# Assessing the Wider Resilience of the Defence Industrial Supply Chain

International Symposium on Military Operational Research (ISMOR)

July 2015

Author: Jay Edwards (CORDA)

**This page is intentionally blank**

# 1 Executive Summary

Recent catastrophic weather events such as Hurricane Katrina in 2005 and the 2011 Tohoku earthquake & tsunami resulted in severe disruption to global supply chains. This study has been conducted to assess the wider resilience of the UK Ministry of Defence (MOD) industrial supply chain. The focus of the study was supply chain resilience to natural hazards and an approach has been developed for the identification, analysis and mitigation of natural hazard risk. This approach can also be also used to analyse other supply chain risks such political unrest, material scarcity and cyber espionage.

The study indicates that the risk in the MOD industrial supply chain needs to be more proactively managed for the following reasons:

1. **Risk is Evident**
   Historical examples illustrate that natural hazards have disrupted supply chains which has impacted government defence agencies both financially and operationally. These examples include the flooding of both BAE Systems, Johnson City and the Atomic Weapon Establishment, Burghfield, and hurricane damage at Homestead Air Force Base, Florida. Historical examples also indicate that defence supply chains are vulnerable to Chinese counterfeit goods, labour strikes and cyber espionage. A RAND report illustrates that the US Air Force is concerned about risks in the industrial supply chain[1].

   Case studies were carried out and supply chain data was collected from three of the MOD's suppliers; BAE Systems Munitions, BAE Systems Maritime and Morgan Composites & Defence Systems. This data indicated that there may be vulnerable nodes in the MOD's industrial supply chain which could be at risk from natural hazards and if compromised could impact the MOD both financially and operationally.

2. **Risk is likely to Increase**
   Supply chain risk is likely to increase in the future due to global warming, increasing global inequality, resource scarcity, growth of organised crime, reduced inventory holdings by MOD and industry, and the drive to find the lowest cost supplier anywhere in the world.

3. **An Approach is Available**
   A pilot approach for the identification, analysis and mitigation of natural hazard risk in the MOD industrial supply chain has been developed. This relies on relatively inexpensive commercial software which can be used to consolidate natural hazard data and collect data from the supply chain via questionnaires. This approach can also be also used to analyse other supply chain risks such political unrest, material scarcity and cyber espionage.

For these reasons mapping and analysing risk in the MOD's industrial supply chain is achievable and extremely important.

[1] RAND, Identifying and managing air force sustainment supply chain risks, Nancy Y. Moore, Elvira N. Loredo, 2015, http://www.rand.org/pubs/documented_briefings/DB649.html

**This page is intentionally blank**

# Contents

# Lists of Figures



# List of Tables

# 2 Introduction

Recent catastrophic weather events such as Hurricane Katrina in 2005 and the 2011 Tohoku earthquake & tsunami resulted in severe disruption to global supply chains. This study has been conducted to assess the wider resilience of the UK Ministry of Defence (MOD) industrial supply chain. The focus of the study was supply chain resilience to natural hazards and an approach has been developed for the identification, analysis and mitigation of natural hazard risk. This approach can also be also used to analyse other supply chain risks such political unrest, material scarcity and cyber espionage.

The study was split into four phases which will be summarised in this paper:

1. **Research** – Historical supply chain problems were researched and existing supply chain risk management practices, natural hazard risk methodologies and supply chain management software were assessed.

2. **Vulnerability Assessment Framework** – A framework was designed to store data and analyse supply chain data collected from three case studies.

3. **Case Studies** – The Vulnerability Assessment Framework was populated with data from three supply chain case studies. Data was collected from BAE Systems Munitions, BAE Systems Maritime and Morgan Composites & Defence Systems.

4. **Pilot Approach** - An example of a working solution for the measurement of natural hazard risk in the MOD industrial supply chain was developed. This approach was found to be appropriate for measuring other supply chain risks.

This study was carried out by CORDA for the Dstl Resilience Programme (Defence Science and Technology Laboratory) under the 'Operational Analysis Capabilities Collaborative Analysis' framework and was sponsored by ACDS Log Ops (Assistant Chief of Defence Staff, Logistical Operations) and DE&S QSEP (Defence Equipment & Support, Quality Safety and Environmental Protection).

# 3 Historical Supply Chain Problems

Historical examples of a government defence agency being financially or operationally impacted by a natural hazard or other wider supply chain problems were collected.

Examples of natural hazards which have impacted a government defence agency financially or operationally:

1. BAE Systems – Johnson City (Flood)
2. Atomic Weapons Establishment – Burghfield (Flood)
3. United States Air Force – Homestead Air Force Base (Hurricane)

Examples of wider supply chain problems which have impacted a government defence agency financially or operationally:

4. Chinese Counterfeit Goods
5. Lockheed Martin – Fort Worth (Strike)
6. BAE Systems – Samlesbury (Cyber Espionage)

The historical examples illustrate that government defence agencies are vulnerable to supply chain risks that can cause a financial or operational impact. They also illustrate that it is important to take into account the full spectrum of risks which a supply chain could be exposed to such as natural hazards, political unrest, pandemics, counterfeit goods and cyber-attacks.

## 3.1 BAE Systems, Johnson City (Flood)

BAE Systems Legacy Platform Solutions was located in Johnson City in New York State and housed manufacturing, design, test, repair and administration departments. In September 2011 the site was flooded with over 16 million gallons of water, as shown in Figure 1[2]. However the disaster recovery was extremely efficient and critical equipment was recovered, cleaned and installed in a nearby facility within two weeks. A new site was opened a year later in the same region but on higher ground.

The financial impact to BAE Systems and the US Department of Defence was significant however there was no operational impact due to the rapid recovery of BAE Systems and supply chain redundancy.

**Figure 1 – BAE Systems, Johnson City**

[2] WBNG, BAE Intends to Stay, September 2011, http://www.wbng.com/news/local/BAE-Assessing-Damages-No-Guarantees-129688708.html

## 3.2 Atomic Weapons Establishment, Burghfield (Flood)

The Atomic Weapons Establishment (AWE) operates a site in Burghfield, near Reading. The site is responsible for the final assembly of Trident mounted nuclear warheads, their in-service maintenance and their eventual decommissioning. In July 2007 the site was flooded and all the buildings in the key nuclear assembly area were inundated by floodwater, as shown in Figure 2[3]. It could have been a critical accident however due to the timing of the flood (Friday afternoon) the majority of the radioactive material had been removed from processing facilities and returned to storage[4].

The flood resulted in approximately £6m of costs[5] for the MOD and there was disruption to nuclear weapons manufacture with no live nuclear work for 9 months[6].

## 3.3 United States Air Force (USAF), Homestead Air Force Base (Hurricane)

The Homestead Air Force base located in Southern Florida was home to approximately 75 F-16's in the 31st Tactical Fighter Wing. In August 1992 Hurricane Andrew hit the air force base and severely damaged the majority of the 2000 buildings on the base. However most of the F16's were evacuated before the hurricane hit[7]. Due to the extent of the damage one third of the site was redeveloped as an Air Reserve base and the rest was sold to developers[8].

The impact on the US Department of Defence was approximately $100m in repair and rebuild costs and three F-16's that were not airworthy at the time were heavily damaged by the hurricane, as shown in Figure 3[9]. There was no significant operational impact due to the number of other Air Force bases that could be used.

**Figure 2 – Atomic Weapons Establishment, Burghfield**


**Figure 3 – Homestead Air Force Base, Florida**

[3] The Telegraph, Britain's Nuclear Weapons factory nearly overwhelmed, October 2008, http://www.telegraph.co.uk/news/uknews/defence/3178392/Britains-nuclear-weapons-factory-nearly-overwhelmed-by-flood.html
[4] The Telegraph, Britain's Nuclear Weapons factory nearly overwhelmed, October 2008, http://www.telegraph.co.uk/news/uknews/defence/3178392/Britains-nuclear-weapons-factory-nearly-overwhelmed-by-flood.html
[5] GetReading, Taxpayers £5m bill for AWE Flooding, July 2014, http://www.getreading.co.uk/news/local-news/taxpayers-5m-bill-awe-flooding-4224736
[6] Nuclear Information Service, Public pay £5m for flood damage, July 2010, http://www.nuclearinfo.org/article/awe-burghfield/public-pay-five-million-pound-bill-flood-damage-uks-nuclear-weapons-factory
[7] Air Special Report, Ten Year After Andrew, August 2002, http://www.air-worldwide.com/_public/NewsData/000258/Andrew_Plus_10.pdf
[8] Los Angeles Times, A ghost town air base, March 1993, http://articles.latimes.com/1993-03-15/news/mn-433_1_air-force
[9] F-16.net, Hurricane Andrew F-16's destroyed, http://www.f-16.net/forum/viewtopic.php?t=5458

## 3.4 Chinese Counterfeit Goods

In 2012 an investigation by the US government reported 1,800 Chinese counterfeit cases in the US Department of Defence supply chain covering a total of 1 million individual parts[10]. Investigators traced 70 percent of the cases back to China and nearly 20 percent were traced to Britain and Canada - resale points for counterfeit Chinese parts. Counterfeit components are generally used components which have been disposed of. They are then reclaimed, cleaned, sanded down and reprinted with fake product markings in facilities such as those shown in Figure 4[11]. The counterfeit components are then resold back to companies supplying the US Department of Defence.

The investigation uncovered counterfeit parts on a number of equipment programmes:

1. **SH–60B Navy helicopter** – Counterfeit electronic parts were found in the forward-looking infrared (FLIR) system which provides night vision capability – one of the FLIRs was sent to the USS Gridley in the Pacific fleet.

2. **C–27J Transport aircraft** – Counterfeit parts were found in a display unit which failed during routine testing.

3. **P–8A Poseidon surveillance aircraft** – Counterfeit parts were found in the ice detection module which failed during a test flight.

4. **Terminal High Altitude Area Defence (THAAD) missiles** – Counterfeit parts were found in mission computers.

The impact on the US Department of Defence included an approximate $2.7m cost to replace parts in THAAD missiles and further costs due to investigations and replacing other parts. There have been no catastrophic failures reported, however this could be a risk.

**Figure 4 – Chinese Counterfeit Good Suppliers**

[10] US Government Printing Office, Investigation into Counterfeit parts in DOD supply chain, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf
[11] US Government Printing Office, Investigation into Counterfeit parts in DOD supply chain, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg72702/pdf/CHRG-112shrg72702.pdf

## 3.5 Lockheed Martin, Fort Worth (Strike)

The Lockheed Martin site in Fort Worth, Texas is an aircraft assembly and manufacturing site which works on the F-35, F-16 and F-2 fighter jets. In April 2003 a two week strike was organised by 4000 unionised staff. Workers had foregone raises due to the global economic crisis and demanded compensation in 2003 due to Lockheed Martin's improved profits[12]. Lockheed Martin brought in non-unionised labour during the strike but they lacked the technical skills required.

The impact was a 3 month delay in delivery of the first of 100 F-16's for the Israeli Air Force[13] and an unknown delay in delivery of F-16's for the Hellenic and Egyptian Air Force[14].

## 3.6 BAE Systems, Samlesbury (Cyber Espionage)

The BAE Systems site in Samlesbury, Lancashire is a manufacturing site which produces the aft fuselage and the vertical and horizontal tails for the F-35 Joint Strike Fighter. Cyber espionage was reported to have occurred against BAE Systems in 2009 and again in 2012 (Lockheed Martin was also targeted). It is likely that certain details about the design and performance of some systems on the F-35 Joint Strike Fighter were stolen[15].

There are reports that the cyber-attacks resulted in programme delays and increased costs for the US Department of Defence and F-35 Partner Nations due to investigations and redesign of critical equipment[16]. In terms of operational impact adversaries are able to reduce technological advantage; the Chinese J-31 stealth fighter is reportedly based on the F-35[17].

[12] Globes, Delay in supply of F-16 to Israel due to Lockheed Martin Strike, http://www.globes.co.il/en/article-701330
[13] Globes, Delay in supply of F-16 to Israel due to Lockheed Martin Strike, http://www.globes.co.il/en/article-701330
[14] F-16.net, F-16 deliveries to mid east allies will be delayed, http://www.f-16.net/f-16-news-article837.html
[15] DEF, Top official admits F35 Fighter Secrets Stolen, June 2013, http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/
[16] DefenseTech, Did Chinese Espionage Lead to F-35 Delays?, February 2012, http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/
[17] DEF, Top official admits F35 Fighter Secrets Stolen, June 2013, http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/

# 4 Literature Review

A wide ranging literature review was carried out with Cranfield University to assess existing supply chain risk management practices, natural hazard risk methodologies and supply chain management software.

## 4.1 Supply Chain Risk Management

A standard three step approach to supply chain risk management was found which aligns to traditional risk management theory:

1. Identify Risk
2. Assess Risk
3. Plan Mitigation

These three areas will be discussed in the following sections.

### 4.1.1 Identify Risk

Supply chain risks emerge due to the increased exposure to a number of risk types that can have direct implications on the ability of the supply chain to continue functioning as intended. These risk types are shown in Table 1.

| **Risk Type** | **Specific Risks**[18] |
|---|---|
| Disasters | Natural hazards, pandemics |
| Geopolitical | Political changes, instability in a country |
| Economic | Raw material price fluctuation, currency fluctuations, market changes, energy price volatility, supplier/partner bankruptcy, rising labour costs |
| Social | Labour force strikes |
| Technological | Changes in technology, unplanned IT disruptions, telecommunications outages |
| Legal | Export/Import bans, sanctions, regulations (health and safety, environmental etc.) |
| Security | Theft, cyber-attacks |
| Product | Conflict materials, material scarcity, counterfeiting |

**Table 1 – Risk Types**

In order to identify these risks the nodes that make up the supply chain must be identified and analysed so that a measurement of risk can be applied to each node. Supply chain mapping can be combined with the data provided by suppliers and risk information providers to create an understanding of risk exposure in a supply chain.

[18] Prof. David Simchi-Levi. (2013) 'Supply Chain and Risk Management', MIT Forum

### 4.1.2 Assess Risk

In order to assess supply chain risk the probability of every risk must be combined with the impact these risks will have on each supply chain node and the outputs of a business or organisation. A risk matrix[19] is the standard approach used to combine probability and impact and is shown in Table 2.

| | | Impact | | | |
|---|---|---|---|---|---|
| | | **Negligible** | **Marginal** | **Critical** | **Catastrophic** |
| **Probability** | **Certain** | 3 | 6 | 9 | 10 |
| | **Possible** | 2 | 5 | 8 | 10 |
| | **Rare** | 1 | 4 | 7 | 9 |

**Table 2 – Risk Matrix**

The risk matrix is used to categorise risks so that the focus can be on frequent and high impact risks. Attention can also be paid to high impact and low probability risks depending on the risk management strategy.

### 4.1.3 Plan Mitigation

The assessment of the risk and impact rating at each supply chain node will form a list of risky and critical supply chain nodes where risk mitigation actions may be required. A number of common mitigation actions are shown in Table 3.

| **Mitigation** | **Description** |
|---|---|
| Supplier Approval Process | A robust supplier approval process will ensure that only suppliers which have a low exposure to risk are chosen. |
| Monitor Supply Chain | A supply chain can be monitored using third party information providers and by communicating with supply chain partners. This will ensure any emerging risks are identified. |
| Build In Resilience | Supply chain resilience can be increased by ensuring that a product has two or more supply chain flows in different geographical locations. |
| Physical Protection | A supply chain location can be physically protected against natural hazards or security risks by building walls, using stilts etc. |
| Contingency Plans | If robust contingency plans exist for each supply chain risk at each node then the recovery time should be much quicker. |
| Insurance | If appropriate insurance is taken out then financial losses can be minimised. |

**Table 3 – Mitigation Actions**

The decision to carry out a mitigation action will be based on a cost-benefit analysis to ensure that the cost of mitigation is not higher than the cost of any predicted losses – both financial and reputational. Putting this into a military context, the MOD would need to balance the benefit of lower operational risk against the cost of mitigation.

[19] Banerjee, A. (2011) 'Equivalence of Risk: A Mathematical Approach', The 29th International System Safety Conference. MGM Grand Hotel, Las Vegas, Nevada 8 Aug – 12 Aug

## 4.2 Natural Hazard Risk

There is an abundance of publically available natural hazard data from around the world that can be found on the internet. However the main problem in trying to integrate these databases is that there is very little commonality in definitions, detail, geographical resolution, geographical coverage, data format and language which makes verifying and comparing the data very difficult.

There are however two international natural hazard databases which have been developed by Munich RE (NATHAN – Natural Hazards Assessment Network[20]) and Swiss RE (CatNet – Catastrophe Network[21]) to calculate insurance rates for companies. These databases have been consolidated from publically available records, academic studies and historical losses. Modelling is also used where data is not available for certain geographical areas and time periods. The two international natural hazard databases offer a high level 1-10 probably and severity ranking for common natural hazards (Earthquake, Volcano, Flood, Storm, Wildfire etc.) for any longitude and latitude in the world. The two databases also include an online world map visualisation tool. Swiss RE CatNet is commercially available and Munich RE NATHAN is currently only available for Munich RE insurance customers. Thus Swiss RE CatNet was used for this study.

## 4.3 Supply Chain Management Software

Supply chain management software started to be developed in the 1980's in order to improve the efficiency and cost effectiveness of complex supply chains[22]. Supply chain mapping software is a sub set of supply chain management software and is now commonly used if an organisation wants to perform the following tasks:

1. **Data Gathering** – Gather data from a supply chain using automated questionnaires which are emailed to suppliers who then forward them on to their suppliers.
2. **Data Storage** – Automatically store the data collected in questionnaires in a database.
3. **Third Party Data Providers** – Use third party data sources such as Swiss RE's CatNet to automatically check risk ratings at each supply chain node.
4. **Analysis and Reporting** – Analyse the risk in a supply chain and produce standard maps and reports.

For this study 16 supply chain mapping software packages were assessed and two (NQC[23] and Value Chain[24]) offered the most promising approach for the assessment of the MOD industrial supply chain.

[20] 'NATHAN', Munich RE, http://www.munichre.com/en/reinsurance/business/non-life/nathan/index.html
[21] 'CatNet', Swiss RE, http://www.swissre.com/clients/client_tools/about_catnet.html
[22] 'An Executives Guide to Supply Chain Management Software Systems', http://www.erp.asia/scm-evolution.asp
[23] NQC, http://www.scc.com/our-isv-programme/isvs/nqc/
[24] Value Chain, http://valuechain.com/

# 5 Vulnerability Assessment Framework

During the study a Vulnerability Assessment Framework was designed to store and analyse supply chain data collected from case studies so that the natural hazard risk could be assessed. The Vulnerability Assessment Framework provides:

1. A standard format for collecting and storing supply chain data which is in Microsoft Excel but can be adapted into a database format in supply chain mapping software.

2. A standard format for the creation of questionnaires which can then be used to collect data from the supply chain. These questionnaires can be integrated with supply chain mapping software.

3. A list of nodes in a supply chain from most risky to least risky. A high risk node in a supply chain would be subject to natural hazards, would take a relatively long time to recover from a disaster, and would produce products which are relatively scarce or unique.

The Vulnerability Assessment Framework is made up of a five step process as shown in Figure 5, the framework was populated with three case studies during the study.

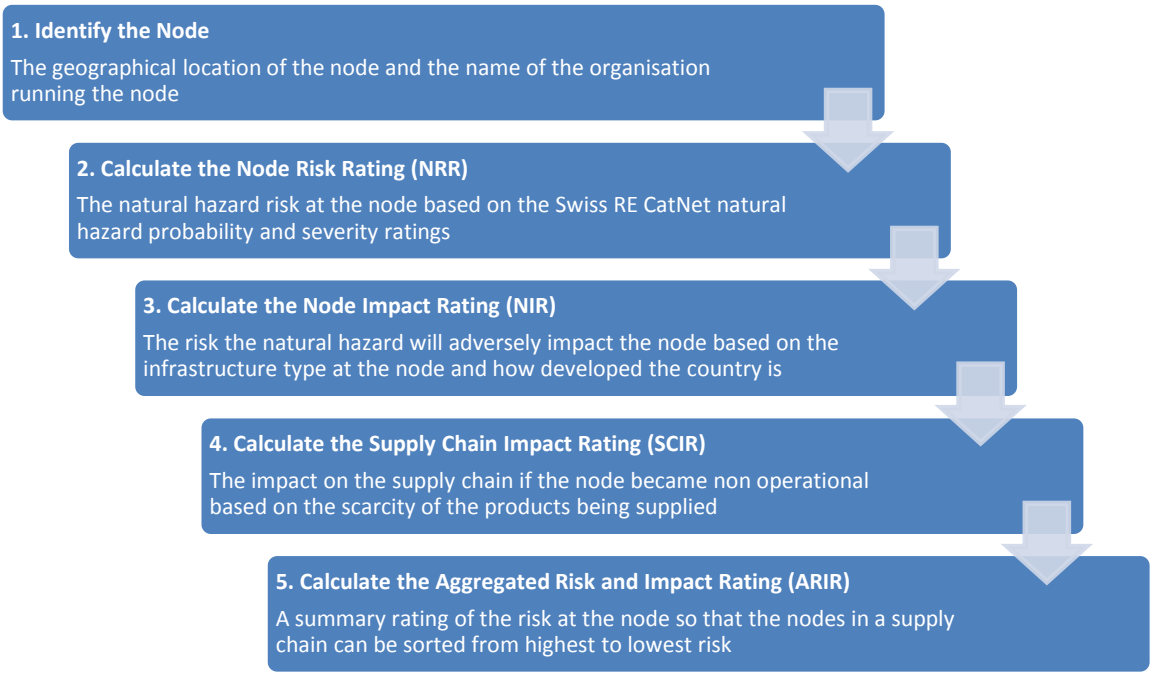


**Figure 5 – Five step Vulnerability Assessment Framework process**

# 6 Case Studies

During the study the Vulnerability Assessment Framework was populated with three case studies from industry. Data was collected from the BAE Systems Munitions, BAE Systems Maritime and Morgan Composites & Defence Systems supply chains down to tier 3. For example tier 1 is BAE Systems, tier 2 is a supplier to BAE Systems and tier 3 is a supplier to the supplier. Figure 6 shows illustrative data for 25 companies (referred to as supply chain nodes) from the three supply chain tiers in the three case studies.

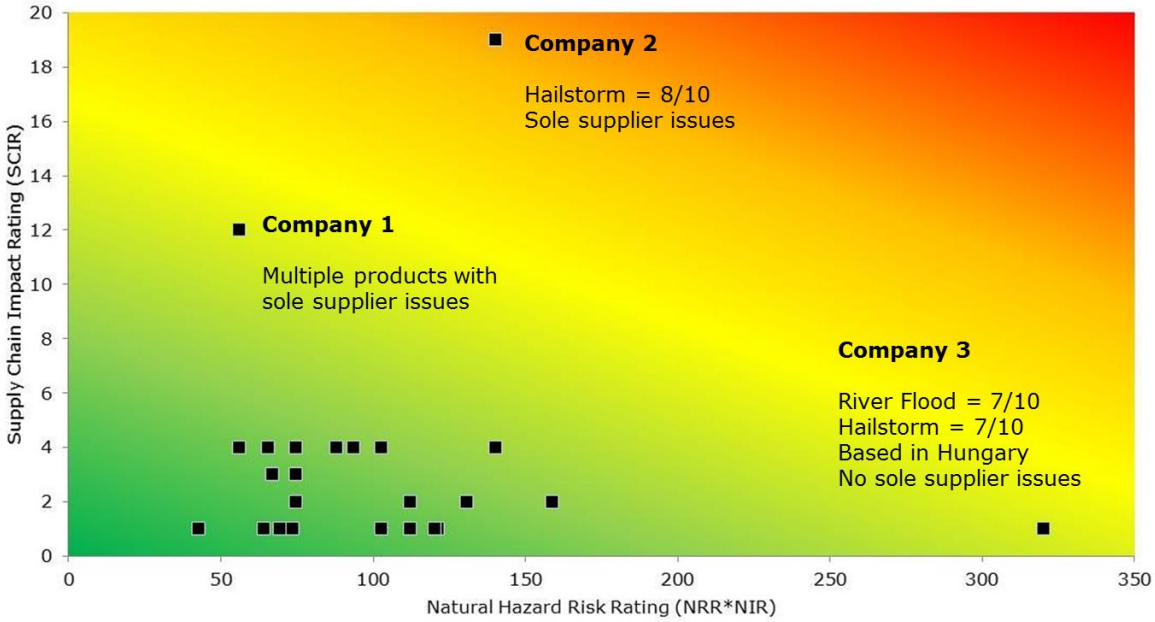


**Figure 6 – Case Study Analysis (Illustrative Data)**

In Figure 6 the Supply Chain Impact Rating (SCIR) on the y-axis is the impact on the supply chain if the node became non-operational based on the scarcity of the products being supplied. The Natural Hazard Risk Rating (NRR*NIR) on the x-axis is measure of the risk and impact of a natural hazard at each node. Some conclusions can be drawn from Figure 6:

1. The majority of the nodes from the three case studies are clustered in the bottom left corner of the graph. This means the natural hazard risk and impact is low and if the node became non-operational it would not have a great effect on the supply chain. Thus no mitigation is required.
2. Company 3 is an example of a node with a very high natural hazard risk and impact due to the river and hailstorm risk, and the location of the node in a developing country. However because the node has a low Supply Chain Impact Rating it would not have a great effect on the supply chain if it became non-operational. Thus no mitigation is required.
3. Further analysis would be required to understand the operational and financial risk to the MOD due to Company 1 and 2 and decide if mitigation is required.

# 7 Pilot Approach

During the study it became clear that if the MOD decided to start assessing the risk in the defence industrial supply chain the method followed in this study would have to be scaled up. This would allow the MOD to automate the data collection from the supply chain and incorporate a number of different measures of supply chain risk.

In order to create a scaled up pilot approach two supply chain mapping companies (NQC[25] and Value Chain[26]) created a software solution which could:

1. **Data Gathering** – Gather data from a supply chain using automated emails containing questionnaires which are sent to suppliers who then forward them on to their suppliers. The data required would include the geographical location of the supplier and the products produced at the site. Specially designed questionnaires could also collect specific information on areas such as natural hazards and cyber security.

2. **Data Storage** – Automatically store the large amount data collected from supply chain questionnaires in a database classified as secret. The database would be based on the Vulnerability Assessment Framework and expanded to be able to handle a number of different risks.

3. **Third Party Data Providers** – Use third party data sources such as Swiss RE's CatNet to automatically check risk ratings at each supply chain node. Other third party data sources could also be used such as Dun & Bradstreet[27] which rates the financial health of a company.

4. **Analysis and Reporting** – Analyse the risk in a supply chain and produce standard maps and reports. This would enable regular supply chain risk assessments to take place. If a disaster were to occur in a part of the world the standard reports could be used to rapidly assess the impact on the MOD.

In order to take this study further the MOD would need to test the pilot approach on an extensive case study for a critical platform. This would allow the pilot approach to be refined further and integrated with other similar projects such as the assessment of cyber risk in the MOD industrial supply chain. There are then two broad options for the implementation of the refined approach across the MOD industrial supply chain:

1. The MOD could set up a team which would assess risk in the wider industrial supply chain and identify high risk suppliers where mitigation may be required.
2. Risk analysis could be pushed out to industry by including the need for regular supply chain risk assessment in defence equipment contracts.

However for either option to be successful the MOD would need to work to create a collaborative environment with industry so that the benefits of risk assessment are understood across the industrial supply chain and buy-in is developed.

[25] NQC, http://www.scc.com/our-isv-programme/isvs/nqc/
[26] Value Chain, http://valuechain.com/
[27] Dun & Bradstreet, http://www.dnb.co.uk/

# 8 Conclusions

Recent catastrophic weather events such as Hurricane Katrina in 2005 and the 2011 Tohoku earthquake & tsunami resulted in severe disruption to global supply chains. This study has been conducted to assess the wider resilience of the UK Ministry of Defence (MOD) industrial supply chain. The focus of the study was supply chain resilience to natural hazards and an approach has been developed for the identification, analysis and mitigation of natural hazard risk. This approach can also be also used to analyse other supply chain risks such political unrest, material scarcity and cyber espionage.

The study indicates that the risk in the MOD industrial supply chain needs to be more proactively managed for the following reasons:

1. **Risk is Evident**
   Historical examples illustrate that natural hazards have disrupted supply chains which has impacted government defence agencies both financially and operationally. These examples include the flooding of both BAE Systems, Johnson City and the Atomic Weapon Establishment, Burghfield, and hurricane damage at Homestead Air Force Base, Florida. Historical examples also indicate that defence supply chains are vulnerable to Chinese counterfeit goods, labour strikes and cyber espionage. A RAND report illustrates that the US Air Force is concerned about risks in the industrial supply chain[28].

   Case studies were carried out and supply chain data was collected from three of the MOD's suppliers; BAE Systems Munitions, BAE Systems Maritime and Morgan Composites & Defence Systems. This data indicated that there may be vulnerable nodes in the MOD's industrial supply chain which could be at risk from natural hazards and if compromised could impact the MOD both financially and operationally.

2. **Risk is likely to Increase**
   Supply chain risk is likely to increase in the future due to global warming, increasing global inequality, resource scarcity, growth of organised crime, reduced inventory holdings by MOD and industry, and the drive to find the lowest cost supplier anywhere in the world.

3. **An Approach is Available**
   A pilot approach for the identification, analysis and mitigation of natural hazard risk in the MOD industrial supply chain has been developed. This relies on relatively inexpensive commercial software which can be used to consolidate natural hazard data and collect data from the supply chain via questionnaires. This approach can also be also used to analyse other supply chain risks such political unrest, material scarcity and cyber espionage.

For these reasons mapping and analysing risk in the MOD's industrial supply chain is achievable and extremely important.

[28] RAND, Identifying and managing air force sustainment supply chain risks, Nancy Y. Moore, Elvira N. Loredo, 2015, http://www.rand.org/pubs/documented_briefings/DB649.html

**This page is intentionally blank**


CORDA
Delivering Successful Futures