

**FORESEC Deliverable D 4.4
Taxonomy on Trends, Drivers,
Threats**

30 April 2009

**Principal authors: Bastian Giegerich, IISS
Reviewed by: CMI**

**CRISIS
MANAGEMENT
INITIATIVE**
Building Bridges for Sustainable Security



systems research
AUSTRIAN RESEARCH CENTERS



Contents

1. Introduction	3
2. Methodology	4
3. Discussion of selected works	6
a. UK Cabinet Office: National Risk Register	6
b. World Economic Forum: Global Risks 2009	8
c. Input from FORESEC work packages	11
d. Comparison	12
4. FORESEC Taxonomy	13

Introduction

Work Package 4 (WP4) is build around the on-line Delphi which involved a broad spectrum of experts and stakeholders from across the EU. This taxonomy paper provides an analytical framework for the next stage of the project.

The Delphi will in part define the universe of trends, drivers, and threats that need to be taken into account in the remaining steps of WP 4. To enable detailed analysis of the Delphi data and an assessment of security challenges and their drivers beyond the statistical analysis and presentation of this data provided by Deliverables 4.2 and 4.3, an analytical framework is needed. The taxonomy on trends, drivers and threats (Deliverable 4.4) will provide such an analytical grid, which is necessary to establish what kind of developments represent high priority issues, in other words to identify those issues that have a high likelihood of occurring and a high impact on European security if they occur. On the basis of Work Packages 2 and 3 and earlier steps in WP 4, the IISS has developed a framework that will enable members of the consortium to analyse, evaluate and summarise the information gathered in the foresight process. In the structure of WP 4, the development of this framework is separated from the application of the analytical grid. The second step will lead to a Report on European Security (Deliverable 4.5). The resulting assessment will be used as input for the scenario work in Work Package 5.

1. Methodology

The taxonomy presented in section four is the result of a multistep process the IISS engaged in between November 2008 and early March 2009. First, the IISS drafted a discussion paper on Deliverable 4.4 which was shared with the FORESEC project coordinator CMI. Initial ideas for the taxonomy were then presented and discussed with the European Commission at the FORESEC mid-term review meeting in Brussels. Based on these steps, a revised discussion paper was shared among all FORESEC consortium partners for comment. The reactions of the consortium members were discussed in depth at a FORESEC management committee meeting. As suggested by the European Commission, the IISS also organised a discussion meeting with a group of FORESEC stakeholders in London. Participants from a variety of backgrounds were asked to provide feedback on the ideas developed by the IISS and specifically whether the suggested analytical dimensions (see below) were appropriate and struck a desirable balance between complexity and feasibility for the purposes of FORESEC and in light of the available data. Throughout the whole process, the IISS team consulted pertinent documents and reports to gain an in-depth understanding of the methodologies and approaches used by different actors. A discussion of selected reports is presented in the next section.

A significant challenge is the complexity of the analytical task at hand. The taxonomy needs to do more than simply classify trends, drivers, and threats in some hierarchical structure. For example, it will not be enough to indicate that a certain trend may cause or is associated with a number of threats. During the initial stages and discussion, the IISS suggested that for the taxonomy to serve as an analytical grid, it needs to speak to the following points:

- Likelihood;
- Severity of impact;
- Sources (i.e. man-made or not);
- Level of impact (EU, national, human security);
- Sector of origin (for example 'environmental' or 'economic');

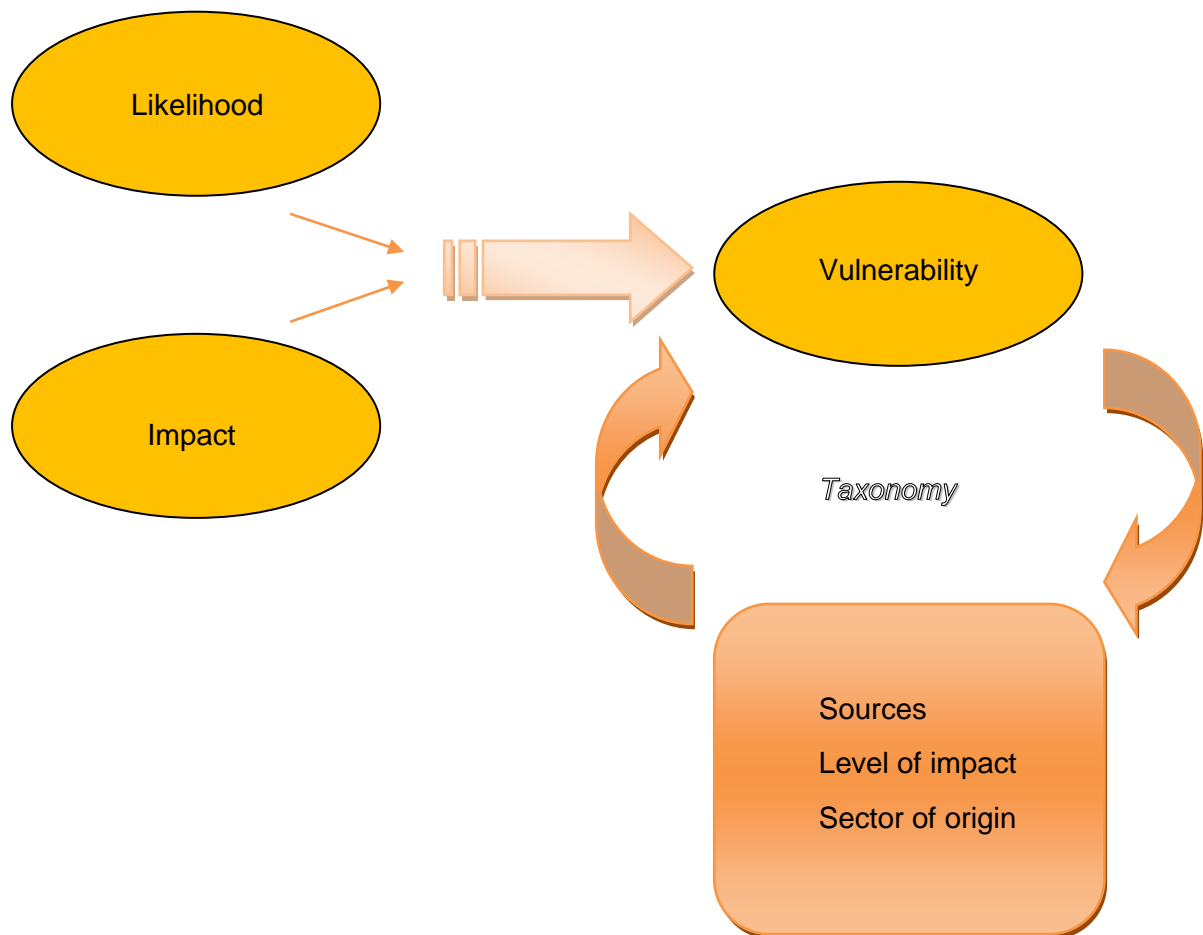
Removed

- *Sector of impact (to mirror sector of origin)*
- *Response (for example 'prevention' or 'mitigation')*

Ideally, these factors would be clustered in the analysis to be conducted in D 4.5. Discussions among the consortium members and with stakeholders generated strong support for an approach that focuses on the key dimensions of likelihood and impact as a measure of vulnerability. Both of these dimensions were included in the Delphi. Remaining factors would serve as additional, second-order filters for the taxonomy as such and could be applied to the resulting picture of vulnerability to generate greater levels of information. However, further debate, including with FORESEC stakeholders, led to the elimination of the following dimensions on grounds of feasibility (data availability, reducing flexibility for policy-makers): 'sector of impact' and 'response'.

Documents like the FORESEC country reports and the ESRIF Working Group 5 state of the art scan already provide useful classifications of threats based on a variety of primary sources. However, the limitation is that these reports very rarely go beyond grouping several threats under different headings thus only establishing a taxonomy in the strict sense of the term. From such taxonomies, however, it is not possible to directly develop priorities, an implicit task for D 4.4. This is not a matter of comprehensiveness or lack of detail but rather a result of the fact that the tool of taxonomies is used in its traditional sense of providing a classification. They are thus ordering devices and useful starting points but do not amount to kind of analytical framework needed for D 4.5. Therefore the IISS team decided to adopt a more expansive definition for D 4.4 than the term ‘taxonomy’ would suggest and interpret the key task as designing a framework that can create a hierarchy of trends, drivers and threats based on European vulnerability to them.

Figure 1: Analytical Framework



2. Review of selected works

This section discusses a selected number of reports from a variety of sources – including input from earlier FORESEC work packages – that proved helpful in devising the FORESEC taxonomy. The aim is not to present a state of the art scan but to discuss and showcase examples of government and non-governmental work of high relevance to the task at hand.

a. UK Cabinet Office: National Risk Register

In 2008 the British government published for the first time a National Risk Register (NRR) which “provides an assessment of the most significant emergencies which the United Kingdom and its citizens could face over the next five years summarised into three categories: accidents, natural events (collectively known as hazards) and malicious attacks (known as threats).”¹ The NRR is based on a cross-governmental national risk assessment which remains classified. It assesses both the likelihood and impact of the risks (both threats and hazards) in order to enable prioritization of the UK’s emergency planning efforts. Priority is given to risks that are relatively likely to occur *and* could have a major impact. The NRR includes only risks that would warrant a central government response, thus what is referred to as “high consequence risks”.² The assessment is relative meaning it compares the two dimensions of likelihood and impact of risks in relation to other risks. The risk assessment process is build on three steps: risk identification, risk assessment (likelihood and impact), and risk comparison. Throughout the process the opinions of government experts, historical, statistical and scientific data are used. The impact of a risk is gauged by a range of effects caused if the risk were to occur: number of fatalities; human illness or injury; social disruption; and economic damage.³ The NRR does not cover risks like climate change or resource competition (as their effects would not be felt within the five year time frame) or street crime (because they do not amount to emergencies warranting central government response).

¹ Cabinet Office (2008): National Risk Register, p. 3, http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/national_risk_register/national_risk_register.pdf .

² Ibid p. 4.

³ See: Ibid pp. 43-44.

The NRR offers the following taxonomy of risks:⁴

1. Natural Events

- 1.1 Severe weather
 - 1.1.1 Storms and gales
 - 1.1.2 Low temperatures and heavy snow
 - 1.1.3 Heat waves
 - 1.1.4 Drought
- 1.2 Flooding
 - 1.2.1 Coastal flooding
 - 1.2.2 Inland flooding
- 1.3 Human disease
 - 1.3.1 Pandemic influenza
 - 1.3.2 New and emerging infectious diseases (e.g. SARS)
- 1.4 Animal disease
 - 1.4.1 Non-zoonotic notifiable (e.g. Foot and Mouth disease)
 - 1.4.2 Zoonotic notifiable (e.g. Avian influenza H5N1)

2. Major accidents

- 2.1 Major industrial accidents
 - 2.1.1 Fires
 - 2.1.2 Contamination
 - 2.1.3 Technical failure (e.g. nationwide loss of electricity)
- 2.2 Major transport accidents
 - 2.2.1 Air
 - 2.2.2 Maritime
 - 2.2.3 Road and Rail

3. Malicious attacks

- 2.1 Terrorist attacks on crowded places
- 2.2 Terrorist attacks on critical infrastructure
- 2.3 Terrorist attacks on transport systems
 - 2.3.1 Rail and underground
 - 2.3.2 Air
 - 2.3.3 Maritime
- 2.4 Non-conventional attacks (involving CBRN materials)
- 2.5 Electronic attacks

All of the risks included in this taxonomy are judged to be high consequence risks. The five risks assessed to have the highest relative impact are:

1. Pandemic influenza;
2. Coastal flooding;
3. Major industrial accidents;
4. Inland flooding;
5. Terrorist attacks on crowded places.

The five risks assessed to have the highest relative likelihood of occurring are:

1. Terrorist attacks on transport systems;

⁴ Ibid pp. 8-30.

-
2. Electronic attacks;
 3. Terrorist attacks on crowded places;
 4. Severe weather
 5. Pandemic influenza.

b. World Economic Forum: Global Risks 2009

The World Economic Forum (WEF) organizes a Global Risk Forum through which the WEF, in conjunction with Citigroup, Marsh & McLennan Companies, Swiss Re, Wharton School University of Pennsylvania, and Zurich Financial Services produces a Global Risks report. The most recent version was published in January 2009.⁵ Given the composition of the Global Risk Forum it is not surprising that the report is focussed heavily on economic aspects and is driven by a corporate and business lens. The report assesses 36 risks on the dimensions likelihood and severity. The methodology for assessing likelihood involves a mix of quantitative and qualitative instruments including expert opinion. Likelihood is expressed in percentages in the following steps: below 1%; 1-5%; 5-10%; 10-20%; above 20%. Severity is analysed according to two factors: economic damage (in USD bn) and fatalities (number of deaths). Risks are evaluated over a 10 year timescale and their likelihood and severity is compared to previous assessments, i.e. the Global Risks 2008 report. Unlike in the UK NRR, risks that will unfold over a longer period, such as climate change, are included. Global risks have been defined according to a number of criteria:

- Scope: only risks that were assessed to potentially affect at least three world regions on at least two different continents were included;
- Cross industry relevance: for a risk to be included it would need to affect at least three or more industries;
- Uncertainty;
- Economic impact: only risks that have the potential to cause around USD 10bn were included;
- Public impact: only risks that have the potential to cause major human suffering and a global policy response were included;
- Multi-stakeholder response: only risks that require a multi-stakeholder response for successful mitigation were included.

⁵ http://www.weforum.org/pdf/globalrisk/globalrisks09/global_risks_2009.pdf .

The taxonomy used in the Global Risks 2009 report uses a sector approach:

1. Economic

- 1.1 Food price volatility
- 1.2 Oil and gas price spike
- 1.3 Major fall in USD
- 1.4 Slowing Chinese economy
- 1.5 Fiscal crisis
- 1.6 Asset price collapse
- 1.7 Retrenchment from globalization (developed economies)
- 1.8 Retrenchment from globalization (emerging economies)
- 1.9 Regulation cost
- 1.10 Underinvestment in infrastructure

2. Geopolitical

- 2.1 International terrorism
- 2.2 Collapse of the Non-proliferation Treaty
- 2.3 US/Iran conflict
- 2.4 US/DPRK conflict
- 2.5 Afghanistan instability
- 2.6 Transnational crime and corruption
- 2.7 Israel-Palestine conflict
- 2.8 Violence in Iraq
- 2.9 Global governance gaps

3. Environmental

- 3.1 Extreme climate change related weather
- 3.2 Droughts and desertification
- 3.3 Loss of freshwater
- 3.4 Cyclone
- 3.5 Earthquake
- 3.6 Inland flooding
- 3.7 Coastal flooding
- 3.8 Air pollution
- 3.9 Biodiversity loss

4. Societal

- 4.1 Pandemic
- 4.2 Infectious disease
- 4.3 Chronic disease
- 4.4 Liability regimes
- 4.5 Migration

5. Technological

- 5.1 Critical information infrastructure breakdown
- 5.2 Emergence of nanotechnology risks
- 5.3 Data fraud/loss

Given that severity is expressed according to two different factors which are not combined in the analysis (economic damage and number of deaths), two separate landscapes emerge. The first assessment with plots likelihood with severity by economic loss highlights the following five risks as potentially causing the highest economic loss:

-
1. Oil and gas price spike (more than USD 1tr; likelihood 1-5%);
 2. Retrenchment from globalization of developed economies (more than USD 1tr; likelihood 5-10%)
 3. Asset price collapse (more than USD 1tr; likelihood above 20%)
 4. Chronic disease (USD 250bn-1tr; likelihood 10-20%)
 5. Fiscal crisis (USD 250bn-1tr; likelihood 10-20%).

The five most likely risks to occur according to this assessment are:

1. Asset price collapse (likelihood above 20%; more than USD 1tr)
2. Slowing Chinese economy (likelihood above 20%; USD 250bn -1tr)
3. Chronic disease (likelihood 10-20%; USD 250bn – 1tr)
4. Retrenchment from globalization of emerging economies (likelihood 10-20%; USD 50-250bn)
5. Global governance gaps (likelihood 10-20%; USD 250bn-1tr).

If severity is expressed as the number of deaths potentially caused the picture changes. The five most severe risks are:

1. Food price volatility (more than 1m deaths; likelihood 5-10%)
2. Infectious disease (more than 1m deaths; likelihood 1-5%)
3. Pandemic (more than 1m deaths; likelihood 5-10%)
4. Chronic disease (200k-1m deaths; likelihood 10-20%)
5. Earthquake (40-200k deaths; likelihood 1-5%).

The five risks most likely to occur according to these dimensions are:

1. Violence in Iraq (likelihood 10-20%; 40-200k deaths)
2. Afghanistan instability (likelihood 10-20%; 8-40k deaths)
3. Global governance gaps (likelihood 10-20%; 40-200k deaths)
4. Chronic disease (likelihood 10-20%; 200k-1m deaths)
5. Critical information infrastructure breakdown (likelihood 5-10%; 1.6-8k deaths).

c. Input from FORESEC work packages

Previous steps in the FORESEC project, including within WP 4, have generated substantial input in terms of what the consortium and stakeholders considered to be pertinent trends and threats. The Delphi generated assessments on both the degree of uncertainty and the importance of 41 trends, drivers and threats for European security. The FORESEC country reports (D 2.2), the report on global trends and major actors (D 2.3) and the kick-off workshop report (D 3.4) served as input into this Delphi. It is implicitly built on the following taxonomy of trend, drivers and threats:

1. Societal

- 1.1 Global population growth
- 1.2 Urbanisation
- 1.3 Aging populations in Europe
- 1.4 Migration
- 1.5 Brain-drain
- 1.6 Decreasing social cohesion
- 1.7 Decrease of state power
- 1.8 Backlash against 'Western' values
- 1.9 Violent extremism
- 1.10 Loss of privacy
- 1.11 Failure to adapt to the complexity of risks

2. Geopolitical

- 2.1 Power shift away from Europe
- 2.2 Assertive Russia
- 2.3 Rivalry among major and emerging powers
- 2.4 Future of the EU
- 2.5 Fragile states
- 2.6 State failure
- 2.7 CBRN terrorism
- 2.8 De-centralised terrorist actors
- 2.9 Middle East peace process
- 2.10 Nuclear Iran
- 2.11 Arms race in Asia
- 2.12 Regional tensions in Asia
- 2.13 Global competition for resources

3. Environmental

- 3.1 Flooding
- 3.2 Droughts
- 3.3 Melting ice caps (Arctic)
- 3.4 Environmental degradation in EU
- 3.5 Permanent damage to marine ecosystems
- 3.6 Pandemics
- 3.7 Hazardous materials

4. Economic

- 4.1 Prolonged recession
- 4.2 Protectionism
- 4.3 Global income equalities
- 4.4 Energy dependency

- 4.5 Global financial markets
- 4.6 Oil shortage

5. Technological

- 5.1 Critical infrastructure vulnerabilities
- 5.2 Cyber attacks
- 5.3 Emerging biotechnology risks
- 5.4 Data loss/fraud

d. Comparison

	UK NRR 2008	WEF Global Risks 2009	FORESEC Delphi
Taxonomy	<ul style="list-style-type: none"> - 23 risks - 3 types - 3 levels deep 	<ul style="list-style-type: none"> - 36 risks - 5 sectors - 2 levels deep 	<ul style="list-style-type: none"> - 41 trends, drivers, risks - 5 sectors - 2 levels deep
Assessment based on	<ul style="list-style-type: none"> - Relative likelihood - Relative Impact 	<ul style="list-style-type: none"> - Absolute likelihood (%) - Absolute severity (economic loss USD) - Absolute severity (number of deaths) 	<ul style="list-style-type: none"> - Likelihood - Importance
Time horizon	5 years	10 years	2025
Scope	United Kingdom	World	Europe
Selection criteria	<ul style="list-style-type: none"> - Requires central government response - High consequence risks only (likely <i>and</i> high impact) 	<ul style="list-style-type: none"> - only risks that potentially affect at least three world regions on at least two different continents were included; - needs to affect at least three or more industries; - Uncertainty; - potential to cause around USD 10bn were included; - potential to cause major human suffering and a global policy response were included; - requires a multistakeholder response for successful mitigation were included. 	<ul style="list-style-type: none"> - Expert opinion - Impact on European security

3. FORESEC Taxonomy

The parameters of the FORESEC project do in some way determine aspects of the taxonomy. For example, the time-horizon has been fixed to be about 15 years, thus 2025, and is hence more long-term than in the other reference reports discussed above. Furthermore, the scope has to be European thus locating the FORESEC work in between the UK NRR and the WEF Global Risks report. The data generated by the Delphi is a key input into the analysis to be conducted in D 4.5 which will apply the framework developed here.

Likelihood: All three efforts mentioned above seek to assess the likelihood of a certain trend or risk manifesting itself. Whereas the UK NRR does so in relative terms, comparing the likelihood of one risk occurring to those of others, the WEF ascribes percentages. In the FORESEC Delphi participants were asked to assess whether the occurrence of a change factor or effect thereof was 'not probable', 'rather probable', 'very probable' or 'almost certain'. The assessment of likelihood will form one of two dimensions of vulnerability for D 4.5.

Impact: Equally all three studies assess in one form or other the impact a certain development or risk would have if it were to occur, the second dimension to vulnerability. The WEF expresses this measure in economic loss and number of deaths. The UK NRR uses a compound measure of relative impact based on the number of fatalities; human illness or injury; social disruption; and economic damage. However, it does not provide a disaggregated assessment of these elements. In the FORESEC Delphi participants were asked to assess whether a development would be 'not important', 'rather important', 'very important' or 'crucial'.

Thus on the two dimensions of **vulnerability** the WEF uses interval scales whereas the UK NRR and the FORESEC Delphi employ ordinal scales. On the one hand interval scales provide more information, on the other it seems impossible to collect the necessary data to arrive at interval scales for the assessment of trends, drivers, and threats covered in FORESEC. A driver like, for example, 'backlash against Western values' cannot usefully be expressed in such terms. Hence D 4.5 will employ ordinal measures of vulnerability.

Source: Only the UK NRR uses a taxonomy that is based on the point of origin of risks. In applying a threats and hazards approach its first order distinction is between natural events, major accidents and malicious attacks. This type of taxonomy is highly effective but risk specific and does not lend itself to drivers who in themselves might have several sources. For this analytical dimension, D 4.5 will this have to distinguish clearly between risks and trends/drivers.

Level of impact: It would theoretically seem possible to distinguish whether a trend or risk is expected to have an impact on global security, European security, national security, local security, or individual security. However, none of the reports do make such an assessment. In fact, the level of impact is used in all efforts as a filter regarding what kind of developments to include. WEF is explicitly concerned with global risks, the UK NRR with national risks, and the FORESEC Delphi obviously aims at trends and threats with an impact on European security. Furthermore, many trends and risks will cut across these levels and manifest itself on several levels at the same time. Thus level of impact does not seem to be a viable ordering principle for the taxonomy.

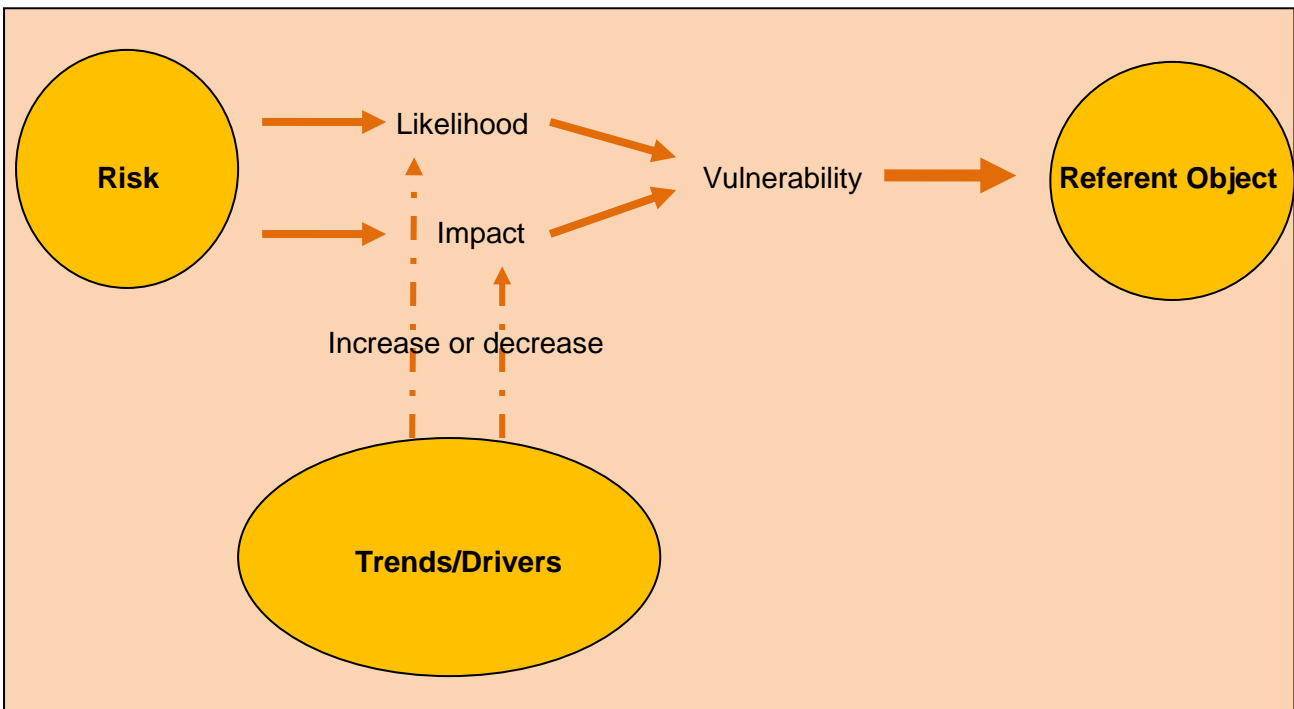
A further level of complexity is added when deploying such a taxonomy for a project aimed at an EU level of analysis and that is the competing pressures from different member state capitals, and

the fluctuating nature of their interests. Differences in perception and prioritization will be the result. To some extent the data generated by the FORESEC Delphi will allow the identification of national and sector differences. While the timescale that this taxonomy takes should help focus on major strategic threats on the horizon, this problem must be borne in mind during analysis if the end product is to prove salient and useful.

Sector of origin: Both the WEF and the FORESEC Delphi use five different sectors in their taxonomies: societal, geopolitical, environmental, economic, and technological. The advantage is that this, unlike the approach of the UK NRR, can be applied to both trends and threats. To ensure compatibility with earlier FORESEC work packages and because of its broad applicability and the data available, this sector approach will be the main ordering principle for the taxonomy.

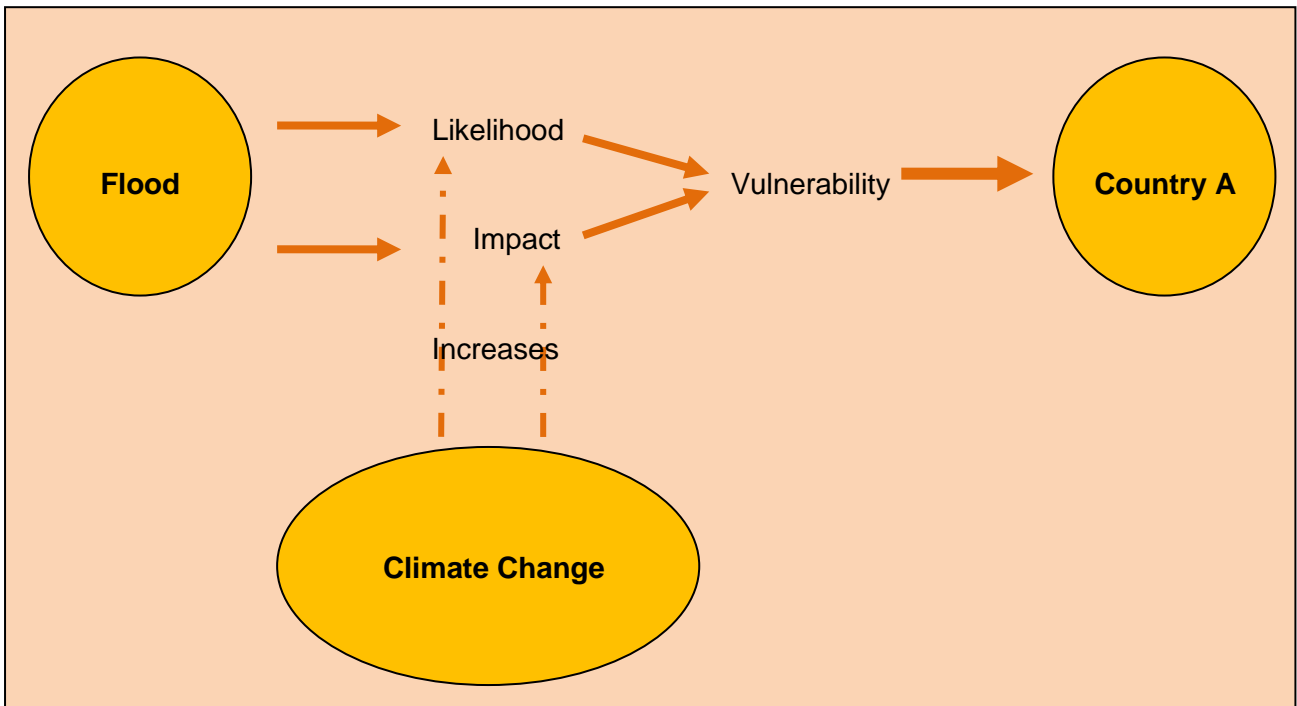
As indicated above, a distinction between risks (threats and hazards) on the one hand and trends/drivers on the other is necessary because the FORESEC project has a broader purpose than risk analysis. Risks, as defined above, are characterised by the fact that the events associated with a certain risk actually unfolding have a direct and observable effect on a certain referent object (such as a country, a society or the EU). Trends and drivers are continuous forces that influence security in a more indirect way and cannot be observed as single or even a series of events. Most importantly, these trends and drivers can: a) increase or decrease the likelihood of a certain risk occurring and b) increase or decrease the impact of a certain risk if it does occur. Thus, trends and drivers affect the vulnerability of the referent object to the risk it is exposed to. This relationship is represented in the following figure:

Relationship between risks and trends/drivers



If this framework is applied to a practical example, the difference becomes easier to understand. For example, the driver 'climate change' might increase the likelihood of floods occurring in 'Country A' as well as the impact of they occur and therefore the vulnerability of 'Country A' to the risk of flooding.

Relationship between flooding and climate change



Taxonomy of trends, drivers, threats

Societal

- Global population growth
 - Urbanisation
 - Aging population in Europe
 - Brain-drain
- Pandemic
 - Pandemic Influenza
- Infectious disease
 - SARS
- Societal fragmentation
 - Violent extremism
 - Backlash against dominant values
- Chronic disease
- Liability regimes
- Migration
- Major accidents
 - Fires
 - Contamination/Air pollution
 - Transport system
 - Air
 - Maritime
 - Road and Rail
- Loss of state power

Geopolitical

- International terrorism
 - Attacks on transport system
 - Rail and underground
 - Air
 - Maritime
 - Attacks on critical infrastructure
 - Attacks on crowded places
 - Attacks with CBRN
 - Cyber terrorism
- WMD Proliferation
 - Collapse of the Non-proliferation Treaty
 - Nuclear Iran
- Interstate conflict
 - US/Iran
 - US/DPRK
- Transnational crime
- Regional conflicts
 - Israel-Palestine conflict
 - Arms race in Asia
- Fragile states
 - Iraq
 - Afghanistan
 - Pakistan
- State failure
- Global governance gaps

- Failure to adapt to complexity
- Global power shift
 - European loss of power/Future of EU
 - Regional rivalries
 - Assertive Russia
- Resource competition
 - Water shortage
 - Oil shortage
 - Food shortage

Economic

- Food price volatility
- Energy dependency
 - Oil and gas price spike
- Major fall in USD
- Prolonged recession
 - Slowing Chinese economy
 - Protectionism
- Fiscal crisis
- Asset price collapse
- Global income inequalities
- Globalization backlash
 - Retrenchment from globalization (developed economies)
 - Retrenchment from globalization (emerging economies)
- Regulation cost
- Underinvestment in infrastructure

Environmental

- Climate change
 - Desertification
 - Land loss
 - Melting ice caps
- Extreme weather
 - Droughts
 - Storms
 - Cyclone
 - Heat waves
 - Low temperatures
- Natural disasters
 - Earthquake
 - Inland flooding
 - Coastal flooding
- Ecosystem damage
 - Biodiversity loss
 - Overfishing

Technological

- Critical infrastructure breakdown
 - Information infrastructure
 - Utilities

Emerging technology risks

Nanotechnology

Biotechnology

Genetics

Data fraud/loss

Cyber attacks