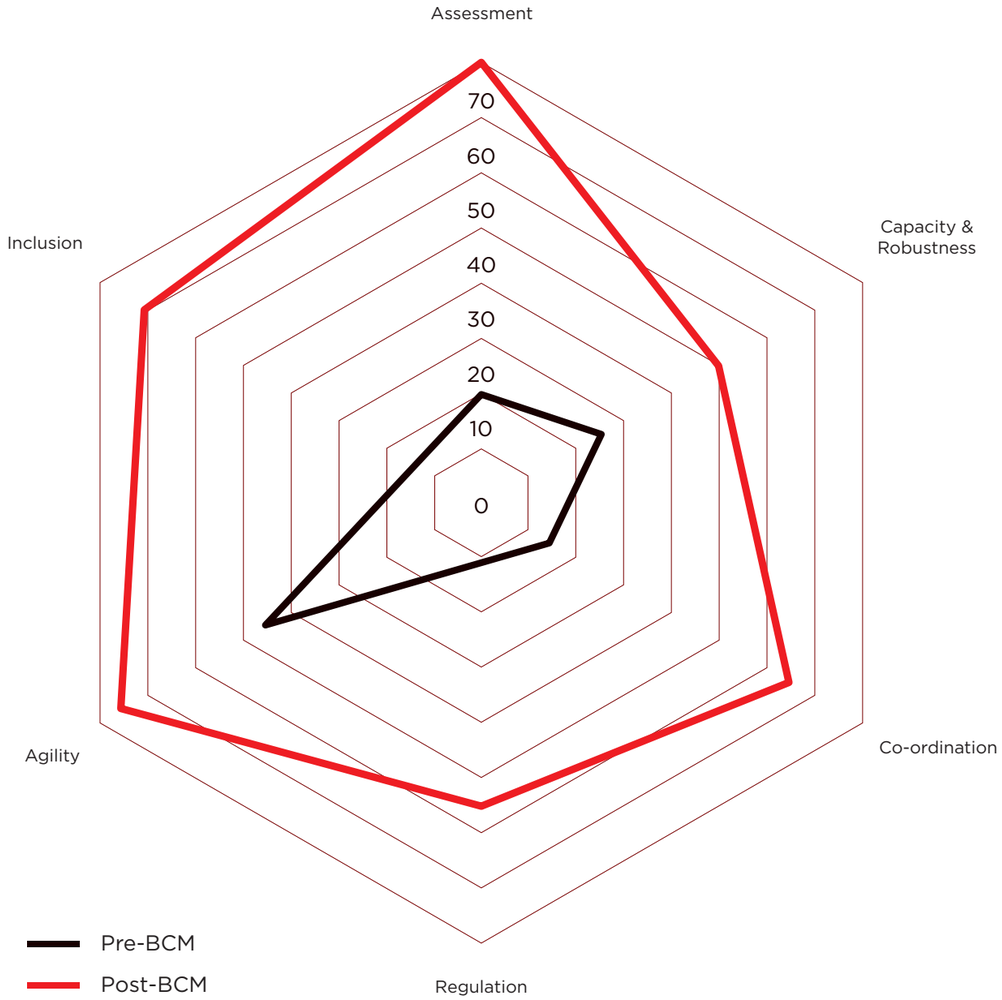
## 8.6 Inclusion

In order to create effective and adaptable plans, the planning process needs to be inclusive of all the stakeholders (subscribers, emergency services, regulators, NGOs, etc.) and those on which the MNO depends (vendors, suppliers, etc.).

As well as making sure that any BCP is more nuanced to the various needs and restrictions of the stakeholders, the act of consultation will help engender shared ownership in respect of response and trust between the parties. This also forms the basis of cross department and organisation communication. Often systems and processes focus on the more mechanical nature of network restoration, the human processes are equally important, in getting operations bring the business quickly back to a sustainable level of service. For example, working across MNOs, vendors, hauliers and customs authorities to arrange for stream-lined equipment importing during a disaster.

22. From John Boyd's "New Conception for Air-to-Air Combat" (c1976)

Taking the above qualities and applying them to Business Continuity Planning and Management should make the overall resilience of the business as shown in the spider diagram below, more encompassing with fewer vulnerabilities for the business.




**Resilience Spider Diagram**





# 9

# Areas of focus for an MNO

# 9.1 Areas of focus for an MNO

At the end of 2015 the United Nations Development Programme (UNDP) launched the Sustainable Development Goals (SDG) as a follow on to the Millennium Development Goals (MDG). Of these SDGs the most relevant to this subject is SDG Goal 9: "Build resilient infrastructure, promote sustainable industrialization and foster innovation" This has a number of targets assigned to it of which the two below are of interest;

- Develop quality, reliable, sustainable and resilient infrastructure, including regional and trans-border infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all
- Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020

## Priority

Also in the recently agreed Sendai Framework for Disaster Risk Reduction the four priorities they identified for action were;

1. Understanding disaster risk.
2. Strengthening disaster risk governance to manage disaster risk.
3. Investing in disaster risk reduction for resilience.
4. Enhancing disaster preparedness for effective response and to "Build Back Better" in recovery, rehabilitation and reconstruction.





A key aspect of these priorities is understanding risk in the context DRR and how its defined, one definition is;

"**Risk** can be defined as 'the potential for consequences where something of value is at stake and where the outcome is uncertain, recognizing the diversity of values. Risk is often represented as probability of occurrence of hazardous events or trends multiplied by the impacts if these events or trends occur' and is constituted of **exposure** ('presence of people, livelihoods, species or ecosystems, environmental functions, services, and resources, infrastructure, or economic, social, or cultural assets in places and settings that could be adversely affected'), **vulnerability** ('propensity or predisposition to be adversely affected... including sensitivity or susceptibility to harm and lack of capacity to cope and adapt') of people, and infrastructure, this combined with the potential of a **hazard** (a physical event that may cause 'loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems, and environmental resources' ) occurrence."[23]

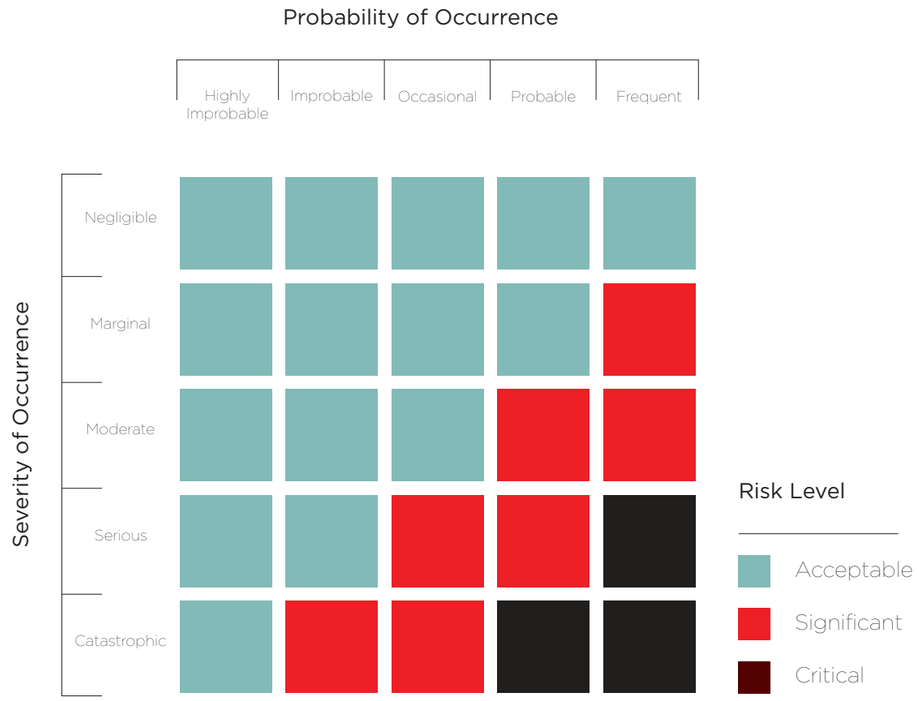
This is often represented by the simplified formula below which represents the collective risk of a scenario;

Risk = Hazard x Exposure/Vulnerability

These types of calculation can help the business determine the level of risk to their business (including staff and subscribers), in order to help figure out what they should respond to.

23. IPCC 2014 Summary for policymakers. in: Climate Change 2014: Impacts, adaptation, and vulnerability. Part A: Global and sectoral aspects. Contribution of working group II to the fifth assessment report of the Intergovernmental Panel on Climate Change (ed. Field, C B, Barros V R, Dokken D J, Mach K J, Mastrandrea M D, Bilir, T E, Chatterjee, M, Ebi, K L, estrada, Y O, Genova, R C, Girma, B, Kissel, E S, Levy, A N, MacCracken, S, Mastrandrea, P R & White l). Cambridge and New York: Cambridge University Press.


**The natural disaster risk triangle and reduction**




**Risk assessment table**

The simplified table above shows the risk level assessment needs to weigh the severity against the probability of the event occurring. This will give some indication of where to focus BCP efforts. For example, a major meteor strike would be catastrophic but it is also highly improbable, whereas if the country in question is on a major and active fault line where the occurrence of earthquakes are frequent and of a potential 1 in a 100 catastrophic severity, it would be more effective to focus BCP resources on resilience efforts for earthquakes rather than a meteor strike.

# 9.2 Understanding the risks

## 9.2.1 Understanding the risks for the business

### Revenue loss

Revenue loss can be caused in a number of ways for the MNO depending on their portfolio of revenue streams

- Loss of post paid revenue as financial mechanisms for collection may be affected.
- PAYG services can be affected by affects on top up mechanisms of the disaster e.g. scratch card vendors either unable to verify cards on the system, loss of cards, resupply of cards, vendor facility and equipment damage, etc.
- Call completion rates dropping due to congestion, network availability, etc.
- VAS availability either due to prioritisation of essential services or by capability damage of the service providers to provide the service. With the loss of resultant subscriptions and revenue shares.
- Advertising and promotional revenues loss either due to lack of "carrier" service availability or suspension due to prioritisation of essential services.
- Loss of roaming revenues either through the inability to access or process cross charging/ mediation with MNO partners/hubs. Also by deliberate policies to suspend roaming charges for visitors caught up in the disaster and incoming relief workers using home network SIMs.
- Disaster credit allowances for humanitarian purposes e.g. giving users a credit allowance for calls and messaging during the crisis, suspension of account terminations due to non-payment, etc. For example, during the earthquake in Nepal (2015) the MNOs took a couple of approaches, one to provide credit top ups directly to their customers and another zero-rated services for their customers.[24]
- Long term increased churn in subscribers could also compound future revenue losses.

24. See page 20 in the GSMA DR Report "Nepal Earthquake Response and Recovery", http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/12/GSMA_Disaster-Response_Nepal_Workshop.pdf





### Asset loss/damage

Depending on the nature of the disaster there could be significant loss or damage of the business's assets including;

- Effective loss of staff, either through mortality or through an inability to get to or be available to work.
- Network infrastructure loss or damage – Towers, BTS, cables, servers, communications equipment, etc.
- Damage or loss of infrastructure providing redundancy to systems – e.g. power generations units such as diesel generators, solar panels, fuel cells, etc.
- Damage or destruction of Buildings and structures – e.g. BTS housings, NOC buildings, corporate premises, etc.
- Spectrum license – if for any reason the operator is unable to comply with regulatory requirements e.g. RTO, QoS, etc. within the constraints of disaster management guidelines they may be subject to fines and potential withdrawal of their spectrum license.
- From a business perspective a lot of this can be calculated in respect of the cumulative risk to the business based on potential damage to objects for a given scenario. Which in turn can be mapped to an evaluation of acceptable risk versus tolerated and unacceptable risks. From there a benefit to cost ratio can be derived for resilience building (risk reduction) for asset loss and damage in a given scenario.

## Reputational damage

Whilst disaster situations are outside of the MNOs control, the affects on the network and their ability to respond (or not) could lead to reputational damage or conversely an enhancement of their reputation. This will depend on their perceived responses to often very specific situations including;

- Inability to restore services within a recognised timeframe or inline with competitors in the market.
- Inability of subscribers to complete calls or get messages through when the network is available e.g. due to network congestion.
- Handling concerns of locals to key infrastructure placement concerns e.g. siting towers/BTS on private roof tops, during and after a disaster landlord /owners may deem that the equipment could be to the detriment to their building, in the case of an earthquake an owner may perceive that the weight of the equipment may contribute to further damage to their building.
- Recovery, coverage and capacity of cells at key facilities e.g. hospitals, displacement centres, etc.
- Poorly researched and/or speculative reporting in the press on network state or individual customer issues.

## Regulatory compliance

Issues here could either be an inability to meet regulatory requirements or from unachievable requirements applied to circumstances outside of which they were designed for. This could lead to significant risks from the regulatory body in the relevant country ranging from censures, fines and potentially curtailment of licenses.
It is in the best interest of the MNO to work with the regulatory authority to insure that the regulatory environment is flexible enough to allow for the depredations brought by the disaster to be managed and to encourage the authorities linked to the process to streamline processes during disasters in such a way as not to exacerbate the MNOs restoration work.

An example of this is where government agencies can effectively create blanket restrictions on transport resources which mean MNOs cannot reach key infrastructure. This happened has happened in past earthquake responses, where all private (and public) helicopters were commandeered, which meant the local MNOs could not source helicopters to get out to remote base stations for fuel re-supply, damage assessment and repair for a short but critical period.





# 9.2.2 Understanding the risks for the network

### Damage susceptibility

The business will need to consider for the most probable disaster scenarios the level of vulnerability within their network infrastructure e.g. roof top towers/BTSs what level of building code is the host site built to? This assessment should be across all the key components of the infrastructure from core to edge, and take into account the level of redundancy employed, possible single points of failure, critical cell sites, etc.

### Utilities

The business will need to assess risks from utilities (especially power) disruption during disaster scenarios, including local generation capabilities, level of redundancy required given adjacent (utility) industry stated RTO and/or vulnerability of alternative supply chains e.g. does the current back up power meet the capacity required before normal power supply can be restored. This should also take into account possible increased power needs in the case of critical cell sites, where transmission power is increased (under license) to allow wider coverage, or the use of alternative backhaul methods.

### Supply chains

The business will need to assess risks of key suppliers and their supply chain meets the internal supply chain requirements e.g. fuel supply for DGs, are the supplier's depots, reserves and transportation sufficiently organised and redundant to provide the necessary supply to meet RTOs in a given scenario? It has be noted by some MNOs that in undertaking supply chain reviews for BCP, they have found ways of increasing the day-to-day reliability of those supply chains.

## 9.2.3 Understanding the risks for the subscribers

### Churn

The business will need to assess risk of longer term customer churn if the perception of the subscriber is that another provider gave a better service during a disaster.

### Payments

How likely will it be that subscribers will not be able to pay post paid bills or pre-pay top-ups both during and in the immediate aftermath of the disaster, where are the vulnerabilities in the revenue chain and estimate the RTO of these e.g. a top-up card vendor may not be able to verify and activate card sales, or post paid bills will not be paid until the banking system is back up.

### End user equiptment

Whilst the end user equipment i.e. phone, is the responsibility of the user (in most cases), if the disaster renders a significant proportion of phones as unusable the MNO may want to consider options to help restore working phones to the subscribers in order to maintain service usage.

Another significant vulnerability is power supply for charging phones.

SIMs tend to be fairly robust and can be easily switched between phones (where the phone has been damaged) but loss of SIM (with the phone) may be an issue, requiring replacement and activation.

Many MNOs run subscriber facing campaigns[25] reminding users of preparations they may want to take to ensure the best chance of continued access to mobile services during a disaster as well as personal safety, especially in areas where there are "seasons" when a scenario is likely to happen.

25. See example of SMART public campaign on Page 8 of GSMA report "Effective Disaster Preparedness and Response Programme", http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Designing-an-Effective-Disaster-Preparedness-Response-Programme.pdf



# 9.3 Implementing and maintaining BCM

## Internally[26]

Establishing a good working management structure for disaster and continuity is key factor in the MNOs resilience, this includes (but not limited to);

- Creation of a core management crisis team including senior executive representation and department heads.
- Creation of Crisis Command Centre, where the relevant personnel can be situated. This may need to be able to be moved and/or made mobile where a disaster affects the designated facility.
- Creation of key working groups covering critical functions e.g. network, marketing, etc.
- Clear definition of roles e.g. RACI example, points of contact and duties with a level of redundancy to cover staff who may be unavailable.

For example, AT&T during simulations will randomly select a number of their personnel to be non-responsive during the test.

- Clear guidelines on command structure and backups for points of failure.
- As described in section 3.1 the establishment of a BCP and cycle (assess, plan, build, test and update) and it's maintenance is a given for BCM. Larger organisations should consider setting up a core team of full time staff dedicated to BCM/BCP as well as those assigned on a part time basis.

26. Also see GSMA report "Effective Disaster Preparedness and Response Programme", http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Designing-an-Effective-Disaster-Preparedness-Response-Programme.pdf

**Externally**

# Establishing a good working management structure for disaster and continuity is key factor in the MNOs resilience, this includes (but not limited to);

## Business partners

A key factor here is to make sure the key business partners BCPs' are in place, aligned with the MNOs and working to the same KPIs e.g. RTO. Hence the need for cascading BCPs from the MNOs down into the partners, along with clear KPIs, points of contact and communication channels (with alternates). For example, Telecom vendors' capability to source replacement equipment from local inventory in a timeframe which allows the MNO to meet their RTO.

## Government

Close links with the relevant government bodies which could affect the MNOs ability to achieve RTO and humanitarian support, these need to be pre-defined, including (but not limited to);

- National Telecoms Regulatory Authority – this is probably the primary point of contact with the Government for the MNO and is often in charge of or heavily influence any disaster planning requirements for MNOs.
- National Disaster and Emergency Authority – where this exists it is usuall the primary authority on crisis management during a disaster and risk management including preparation and policy. As such it will often have an IT and Communication brief either directly or through the National Telecoms Regulatory Authority.

MNOs may have requirements to meet in terms of disaster preparedness and reporting (especially during a crisis) from this authority so a clear engagement process should be set up.

- Customs and Immigration Authorities – whilst MNOs may have limited access or direct contact with these authorities, they could prove to have direct effect on recovery efforts critical path e.g. in bringing telecoms equipment and specialist personnel into the country. So having clear and flexible engagement processes either directly or through the above authorities should be pre-defined.

## Humanatarian agencies

Whilst not critical to network recovery, humanitarian agencies rely heavily on communication to fulfil their front line services in disaster relief as effectively as possible. This will often mean bringing in key infrastructure for key staff in order to maintain planning, e.g. Satellite phones, localised unlicensed (e.g. WiFi) networks and backhaul (VSAT), UHF radios, etc. this is comes at a high cost for the NGOs so their ability to effectively leverage local network resources from the MNO is key. Also they recognise that mobile telecom channels are often the most effective method of communicating with the general populace during a disaster so having those channels available through coordination with the local MNOs and Authorities will help in their work.

GSMA DISASTER RESPONSE

# Humanitarian agencies include (but not limited to);

## International agencies:

- **United Nations – often at the forefront of any international response (at the invitation of the National Government)**

**UN Office for the Coordination of Humanitarian Affairs (OCHA)** is the part of the UN responsible for bringing together humanitarian actors to ensure a coherent response to emergencies. OCHA also ensures there is a framework within which each actor can contribute to the overall response effort. ( http://www.unocha.org ). OCHA also coordinates the cluster system for managing resources and organizations during a disaster.

**World Food Program** is a UN agency, which as well as their primary mission of providing food supplies during and post disaster situations also handles a lot of the logistical work including the lead on the ETC (see below).

**Emergency Telecommunications Cluster (ETC)** is an association of agencies, NGOs and private companies committed to providing the coordination of telecom resources during a crisis. This is probably the primary point of contact with the UN and its agencies during a crisis and ideally an MNO should have a clear point of contact with the local representative of the ETC or where that does not exist then into the global ETC through the GSMA Disaster Response team.

---

- **International NGOs**

There are a number of international NGOs who may be active in the country or who will come in as part of any UN led international disaster relief programs and like the UN agencies above require communications support to help them deliver their services in country.

Some of these NGOs may already have relationships with the MNOs (if not at a country level then possibly at a group level) through various CSR initiatives. They include NGOs such as Red Crescent/Red Cross, OXFAM, Save the Children, Plan, etc. Some of these NGOs may also be able to help support MNO staff caught in the crisis or having to work in demanding circumstances.

## Local NGOs

These tend to be smaller localised (to the country or region) NGOs with more of a “grass roots” approach. They also have communication support needs in the work they do but are more reliant on local telecom resources such as the MNOs network. They may also have a high quality of local information which could be helpful to the MNO in their restoration work.

# 9.4 Financing resilience investment

This section will highlight possible mechanisms which will help identify the value and/or help finance building resilience into the network and supporting business processes to be more effective in the face of disasters.

## Insurance

Taking out insurance with catastrophe cover is the most obvious mechanism to guard against losses from a disasters impact. In respect of the cost of building in resilience, most insurance companies will consider lower premiums where the business can show they have increased their businesses' resilience both to capital and revenue loss. This in turn could be factored into the cost:benefit ratio calculations to building resilience.

## Catastrophe Bonds & Reinsurance

Although not a direct benefit to MNOs, the insurance industry will attempt to mitigate the potential cost of insured losses in a disaster by reinsurance (passing on risk to a number of ceding companies) thereby spreading the risk. Alternatively, they may also issue short term catastrophe bonds to investors. In both cases the risk passed on is lowered by efforts to build resilience in the organisation being insured, this will help the principal insurer mitigate their risks and in turn lower premiums to the business.





## Catastrophe modelling

Insurance companies who offer insurance against disasters will usually model the risk through catastrophe modelling, which takes into account the potential capital and revenue loss of the business for a combination of disaster scenarios against the probability of the disaster occurring. Again where the business can show efforts to make the business and its infrastructure more resilient this will affect the "Cat" modelling and the resultant premium.

## Micro Insurance

With the uptake of financial services, such as mobile money (and related services) especially within the poorer segments of society, there has also been growing availability of micro-insurance services e.g. crop insurance for small holding farmers. Which could be extended (in theory) to cover disaster situations. For micro-insurance to be profitable for the insurers it requires a large client base which is something MNOs can potentially offer.
Whilst this won't decrease the cost of building resilience for MNOs it will help increase the resilience of their subscriber base by giving them greater access to capital, credit and insurance thereby improving their ability to recover, which in turn will help protect long term ARPU for the MNO.

## Donor and Government Grants

In certain circumstances national Governments, international donors and AID agenecies may offer grants, expertise or platform access, which can help build resilience, especially where it can be proven to help protect the most vulnerable sections of a society and aid its recovery during and after a disaster. For example, see the Rockefeller's initiative "100 Resilient Cities" [27]

27. https://www.rockefellerfoundation.org/our-work/initiatives/100-resilient-cities

# 9.5 Plan for resilience

It is widely accepted that spending on DRR can result in significant savings when a disaster strikes. An Australian commission in 2013 estimated that the annual economic cost of natural disasters would rise from $6 billion in 2012 to $12 billion by 2030 and $23 billion by 2050. It also estimated that increased Australian Government expenditure on pre-disaster resilience (of about $250 million per year) would reduce these costs by more than 50 per cent by 2050. However, spending on DRR for mobile networks could introduce significant cost depending on the actions taken. This is why it is important to consider DRR spend in accordance with the type, frequency and likelihood of a disaster happening in a given period and the most cost effective methods of dealing with such effects.

Some of the cost may be mandated by regulatory conditions and should be planned into capital and operational costs by the MNO. To help further investment in DRR, BCPs should be factored into the MNOs capital investment stages programmes as;

## Network restoration after a disaster

Whilst immediate restoration efforts are focused on re-establishing the service and may include a number of short term measures e.g. using a COW for immediate coverage needs the medium term re-build/recovery of capacity could be an opportunity to introduce a number of measures with better DRR qualities e.g. more effective bracing for IT and Telecoms equipment.

## Network upgrades and investment

Normal capex investment lifecycles will see elements of the network replaced and major upgrades will bring in improvements in network capacity, QoS, etc. During these phases the additional cost of planning in DRR steps could be a lot less. For example, upgrading a network to LTE/4G should in theory offer more flexibility and resilience as a pure IP topology, allowing for greater network re-configuration to handle network outages and congestion issues. Also, rather than re-cycling older phased out equipment consider holding some key components in storage for use in post disaster repairs (if only temporary), whilst replacement equipment is being sourced.

## Capacity upgrades

As CAGR of the network improves so there will be planned capacity upgrades, again embedding DRR into the planning phases could help see a network resilience uplift and make sure in implementing the upgrades no unnecessary vulnerabilities are introduced to the network. For example, the upgrade of microwave links to LoS MIMO technologies as well as boosting capacity have shown to be less susceptible to vibration (which may be caused by high winds) also the separation of transmitters can effectively be seen as a level of redundancy.





# 10 Reference

## Glossary

| | |
|---|---|
| ARPU | Average Revenue Per User |
| BCM | Business Continuity Management |
| BCP | Business Continuity Planning |
| 3G | Third Generation (mobile network) |
| 4G | Fourth Generation (mobile network), see LTE |
| API | Application programming interface |
| BTS | Base Transceiver Station |
| CAGR | Compound annual growth rate |
| Cat | Catastrophe |
| CDR | Call Detail Record |
| CMT | Crisis Management Team |
| COWs | Cell on Wheels |
| COLT | Cell on Light Truck |
| DG | Diesel Generator |
| DRR | Disaster Risk Reduction |
| ETC | Emergency Telecommunications Cluster |
| GSMA | GSM Association |
| IP | Internet Protocol |
| KPI | Key Performance Indicator |
| LoS | Line of Sight (microwave) |
| LTE | Long Term Evolution (4G mobile network) |
| MDG | Millennium Development Goals |
| MIMO | Multiple-Input and Multiple-Output |
| MNO | Mobile Network Operator |
| MOIC | Ministry of Information and Communication |
| NGO | Non-Governmental Organisation |
| NOC | Network Operations Centre |
| OODA | Observe Orientate Decide Act |
| QoS | Quality of Service |
| RTO | Recovery Time Objective |
| SDG | Sustainable Development Goals |
| SIM | Subscriber identity module |
| SMS | Short Messaging Service |
| UHF | Ultra high frequency (radio) |
| UN | United Nations |
| UNFCCC | United Nations Framework Convention on Climate Change |
| UNOCHA | United Nations Office for the Coordination of Humanitarian Affairs |
| UNWCDR | RUN World Conference on Disaster Risk Reduction |
| VSAT | Very-small-aperture terminal (Satellite) |
| WFP | World Food Programme |

## RACI Matrix

A Roles and responsibility matrix is useful in setting up key processes on who should be;

- Responsible, who is the author/owner of a task/responsibility.
- Accountable, who has ultimate signoff and approval authority for a task.
- Consulted, who provides information and/or has the capability necessary to help complete the task.
- Informed, who must be notified of the results of the task/action but need not be consulted.

## Vendor Catalogues

An example of a vendor catalogue can be found here - http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/11/DR_vendor_catalogue.pdf

## Regulatory position

The “Emergency Mobile Telecommunications Regulatory Best Practice” can be found here - http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/GSMA-Industry-Position_Emergency-Telecoms-Regulation.pdf

## Humanitarian Connectivity Charter

The “Emergency Mobile Telecommunications Regulatory Best Practice” can be found here - http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/GSMA-Industry-Position_Emergency-Telecoms-Regulation.pdf

Principles

http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/07/Charter_Principles_document.pdf

Activities

http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/07/Charter_Activites_document.pdf

To download the GSMA Disaster Response report visit the GSMA website at www.gsma.com/mobilefordevelopment/

**GSMA HEAD OFFICE**
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601