INSTITUTE FOR RISK AND DISASTER REDUCTION
MULLARD SPACE SCIENCE LABORATORY

CASCADING EFFECTS OF GLOBAL POSITIONING AND NAVIGATION SATELLITE SERVICE FAILURES

Pescaroli, G., Green, L.M., Wicks, R. T., Bhattarai, S. and Turner, S.

CASCADING EFFECTS OF GLOBAL POSITIONING AND NAVIGATION SATELLITE SERVICE FAILURES

A review for improving continuity management and organisational resilience

Pescaroli, G., Green, L.M., Wicks, R. T., Bhattarai, S. and Turner, S

Please cite this report as:

Pescaroli, G., Green, L.M., Wicks, R., Bhattarai, S. and Turner, S. Cascading effects of global positioning and navigation satellite service failures. UCL IRDR and Mullard Space Science Laboratory Special Report 2019-02, University College London. DOI: 10.14324/000.rp.10076568

See also:

Wicks, R.T., Pescaroli, G., Green, L., and Turner, S., Organisational Resilience for Severe Space Weather, UCL IRDR and Mullard Space Science Laboratory Special Report 2019-01. DOI: 10.14324/000.rp.10076567

Affiliations

Dr. Gianluca Pescaroli, Prof. Lucie Green, Prof. Robert Wicks and Dr. Santosh Bhattarai are academic staff at UCL. Mr. Stuart Turner is Head of Emergency Management, London Borough of Ealing.

Websites:

www.ucl.ac.uk/risk-disaster-reduction
www.ucl.ac.uk/mssl

Follow us on twitter: @UCLIRDR | @Dr_Lucie | @RobTWicks

Contact: g.pescaroli@ucl.ac.uk, lucie.green@ucl.ac.uk

Acknowledgements

This work was supported by UCL's Knowledge Exchange and Innovation fund.

Disclaimer

This report contains guidelines written for non-academic audiences, which summarize scientific research in order to support the work of end users. It is not a substitute for technical advice or consultation of the full papers quoted in the references. These guidelines may not be resold or used for any commercial purpose.

Cover image: United States Air Force Navstar-2F satellite, part of the Global Positioning System (GPS).

Executive summary

Global navigation satellite systems (GNSS) provide vital timing and positioning services that are embedded across many sectors such as communication, transport and finance. Despite being an "invisible" infrastructure, GNSS is heavily interconnected with other services and is essential for maintaining "business as usual" activities. However, GNSS services can be affected both by natural and human-made threats, with practical implications for continuity plans and management strategies aimed at maintaining operational capacity. When building resilience to GNSS failures the possibility of cascading impacts must be taken into account. This report provides an essential overview of the most critical elements that could affect day-to-day operations, discussing the challenges around coping with such impacts and laying out guidance aimed at improving organisational resilience.

Introduction

Satellites are classed as Critical National Infrastructure. This infrastructure provides modern society with several key services, such as positioning and timing data, through global navigation satellite systems (GNSS). Various countries have, or are in the process of, establishing their own GNSS including America's Global Positioning System (GPS, Figure 1), Russia's Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS), Europe's Galileo and the Chinese Beidou Navigation Satellite System (BDS). A report by the Government Office for Science in 2018 suggested that GNSS could be defined as an "invisible utility" that enables communication systems to work, supports emergency services, and facilitates "the movement of goods and people, and the global supply lines that underpin our economy". It is clear that GNSS is incorporated into many services and sectors so it is vital that possible impacts triggered by GNSS disruption are well known. In addition, technological interdependencies are increasingly diffused and integrated at all levels of society, from "just-in-time" deliveries to activity trackers for monitoring personal training, which further increases the challenges that arise should GNSS fail.

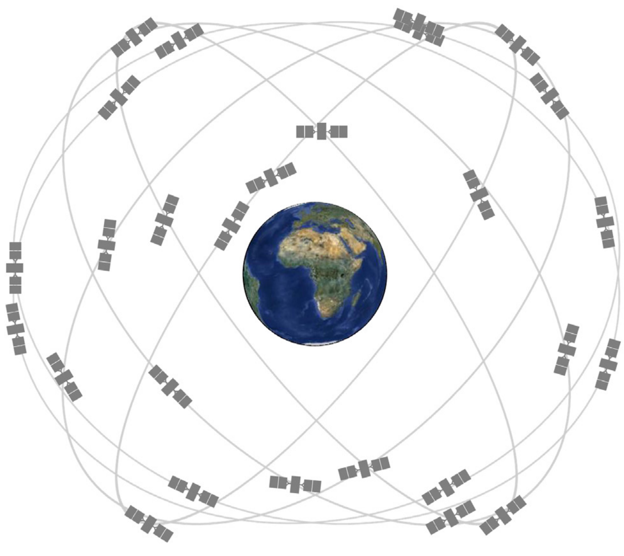

Figure 1: Schematic illustrating the GPS constellation of satellites. Source: www.gps.gov

GNSS outages can be a consequence of extreme space weather events produced by solar flares, energetic particles and/or geomagnetic storms (Cabinet Office/ BEIS 2015). Therefore having an effect society and the economy, for example the financial industry (Green et al., 2016). Possible vulnerabilities associated with GNSS failures can also be caused by human-made threats (Pescaroli et al., 2018), such as anthropogenic space weather generated by high-altitude nuclear weapon detonation (Gombosi et al., 2017) or cyber-attacks.

Attention is now turning to understanding the cascading effects of technological system failures on organisational resilience and wider society. For example, the cascading impact of wide-area power failures has been studied by UCL and London Resilience (Pescaroli et al. 2017). So far though, a detailed assessment of the cascading impacts of a failure of GNSS services has not yet been carried out.

Cascading effects can be defined as, "The dynamics present in disasters, in which the impact of a physical event or the development of an initial technological or human failure generates a sequence of events in human subsystems that result in physical, social or economic disruption" (Pescaroli and Alexander, 2015). Therefore, an initial impact can trigger other phenomena that in turn have consequences with significant magnitudes. Cascading effects are more related to the size of the technological or societal vulnerability than the magnitude of the initial hazard itself. For example, a low-level hazard can generate a chain of significant impacts if vulnerabilities in the system (or subsystems) are widespread and not properly addressed. For these reasons, it is necessary to isolate elements in any chain and see them as individual (subsystem) disasters in their own right.

Figure 2, taken from Pescaroli and Alexander (2015), illustrates the differences between: (a) a linear path in the chain of effects, and (b) a complex path of cascading effects. In cascading disasters, secondary emergencies can escalate and become the centre of a crisis (Pescaroli and Alexander, 2015). This concept has been expressed with the inclusion of the "E/C" spots in the figure, which create new escalation points and influence the evolution of the impacts by triggering their own chain of effects. These E/C spots can be interpreted as being a critical juncture in the chain of reactions triggered by a disaster, in which existing vulnerabilities amplify the cascade leading to a bigger impact than the mere reaction to the primary disaster would suggest (Alexander 2018).

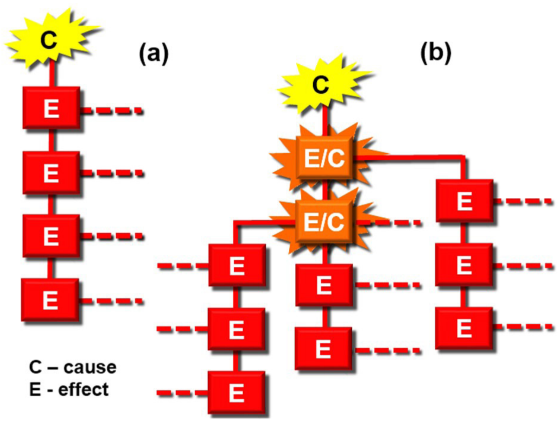

Figure 2: Flow chart illustrating the chain of events during a cascading disaster

The purpose of this document is to provide an overview of the vulnerabilities and interdependencies of GNSS in the UK and thus an overview of GNSS failures and their cascading effects for an operational audience. It does not pretend to be exhaustive, and nor can it be whilst introducing a complex topic to practitioners. First, we will discuss compliance with ISO standards and then we define the key functions of GNSS. Following this we provide an overview of possible challenges associated with failures followed by a table that describes the affected sectors and the associated possible cascading effects with a focus on operational impacts. In conclusion, we provide some basic recommendations for improving continuity management strategies and organisational resilience.

Compliance with ISO standards

This report has been designed to support the application of International Organisation for Standardisation (ISO) standards. In particular:

- ISO 22301:2019 "Security and resilience — Business continuity management systems — Requirements";

- ISO/IEC 27031:2011 "Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity";

- BS 65000:2014 "Guidance on organisational resilience", and in particular the consistency of resilience measures.

There are different uses of the following sections. First, the description of GNSS functions and the cascading effects of possible disruptions can support a better understanding of the operational context and of "invisible" risks that can compromise organisational resilience. We identify possible escalation paths to increase the awareness of critical interdependencies, mitigating their impacts, increasing flexibility of response, and defining procedures for faster recovery. Second, the outline scenarios and their cascading effects are intended as cornerstone elements for developing exercise and testing procedures, including disruptions to processes, suppliers, and critical technology. In conclusion, the checklist available at the end of this report is a practical tool to help assess possible criticalities in existing planning processes, identifying gaps between readiness capabilities and business continuity requirements so that corrective actions that improve continuity strategies and procedures can be introduced.

The assumption of this report is that each organisation is unique, and the short description that we provide can be seen as a starting point for further work that integrates specific organisational needs. In order to maximise the effectiveness of this work, we strongly encourage consideration of which critical vulnerabilities could affect an organisation in a scenario of GNSS disruption and other technological failures such as extended blackouts.

Key functions of GNSS

According to reports by the Swedish Civil Contingency Agency (2016) and the UK Government Office for Science (2018), there are two essential functions provided by GNSS:

1. Timing: Use of GNSS for synchronising information and time data between different systems e.g. for data records or for co-ordinating two or more communication systems. Other applications described by the UK Government Office for Science (2018) include power grid synchronisation, financial transactions, railway sensor timing and wireless network operations.
2. Position: To provide accurate positioning data, maps, navigation support, and monitoring services. Users described by the UK Government Office for Science (2018) include the legal domain (e.g. border disputes); security (e.g. asset tracking); transport (e.g. buses); leisure (e.g. social networking); agriculture (e.g. smart fertilisation); marine (e.g. containers tracking); aviation (e.g. air traffic control); military (e.g. command & control); civil engineering (e.g. bridges and dams); surveying and mapping and scientific applications (e.g. meteorology).

An overview of sector dependencies on GNSS can be summarised in the table below (UK Government Office for Science, 2018).

	Telecom	Emergency Services	Energy	Finance	Food	Transport
Time						
Position						

Table 1: Sector dependency on time and position data (Government Office for Science, 2018)

An immediate implication of this table, as noted by the Dutch National Institute for Public Health and the Environment (2016), is that there are different levels of dependency on satellite systems in many sectors, for example in telecommunications (both landline and mobile), internet and (financial) data traffic, logistics, transport, emergency response and management, as well as military and national security implications.

GNSS disruption scenarios

There are dynamics of scale, frequency and concurrency that have to be considered in the assessment of possible impacts and scenarios for GNSS interruption. Short-term (few hours) and localised (few 100 km) failures of GNSS caused by the blockage of satellite radio transmissions in the upper atmosphere are quite common and have relatively low impact, as happened for example in 2003 when extreme space weather disrupted some GNSS functions, affecting UK aviation for a few hours (Cabinet Office, 2017).

More extreme space weather can directly disrupt the operation of satellites themselves through high radiation doses that lead to on-board computer upsets and loss of satellite operations. Additionally, satellites can be "disorientated" if the system that maintains their pointing (e.g. star tracker) gets confused by spurious data created from the impact of high-energy particles. Permanent damage and even complete failure of satellites can also occur. In this case it would be necessary to replace the satellites, potentially taking many years to return performance to current levels. In that intervening period some level of GNSS performance may be possible, but the more satellites that are lost the more the service will be degraded (loss of accuracy in position and timing). Additionally, the system becomes more vulnerable to further disruption as fewer satellites means that the interruption of signals from one satellite due to space weather will have a larger impact on the accuracy of the service.

Official scenarios adopted by the authorities in Europe include, for example, two weeks GNSS outage, likely caused by extended radiation storms or an extended period of solar flare activity. A scenario in which more satellites are compromised implies restoration and recovery processes of longer than one month. Thus, it can be expected that the extent and duration of the cascade of events resulting from GNSS loss is associated with the capacity of users shifting to a “Plan B”. The widely known independent backup to GNSS is the (ground-based) e-Loran system, but development and operation of e-Loran receivers and transmitter networks have been slow and stop-start, mainly because GNSS has met user needs. However, even if society has not yet experienced it, longer term and cross-scale GNSS failures cannot be excluded and could increase damage as well as the level of uncertainty in scale and level of impacts. For example, an extended GNSS disruption would test the capacity of society to shift to a backup or a lower tech solution used in the past with strong implications for society.

GNSS failures could happen alone or concurrently with other on-going emergencies. For example, considering the increase in terrestrial weather extremes such as floods or storms in the UK, concurrent emergencies are possible. A lack of past examples of widespread technological disruption should not prevent us considering what the future may hold and our research has indicated that this is far from being an exercise in “crying wolf” (Pescaroli et al., 2018). In September 2017, the strongest solar flare in 12 years degraded radio and GNSS signals while emergency services were dealing with Hurricane Irma (Pescaroli et al., 2018). In general, the so-called Carrington event is used as the reasonable worst-case space weather scenario (e.g. Green et al., 2016). An event similar to the Carrington one would mean that GNSS would be “rendered inoperable for one to three days” (Cannon et al., 2013), which requires us to consider the challenges associated with this level of disruption. In addition to space weather another scenario for consideration is that of GNSS jamming. Although illegal, devices are cheap and easy to source. A state-organised cyber-attack or high-altitude nuclear weapon detonation could have similar effects. GNSS users in various sectors should have backup strategies in place to deal with localised GNSS outages. Some of these strategies will also be effective during widespread outages.

Challenges associated with GNSS disruption

The problems caused by GNSS disruption are associated with dependence on frontier technology and thus organisational resilience is dependent on the capacity to switch to backup or buffering solutions that often are low-tech. This has three key challenges for continuity management and organisational resilience:

1. Implications for the "just-in-time" economy, for which even a slowing down of processes has massive implications in terms of societal and economic costs, creating bottlenecks affecting supply and services, and spreading cascading effects across domains;

2. Limited availability of buffering solutions that become unavailable due to budget cuts and production pressures, which is a recurrent problem in disaster risk reduction and management at present;

3. Possible loss of knowledge about the routines and procedures that assured the functioning of systems in the pre-internet era. This is determined by two factors: loss of knowledge through retirement of experienced staff and loss of knowledge through the increased volatility of the job market. This means that previously used low-tech internal organisational procedures are not transferred because of the turnover of personnel.

The European Commission's Joint Research Centre argued that there could be vulnerabilities associated with GNSS dependencies embedded in other infrastructure (e.g. via timing signals), and that these could be unknown (Krausmann et al., 2016). Moreover, it has been argued that existing vulnerabilities need to be better assessed and mitigated, introducing for example redundancies and buffering strategies consistently amongst stakeholders. The impacts associated with GNSS disruption are very challenging to address because they are "hidden".

An overview of cascading effects of GNSS failure

The sectors impacted by GNSS disruption and their cascading effects are discussed in this section. In order to provide an overview of the recurrent paths that have been reported in the literature, each point is described in detail in Table 2 that follows. Please note that this does not pretend to be predictive or fully exhaustive. Its goal is to help emergency managers, emergency planners, and policy makers to have a rapid overview of the common issues that could arise. It is intended for training and operational purposes only. The impacts, timelines, and escalations are generic, and differences may exist between countries and between organisations. It must be noted that the literature on the subject is limited, and the lack of wide-scale precursors implies that there is a high level of uncertainty that could orient the different escalation paths. Moreover, the cross-sectoral diffusion of GNSS as an "invisible utility", as well as its growing integration in the system of systems, implies that there could be vulnerabilities that could have not yet been understood and identified.

Table 2 and Figure 3 build on the idea that cascading effects can amplify a secondary emergency. In Table 2 we categorise the impacted sector and the cascading relevant effects that are triggered. We also point out and describe some possible escalations of crises. Please note that in the description we do not mention the military sector and their facilities. Before using this application to build scenarios, please note that a specific operational context can influence the content of Table 2. Please also note that there are no definitive answers to these questions instead they should be intended as support tool for an evolving process, and further considerations should include technological failures at large.

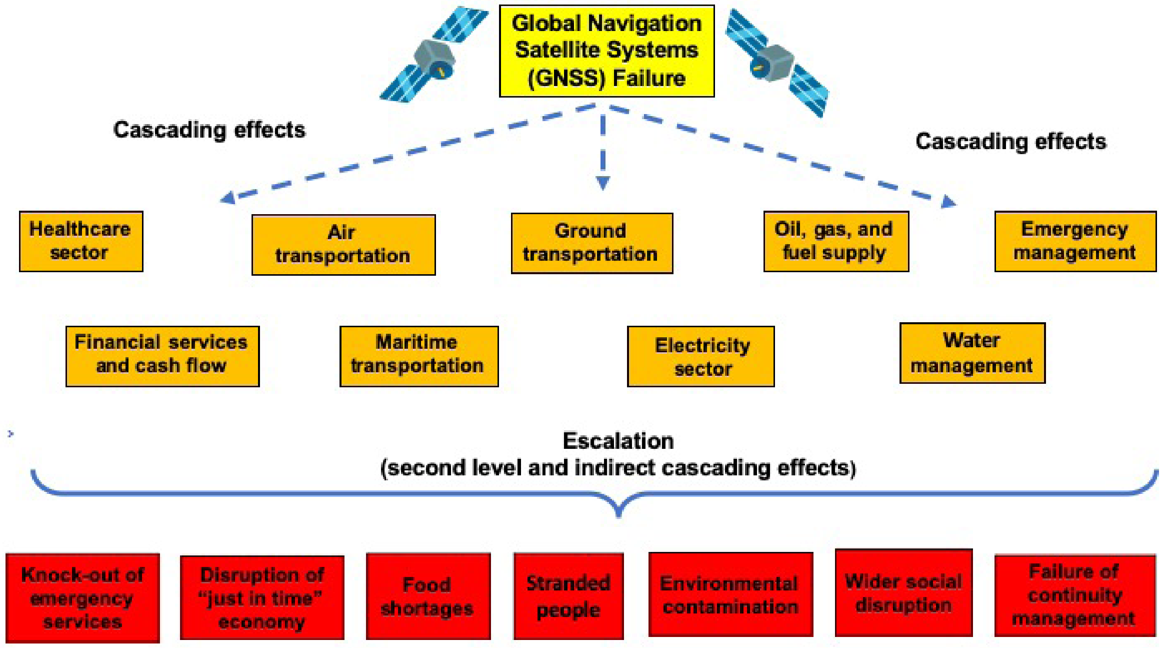

Figure 3: Schematic illustrating the escalation pathways for GNSS failures

Impacted Sector	Cascading effects
Healthcare	Possible increase in the loss of life and injuries associated with: → Raised number of accidents due to positioning failures and failures of anti-collision systems; → The decreased effectiveness of emergency services including hospitals, and ambulances; → Delays in dispatching ambulances and in them reaching patients.
Financial services and cash flow	GNSS disruption could cause loss of timing and synchronisation which could greatly decrease the reliability of the financial sector, affecting in particular: → Financial transactions, automated trading, cash flow; → Distribution and consumption of goods and services. In this case, the wider consequences may be expected in particular in those areas where the use of physical money has been largely substituted by cashless transactions and automatic cashing. i.e. lost buffering capacity to switch to traditional payment options.

Air transportation	Air transportation disruptions can be expected with interference in the navigation systems and vehicle tracking systems, creating possible issues during flights but also during landing and taking off operations: → Delayed aircraft and stranded passengers at airports; → Safety issues in landing / flying due to the lack of precision; → Reduced availability of certain goods and reduced effectiveness of the logistic chain; → In case of extended disruption limited to this sector, the reference case study may be the one of the volcanic eruption of 2010, where the management of stranded citizens became a major crisis despite other physical impacts. Note that the dependency on GNSS in air transportation sector is expected to increase in the near future.
Maritime transportation	Reduced efficiency of maritime transportation. Some systems on board ships will not work, e.g. reduced capacity of anti-collision systems, leading to: → Cargo stuck outside or inside harbours due to increased difficulties in manoeuvres, tracking, and increased risk of collision. Moreover, there could be possible conflicts with insurance policies and legal responsibilities of manoeuvring vessels; → Increased number of boats in distress due to loss of ability to navigate using methods other than GNSS during night-time or in case of reduced visibility such as fog; → It is possible that some area such as islands may suffer reduced vital connections e.g. ferries.
Ground transportation	Severe disruptions could be expected in this sector: → Railroads will be affected by failure in timing, telecommunication, selective door opening, with implications for community and transportation of goods; → Road transportation could be affected by loss of communication, time and positioning affecting e.g. integrated public transportation and both public and private command and control. For example, cash transportation activities could hampered because the moment-to-moment position of the cash-in-transit vehicles could not be sufficiently verified; → Possible issues can arise in the garbage removal and redistribution process, causing possible effects on healthcare; → The integration of GNSS in car alarms and speed monitoring could have impacts in the medium term on insurance claims, increasing the challenges for claims; → Future development of self-driving cars may exacerbate these issues.

Electricity sector	The electricity sector will have difficulties in industrial information and control systems, associated in particular with the use of GNSS for synchronisation: → Most stakeholders may be able to deal with such a disruption, if good continuity management procedures have been implemented, shifting to internal clocks. However, localised blackouts could be expected. A full list of cascading effects for electricity blackout has been already described in our previous guidelines (Pescaroli et al., 2017); → In case of extended scenarios (e.g. weeks) it is possible that internal clocks could start to drift requiring more monitoring and adjustments.
Oil, gas, fuel supply	The energy sector has a very large number of dependencies on GNSS, the extent of which is not completely clear. For example, GNSS has been integrated in offshore oil and gas drilling that could be affected, reducing the reliability of fuel supply. Moreover, it is possible that if GNSS failures activate telecoms disruptions these could cause cascading failures in this regard.
Telecoms	Telecoms have low dependency on GNSS, but this is expected to increase e.g. with the use of 5G. Further elements have been included in other categories as they primarily impact other sectors such as the raised number of alarms for emergency services.
Water management	Some reports include generic description of possible impacts and cascading effects on water management but these should be investigated further.
Emergency Management	GNSS has been largely integrated to the operational capacity of first responders: → False alarms confusing decision makers on what is a real source of escalation, because many safety tools are actually dependent on GNSS and failures could lead to “overlapping” sensitivity; → Uncertainty in jurisdictions and coordination (e.g. restoration of damaged infrastructure) because of the many uncertainties in the assessment process of GNSS as a “hidden infrastructure”; → The failure of other services such as financial transaction or transportation would impact the organisational capacity of first responders; → Lifeguard and other sea rescue activities may be unable to support vessels in distress because on the effects on maritime transportation (e.g. multiple vessels unable to communicate their exact position).

Escalation	Cascading effects
Knock-out of emergency services associated with compounding drivers	Compounding risk refers to the risk of concurrence of the GNSS failures with other hazardous conditions that could increase the complexity of the emergency: e.g. heat waves, which can increase wildfires, stressors on the health sector, and importance of refrigeration in food consumption, supply and production; cold weather and snow, which can be associated to loss of life related to lack of heating, or lower maintenance of the grid. In those cases, first responders could be subject to “knock-out scenarios” where deployment is stuck in the moment of maximum need.
Disruption of “just in time” economy	It is possible that the combination of failures in the transportation and financial sectors, could escalate disrupting the “just-in-time” economy, eventually causing an economic recession if long-lasting: → Supply lanes may be strongly affected as the “just-in-time” economy is heavily reliant on fast transactions and timely supply. For example, the cascading effects of disruption of maritime transportation include wider impacts on the economy and production, as the just in time system relies heavily on container transportation; → Consumers may not be able to maintain their routines, e.g. buying food, access public transportation (etc.). This would affect households, individuals, businesses but also emergency planners themselves, reducing their operational capacity; → It can be foreseen that SMEs could be fatally compromised for the limited availability of redundant resources and medium-term effect on credit; → The interruption of trading could induce financial losses, but also increase volatility and affect trust in the medium term. The risk of failures could facilitate the development of other issues associated with cyber security, such as market manipulation. Note: There are different levels of awareness of these vulnerabilities among operators, and the EU JRC highlight the existence of “non-uniform level of preparedness”.
Food supply: food shortages	Food shortages may be triggered by an extended GNSS failure, as an effect of the disruption of “just-in-time” economy. In other words, due to the limited amount of stored supply even the gravity of limited but extended failures could be exacerbated by existing bottlenecks/lack of buffering. This could happen at different levels simultaneously due to: → Possible dependencies on imported food via maritime transportation; → Possible dependencies on ATM, and electronic transitions that guarantee the circulation between producers, distributers, and consumers. The wide-spread use of ATMs, automatic cashiers, and the high reliance on cashless payments in everyday consumer’s behaviour decreases the resilience of the supply chain and can result in reduction in cash flow, and blockage of cashless transitions; → Increase of travel time associated with ground and air transportation; → GNSS failures could affect precision farming, impacting the sector productivity in the longer term.

Cross-sector transportation failures: Stranded people	Due to multiple transportation failures, stranded citizens could become a primary crisis to manage in case of long-lasting failures for two key issues: → A "worst case scenario" affecting air transportation could be referred to the volcanic eruption of 2010, but this could be escalated by lack of buffering in the rail, road and maritime transportation, see above.
Environmental Contamination	Failures associated with energy production and storage may become out of control and escalate into wider environmental contamination. The possibility of collision of oil tankers is increased, if the automatic identification system (AIS) is not functioning.
Wider social disruption	The unavailability of GNSS in all sectors of transportation will affect the logistics of goods and services and will increase the strain on ordinary activities at all levels of government and management: → Reduced capacity of workers to access the workplace due to transportation bottlenecks. The most affected will be urban areas subject to high levels of commuting, which are often the most dependent on both cashless transaction and public transport; → Health issues arising from the loss of effectiveness of other sectors, such as transportation of food or safety of chemical sites; → Long-term issues associated with loss of precision in the building of infrastructure in progress during the GNSS failure; → Rise in the number of accidents to which reaction could be limited by loss of efficiency of services.
Failure of continuity management	The major challenge could be that the cross-sectoral failures may force a move from high tech procedures to lower tech intensive options. Main effects: → Un-assessed vulnerabilities could lead to a possible "surprise effect" that could limit undertaking effective countermeasures; → Public and private organisations can be affected by a lack of access to services and personnel, becoming a strain for maintaining productive capacity.

Table 2: Overview of cascading effects of GNSS failures

Recommendations for improving continuity management

Official reports such as the one by the Government Office for Science (2018) provide guidelines for increasing the resilience of technology to GNSS failures. However, considering the cascading effects described above, the following questions can be used as a basic guide to facilitate dynamic improvements in continuity management systems and the consistency of resilience measures:

List the technological systems that services or departments in your organisation are most dependent on?

Did you consider how GNSS is related to those systems?

Are you using any forward-looking tools and wider impact assessment methods for assessing the possible impacts of technological disruptions? (e.g. blackouts)

Did you assess the cascading effects of technological disruptions in your planning and strategies? (e.g. blackouts)

Are any of your business continuity contingencies reliant on GNSS?

Did you consider how GNSS failure could affect your organisational resilience?

Have you ever exercised a scenario of a GNSS failure in your organisation?

Did you consider how to manage your business in case of disruption of cashless transactions and financial movements?

Did you exercise disruption to cashless transactions?

References

- Alexander, D.E. (2016). *How to write an emergency plan.* Dunedin Academic Press, Edinburgh.
- Alexander, D. E. (2018). *A magnitude scale for cascading disasters.* International Journal of Disaster Risk Reduction.
- *BSI Standards (2019) Societal security - Business continuity management systems-Requirements. BS EN ISO 223101:2019. The British Standards Institution.*
- BSI Standards (2014) *Guidance on organisational resilience.* BS 65000:2014, The British Standards Institution.
- Cabinet Office (2017). *National risk register of civil emergencies 2017 edition.* Cabinet Office, London.
- Cabinet Office and Dept. for Business Innovation & Skills (2015). *Space weather preparedness strategy, Version 2.1.* Cabinet Office, London, UK.
- Cannon, P. S., et al. (2013). *Extreme Space Weather: Impacts on Engineered Systems.* Royal Academy of Engineering London, UK.
- Government Office for Science (2018), *Satellite-derived Time and Position: A Study of Critical Dependencies,* the Blackett Review. Government Office for Science, UK.
- Green, L., Deighton, R., Baker, D. (2016). *Building Space Weather Resilience in the Finance Sector.*
- Gombosi, T.I., Baker, D.N., Balogh, A. et al. (2017). *Anthropogenic Space Weather.* Space Sci Rev 212: 985.
- Hapgood, M. (2017). *Satellite navigation—Amazing technology but insidious risk: Why everyone needs to understand space weather.* Space Weather, 15(4), 545.
- ICAO (2018) *Dual frequency multi-constellation (DFMC) Global Navigation Satellite System (GNSS).* ICAO Navigation Systems Panel, CONOPS V6.4
- Krausmann, E., Andersson, E., Gibbs, M., Murtagh, W. (2016). *Space Weather & Critical Infrastructures: Findings and Outlook.* EUR 28237 EN, 2016, doi:10.2788/152877
- National Institute for Public Health and the Environment (2016). *National Risk Profile 2016.* National Institute for Public Health and the Environment,, The Netherlands
- Pescaroli, G., Turner, S., Gould, T., Alexander, D.E., and Wicks, R. (2017). *Cascading impacts and escalations in wide-area power failures.*
- Pescaroli, G., Wicks, R. T., Giacomello, G., & Alexander, D. E. (2018). *Increasing resilience to cascading events: The M. OR. D. OR. scenario.* Safety Science.
- Pescaroli, G., and Alexander, D. E. (2015). *A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor,* Planet@Risk, Global Forum Davos, 3(1), 58.
- Pescaroli, G., and Alexander, D.E. (2016). *Critical infrastructure, panarchies and the vulnerability paths of cascading disasters,* Natural Hazards, 82(1), 175
- Royal Swedish Civil Contingencies Agency (2016). *A summary of risk areas and scenario analyses 2012–2015.* ISBN: 978-91-7383-681-4 Swedish Civil Contingencies Agency.