> Resilien-Tech

"Resilience by Design": a strategy for the technology issues of the future

Klaus Thoma (Ed.)

acatech STUDY
April 2014

acatech
NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

Editor:
Prof. Dr. Klaus Thoma
Institutsleiter
Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut, EMI
Eckerstraße 4
79104 Freiburg
klaus.thoma@emi.fraunhofer.de

Series published by:
acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING, 2014

Munich Office
Residenz München
Hofgartenstraße 2
80539 Munich

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

Berlin Office
Unter den Linden 14
10117 Berlin

T +49 (0) 30 / 2 06 30 96 0
F +49 (0) 30 / 2 06 30 96 11

Brussels Office
Rue d'Egmont/Egmontstraat 13
1000 Brüssel
Belgium

T +32 (0) 2 / 2 13 81 80
F +32 (0) 2 / 2 13 81 89

E-mail: info@acatech.de
Web site: www.acatech.de

Coordination: Dr. Anna Frey, Dr. Martina Kohlhuber
Edited by: Linda Treugut, Dr. Anna Frey, Dr. Martina Kohlhuber, Sandra Lehmann
Layout-Concept: acatech
Conversion and typesetting: Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS, Sankt Augustin

> THE acatech STUDY SERIES

This series comprises reports presenting the results of projects carried out by the National Academy of Science and Engineering. The studies are intended to provide informed assessments and future-oriented advice for policy-makers and society.

> CONTENTS

PROJECT

> PROJECT MANAGEMENT

Prof. Dr. Klaus Thoma, Fraunhofer Institute for High-Speed Dynamics – Ernst-Mach-Institut (EMI)/acatech

> PROJECT GROUP

- Peter Andres, Deutsche Lufthansa AG
- Prof. Dr. Claudia Eckert, Fraunhofer Institute for Applied and Integrated Security/acatech
- Alexander Kluge, Deutsche Bahn AG
- KPMG AG Wirtschaftsprüfungsgesellschaft
- Wolfgang Müller-Pietralla, Volkswagen AG
- Prof. Dr. Friedbert Pflüger, European Centre for Energy and Resource Security
- Prof. Dr. Ortwin Renn, University of Stuttgart/acatech
- Prof. Dr.-Ing. Jochen Schiller, Research Forum on Public Safety and Security/Freie Universität Berlin
- Prof. Dr.-Ing. Eckehard Schnieder, Technische Universität Braunschweig/acatech
- Prof. Dr. Klaus Thoma, Fraunhofer Institute for High-Speed Dynamics – Ernst- Mach-Institut (EMI)/acatech

> REVIEWERS

- Prof. Dr.-Ing. Bernd Hillemeier, member of acatech Executive Board (chair of the review panel)
- Prof. Dr.-Ing. habil. Jürgen Beyerer, Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB/acatech
- Prof. Dr. Leonhard Reindl, Department of Microsystems Engineering (IMTEK), University of Freiburg

> ASSIGNMENTS/CONTRIBUTORS

- Dr. Lars Gerhold, Research Forum on Public Safety and Security/Freie Universität Berlin
- Gabriel Bartl, Research Forum on Public Safety and Security/Freie Universität Berlin
- Lucas Daus, KPMG AG WPG
- Burkhard Kesting, KPMG AG WPG
- Timo Kukuk, KPMG AG WPG

> CONSORTIUM MEMBERS/CONTRIBUTORS

- Daniel Hiller, Fraunhofer Institute for High-Speed Dynamics – Ernst-Mach-Institut
- Dr. Tobias Leismann, Fraunhofer Institute for High-Speed Dynamics – Ernst-Mach-Institut
- Benjamin Scharte, Fraunhofer Institute for High-Speed Dynamics – Ernst-Mach-Institut

> PROJECT COORDINATION

- Dr. Anna Frey, acatech
- Dr. Martina Kohlhuber, acatech

> PROJECT PROCESS

07/2012 – 06/2014

> FUNDING

SPONSORED BY THE

Federal Ministry of Education and Research

The project was funded by the Federal Ministry of Education and Research (BMBF) (funding reference 13N12276).

Project administrator: VDI Technology Centre

1 INTRODUCTION

BENJAMIN SCHARTE, DANIEL HILLER, TOBIAS LEISMANN, KLAUS THOMA

On the morning of 7 July 2005, 56 people (including the bombers themselves) were killed in a series of four suicide bombings in London that targeted three underground trains and a double-decker bus. More than 700 commuters on their way to work were injured in the blasts. It was the worst Islamist terror attack ever carried out on UK soil.[1] Nevertheless, by the morning of 8 July, bus services had been resumed and by the end of the day much of the underground network was also up and running again, except for those parts that had been directly affected. Most Londoners had already started using public transport again, in part as a conscious signal to the terrorists that they would not be cowed by them.

Terrorist attacks, natural disasters and major accidents can cause serious, irreversible disruption and changes to the daily lives of large numbers of people. While the greatest impact is felt by those who are directly caught up in catastrophic events of this nature – the dead and the injured, their families, trauma victims, first responders and professional members of the emergency services – they are not the only ones to be affected. In addition to the direct impacts on the groups described above, adverse events can also have numerous indirect negative repercussions. Terrorist attacks can paralyse transport infrastructure, natural disasters can cause huge areas to become uninhabitable and accidents at power plants, for example, can wreak havoc with the energy supply. They can thus seriously impair the ability of society as a whole to function normally and, in the worst-case scenario, can even lead to the failure of the entire system.

The impact of Hurricane Katrina provides a case in point. When it hit New Orleans in late summer 2005, it left the city virtually uninhabitable for several months, provoking the collapse of law and order, medical care, the energy supply, communication systems and a whole host of other important services.[2]

In addition, the annual financial cost of all the natural disasters around the world comes to more than 200 billion US dollars,[3] while the combined financial losses resulting from terrorism, organised crime, accidents and other catastrophic events are even higher. Furthermore, the growing complexity of our modern world combined with parallel long-term change processes such as the declining population in Germany and the threat of global overpopulation will simply serve to accentuate the negative consequences of any future adverse events.[4] In an increasingly interconnected world, even minor and superficially harmless disturbances can ultimately result in severe damage to the system as a whole.

However, none of this necessarily means that individuals, societies and their technological systems must be completely defenceless in the face of these adverse events and powerless to prevent their negative consequences. There are significant differences in the way that different people and different social and technological systems anticipate and react to adverse events. All have the potential to be – or fail to be – "resilient" in response to threats such as terrorism, crime, natural disasters and major accidents.

All of this raises the question of what exactly is meant by "resilience". Over the course of the past 60 years, the term has been adopted by a variety of completely different disciplines, beginning with developmental psychology and going on to include ecology, the social sciences and engineering.[5] This study will focus on the use of the concept of resilience in the context of security research.

Security research aims to identify and analyse vulnerabilities of all types – for example in relation to natural

1 Muir/Cowan 2005.
2 Westrum n.d., p. 1.
3 United Nations Secretary-General's High-level Panel on Global Sustainability 2012, p. 47.
4 Coaffee et al. 2009, pp. 122 – 132.
5 CSS Analysis 2009, p. 1; Flynn 2011; Kaufmann/Blum 2012, p. 237ff; Plodinec 2009, p. 1.

disasters, terrorism, crime or accidents – and develop recommendations and technologies geared towards mitigating or preventing the associated risks without impinging upon people's freedom or civil rights. It involves researching ways of helping to protect against unlawful or deliberately harmful actions targeted at people, infrastructure or organisations. This also includes minimising the damage caused by active attacks or by natural disasters and industrial accidents. Security research also investigates strategies and procedures for rapidly returning the system or infrastructure to normal functioning in the event of a disturbance. The overall long-term goal is to build an infrastructure that isresistant fault-tolerant and robust. Since security research cuts across a wide range of academic disciplines and policy areas, its future development calls for new approaches. In its early days, it was dominated by a "bottom-up", technology-based approach where individual basic technologies were developed separately from each other for security research purposes and were only combined and put to practical use when it came to engineering the final product. Nowadays, however, a "top-down", scenario-based approach centred on threat and hazard scenarios is increasingly coming to the fore. The goal of this more recent approach is to develop systematic, security-relevant global concepts and use risk analyses to minimise the susceptibility and vulnerability of the systems in question.

Against this backdrop, acatech's "Resilien-Tech" project – which provided the basis for this study – aimed to achieve a better understanding of the concept of resilience as applied in the field of security research, so that concrete recommendations could be formulated for decision-makers in government, business and society as a whole. The project partners were acatech – National Academy of Science and Engineering and the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut EMI. acatech is an autonomous, independent, non-profit organisation whose remit is to represent the interests of Germany's technological sciences both at home and abroad. As a working academy, acatech provides up-to-date advice to policymakers and the general public on strategic issues relating to the technological sciences and technology policy. This was also the joint goal of acatech and the Fraunhofer EMI in the Resilien-Tech project. Although the concept is being used more and more in security research theory, no consensus had previously existed in Germany regarding a framework for defining the application of resilience in the field of security. The Resilien-Tech project therefore identified the opportunities and prospects that this approach provides for the development of future scenarios in the areas relevant to the security of our society. In addition, three expert workshops were held on the national perspectives on resilience, international perspectives on resilience and resilient businesses. These expert workshops enabled the full range of themes associated with resilience in the field of civil security research to be comprehensively analysed and investigated. Concrete approaches to developing resilient technological and socioeconomic systems were formulated, with particular emphasis on the protection of critical infrastructure systems. These are encapsulated in the recommendations, which are intended as guidelines for shaping future research strategies and roadmaps. The recommendations are published in the acatech Position Paper "Resilien-Tech – 'Resilience by Design': a strategy for the technology issues of the future".

The term and/or concept of resilience has been used across a variety of different scientific disciplines for at least 60 years. As a result, it is not a straightforward concept to work with when it comes to implementing policy strategies. Nevertheless, the very fact that a wide range of different research areas are interested in resilience suggests that it is a concept with the potential to deliver value-added. American resilience researcher Stephen E. Flynn argues that it provides an "intellectual center of gravity to inform and support a concerted multidisciplinary effort to better understand and manage global and societal risk."[6] The goal of this study was to define the specific

6 Flynn 2011.

meaning that resilience has taken on in the field of security research. In order to do this and to better understand where this definition fits within the overall context, we will begin with a brief outline of the history of resilience as a term and a concept. Our overview will begin in the field of developmental psychology and in particular with the work of American psychologist Emmy Werner. It will subsequently examine the ideas of Canadian ecologist C.S. Holling and US political scientist Aaron Wildavsky, before ultimately arriving at the field of security research. This section will also discuss which level of resilience was focused on in the Resilien-Tech project. It is necessary to clarify from the outset whether the term "resilience" refers to an individual, a group of people, society as a whole or perhaps specific parts of a society such as the relevant technological systems. Moreover, the primary focus of resilience can either be on the social aspects or on predominantly technological solutions. Both the following discussion of the concept's origins and the description of the Resilien-Tech project are key to understanding the specific focus of this study.

The word "resilience" is derived from the Latin verb resilire, which means to spring back. The Duden dictionary of the German language defines resilience as "mental endurance; the capacity to overcome difficult situations without suffering any lasting damage".[7] This definition is indicative of how the term is normally used in the field of psychology (see below). In medicine, resilience is sometimes used to describe a person's resistance to disease – particularly infections –, or their ability to make a swift recovery.[8] Meanwhile, the fields of physics and materials science stick closer to the original Latin meaning, using resilience to refer to a material's ability to deform elastically when acted upon by energy. In this context, resilience is measured as the maximum energy that the material is capable of absorbing per unit volume without creating a permanent deformation (i.e. without deforming plastically or becoming brittle). A good illustration of resilience is provided by the behaviour of springs, which are able to return to their original state even after being subjected to extreme forces. A material's resilience is thus characterised by its elasticity, flexibility and ability to withstand high loads.[9]

The first time that resilience was used as a scientific concept rather than simply as a measurement was in the field of developmental psychology. Indeed, the Duden dictionary still states that the word is used especially in psychology.[10] In this context, it is taken to mean mental endurance or resistance. Even before they started using the term "resilience", trauma researchers in the 1940s and 1950s were already studying how people manage to lead successful lives despite living in difficult circumstances. Their investigations were centred on the idea of emotional strength, i.e. individuals' capacity to overcome misfortune and cope with stress and[11] adversity. The initial studies focused primarily on the specific stress and difficulties experienced by subjects suffering from schizophrenia. The researchers were interested in explaining why the impact of the condition was relatively mild in certain individuals. They found that the people who were best able to cope with their schizophrenia were also those subjects who had already been coping relatively well with their lives before being diagnosed with the condition – i.e. the people who had a job, were married, had good social skills and were able to take responsibility. Subsequent studies of the children of schizophrenic mothers revealed that a surprisingly high proportion grew up to lead successful adult lives. It was clear that certain individual characteristics enabled them to overcome the adverse circumstances experienced during their childhood.[12]

The concept of resilience achieved its breakthrough in the field of developmental psychology during the 1970s thanks

7 DUDEN 2013 (own translation); Plodinec 2009, p. 1.
8 Kaufmann/Blum 2012, p. 237.
9 Kaufmann/Blum 2012, p. 237, Plodinec 2009, p. 1f.
10 DUDEN 2013.
11 DUDEN 2013; Kaufmann/Blum 2012, p. 237; Ungericht/Wiesner 2011, p. 188.
12 Luthar et al. 2000, p. 543f.

to the groundbreaking work of Emmy Werner. Unlike the earlier trauma research studies, she investigated subjects who had experienced a much wider range of adverse circumstances while growing up. Rather than simply looking at their parents' mental illnesses, she considered a whole host of social and economic factors and other influences. In her celebrated longitudinal study "The Children of Kauai", she followed the development of just under 700 children born on the Hawaiian island of Kauai in 1955, assessing and comparing their development at the ages of one, two, ten, 18, 32 and 40. Werner was able to confirm her expectation that the circumstances experienced by a person during their childhood had a significant influence on their individual success later in life. People who had uncomplicated, carefree childhoods had a better chance of leading successful adult lives than those who had grown up in unstable family or financial circumstances or had to contend with other serious problems in their immediate social milieu. More surprisingly, however, she also recorded positive development in a third of the 210 study participants who had grown up in extremely difficult circumstances. These subjects also somehow managed to achieve a regular income, a stable family life and a healthy social environment in their adult lives. In other words, they had shown themselves to be resilient. Werner then turned to the question of why some children were able to develop positively despite growing up in unfavourable circumstances. She sought to detect possible protective factors that may help people build up their resilience to adversity. The protective factors that she identified included personality traits such as healthy self-esteem, the ability to distance oneself emotionally from problems and a lack of inhibition in terms of approaching other people which enabled subjects to find role models outside of their unstable family lives, for example at clubs or other social institutions. In the years following the publication of Werner's seminal work, the concept of resilience continued to be developed in the field of developmental psychology. Whilst strong individuals were described as "invulnerable" in the early studies, "resilient" has now been widely adopted as the term of choice. The word implies positive adaptation by an individual to changed circumstances and, importantly, it eschews a simplistic, black-and-white approach. It encompasses the underlying mechanisms that build resilience with the help of certain factors. The protective factors were expanded to include not only purely internal, individual personality traits but also external factors that enable the development of resilience. It is now customary to distinguish between three different types of factors: a person's innate, genetically determined characteristics, the characteristics of their family and the characteristics of their wider social milieu. Notwithstanding the occasional persistence of theoretical and terminological vagueness and inconsistency, most of the literature continues to argue that resilience has considerable potential to improve our understanding of the development of high-risk groups.[13]

In developmental psychology, resilience thus refers to an individual's ability to cope with and defy adverse circumstances in their lives. Against this backdrop, the work of Canadian ecologist Crawford S. Holling marked a quantum leap in the field of resilience research. In 1973, he published an article entitled "Resilience and Stability of Ecological Systems" in the Annual Review of Ecology and Systematics. As well as extending the application of the resilience concept from developmental psychology to the field of ecology, Holling's article also ushered in a paradigm shift in how people thought about resilience. This was the first time that the term "resilience" had been used to refer not to a specific individual ability but to entire ecosystems. Holling radically challenged the prevailing view of ecosystems as stable entities that exist in a state of equilibrium.[14] This was a fundamental concept of traditional ecology that had been widely accepted for many years. Rooted in classical mechanics and thermodynamics, it stated that after being exposed to an external shock, systems would continuously, steadily and smoothly return to their original state of stable equilibrium. Holling's seminal article strongly disputed this idea of a

13 Kaufmann/Blum 2012, p. 237; Luthar et al. 2000, p. 544; Ungericht/Wiesner 2011, p. 188f.
14 Holling 1973, p. 14ff.

"balance of nature" where, given enough time, a system would always be capable of healing itself.[15] His conclusions were based on observations of the behaviour of real ecosystems such as fish populations in the Great Lakes.[16]

According to Kaufmann/Blum and Walker/Cooper, Holling's 1973 article marked a "complexity turn" in the field of ecology.[17] By identifying a completely different fundamental problem, Holling had shifted the focus of his research. He was no longer primarily concerned with looking for minor deviations from the optimal state of inherent stability. Instead, he believed that in order to fully understand how ecosystems work it is necessary to study highly unstable situations, critical disturbances and major deviations from what had hitherto been perceived as a state of stable equilibrium. Ultimately, what Holling was interested in was the system's ability to survive adverse events.[18] This is why he also drew a fundamental distinction between an ecological system's stability and its resilience. He believed that both properties – stability and resilience – represent possible responses of an ecosystem to external disturbances:

> *"The behavior of ecological systems could well be defined by two distinct properties: resilience and stability. Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variable and parameters and still persist. In this definition resilience is the property of the system and persistence or probability of extinction is the result. Stability, on the other hand, is the ability of a system to return to an equilibrium state after a temporary disturbance. The more rapidly it returns, and with the least fluctuation, the more stable it is."*[19]

Another factor that sets Holling apart from the work and ideas of Werner and the developmental psychologists relates to the type of disturbances and adverse events for which resilience can exist or be developed. Werner focuses on the extremely difficult circumstances that characterise people's lives, i.e. constant, long-term conditions that resilient individuals are able to process and come to terms with. Although she does not completely exclude events such as the subject suffering a death in the family, falling seriously ill themselves or other short-term changes of this type, she does believe that they are secondary compared to difficult circumstances of a more general nature. Holling, on the other hand, turns this approach completely on its head. He is not interested in predictable, known shocks or long-term disturbances which in his opinion belong to the antiquated concept of a balance of nature.[20] Instead, he wants to discover how ecosystems are able to win the evolution "game", where the only prize for the winners is "to stay in the game".[21] According to Holling, the main threat to an ecosystem's ability to survive comes from abrupt, radical and irreversible changes triggered by unusual, unanticipated and surprising events.[22] In non-resilient systems conceived only with stability in mind, the deterministic features that previously enabled an equilibrium to be maintained prevent the system from responding flexibly to such events, causing it to collapse.[23]

15 Holling 1973, p. 1f; Kaufmann/Blum 2012, p. 238; Walker/Cooper 2011, p. 145ff.
16 Holling 1973, p. 6ff.
17 Kaufmann/Blum 2012, p. 238; Walker/Cooper 2011, p. 145.
18 Holling 1973, p. 14ff; Kaufmann/Blum 2012, p. 238f; Walker/Cooper 2011, p. 145ff.
19 Holling 1973, p. 17.
20 Holling 1973, p. 21.
21 ibid., p. 18.
22 Holling 1973, p. 21; Kaufmann/Blum 2012, p. 239.
23 Holling 1973, p. 21.

> *"A management approach based on resilience, on the other hand, would emphasize the need to keep options open, the need to view events in a regional rather than a local context, and the need to emphasize heterogeneity. Flowing from this would be not the presumption of sufficient knowledge, but the recognition of our ignorance; not the assumption that future events are expected, but that they will be unexpected. The resilience framework can accommodate this shift of perspective, for it does not require a precise capacity to predict the future, but only a qualitative capacity to devise systems that can absorb and accommodate future events in whatever unexpected form they may take."*[24]

Without Holling's work, the subsequent transfer of the concept of resilience to what is today broadly referred to as security research (see above) could never have happened.[25] Several ideas that play an important role in the context of security were already present in Holling's seminal 1973 article. These include the emphasis on flexibility as a key property of resilient systems, the focus on serious adverse events that are both unanticipated and abrupt, the adoption of a wider perspective that goes beyond the purely local context and the importance of heterogeneity to resilience. Holling's work also led to the idea of resilience being taken up by a variety of different, frequently interdisciplinary research fields. One example is the field of information science, where resilience describes the ability to tolerate errors and deviations, thus constituting one of the key traits of the Internet, alongside its global and decentralised nature.[26] Further examples include its association with the technological sciences, ecology and behavioural science, as well as the use of the term in geography, especially at the interfaces between individual fields such as ecosystems and political structures.[27] It was the 1980s before resilience finally came to be used in connection with disasters, primarily by engineers in the context of technical infrastructure. They used resilience to describe the capacity to cope successfully with a disaster.[28] The term was also adopted by the social sciences at around the same time. Today, this dual approach featuring technological sciences on the one hand and social sciences on the other is no longer only a characteristic of security research but also of the study of resilience itself.

It was the US political scientist Aaron Wildavsky who was initially responsible for "translating" the concept of resilience into the language of the social sciences. In his 1988 book "Searching for Safety", Wildavsky embedded the idea of resilience into his holistic vision of society as a whole. His principal interest was in how (technological) innovations come about. This led him to go one step beyond classical theory, just as Holling had done before him in the field of ecology. In Wildavsky's case, this involved challenging classical uncertainty theory, which regarded uncertainty as a problem that is automatically solved by technological and intellectual progress. Wildavsky, on the other hand, sees risk and uncertainty as positive factors, since innovation and social progress would be impossible if people did not take risks and confront uncertainty. In his view, security arises as a result of anticipation and/or resilience:[29]

> *"Anticipation is a mode of control by a central mind; efforts are made to predict and prevent potential dangers before damage is done. [...] Resilience is the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back."*[30]

---

24 ibid.
25 Kaufmann/Blum 2012, p. 240.
26 Gürtler et al. 2010, p. 132.
27 Coaffee et al. 2009, p. 116; Gebhardt et al. 2011, p. 760; Plodinec 2009, p. 1.
28 Plodinec 2009, p. 1.
29 Kaufmann/Blum 2012, p. 240f.
30 Wildavsky 1988, p. 77.

Rather than regarding anticipation and resilience as mutually complementary strategies for attaining security, Wildavsky believes them to be diametrically opposed. He views anticipation as an "uncertainty avoidance strategy". He claims that avoiding uncertainty – for example by refusing to approve potentially beneficial medicines because of concerns about their safety – has the effect of hindering innovation and progress. Since we can never know *a priori* whether a technology will turn out to be beneficial or harmful to society, Wildavsky strongly argues the case for a strategy based on resilience. According to this approach, learning processes based on trial and error enable greater security to be achieved in the long term. Wildavsky understands resilience as a security strategy for finding the best way of organising and implementing a response to harmful events that have already occurred. Resilience is thus a purely reactive phenomenon in this context. According to Wildavsky's definition – which would come to be widely adopted by the research community – anticipation and prevention are only useful as strategies for combatting known, predictable and quantifiable threats. In contrast, a resilient society is able to cope with unanticipated threats, adapting and realigning its processes, organisations and systems in order to minimise its vulnerabilities, eliminate instabilities and successfully overcome unpredictable critical situations.[31]

Wildavsky drew his distinction between anticipation and resilience at a very abstract level. The understanding of resistance, protection and prevention as being diametrically opposed to resilience has been developed significantly in the contemporary debate. Today, resilience is viewed as a general, holistic problem-solving approach geared towards increasing the "general ability of technological and social systems to endure and regenerate".[32] It makes no difference in principle whether the hazards and vulnerabilities in question are known or completely new and unanticipated. A resilient society is capable of acting and reacting in the face of any kind of hazard or vulnerability. Accordingly, prevention and anticipation have now come to be regarded as key components of resilience. This is something that was already hinted at earlier. Resilience does indeed allow instabilities to be eliminated, unpredictable critical situations to be overcome and vulnerabilities to be minimised. In order for this to happen, however, societies must be as well-prepared as possible and must take the appropriate measures to ensure that avoidable adverse events are nipped in the bud. In the contemporary debate, these components of resilience are referred to as prevention and preparedness.

While some academics such as the American disaster experts Kathleen Tierney and Michel Bruneau[33] continue to draw a distinction between anticipation, prevention, protection and resistance on the one hand and resilience on the other[34], a more holistic understanding of the concept has been widely adopted in the field of applied security research. One prominent example is the definition of America's Community and Regional Resilience Institute (CARRI): "Community resilience is the capability to anticipate risk, limit impact, and bounce back rapidly through survival, adaptability, evolution, and growth in the face of turbulent change."[35] Another is the definition produced by the National Academies' Committee on Increasing National Resilience to Hazards and Disasters: "Resilience: The ability to prepare and plan for, absorb, recover from or more successfully adapt to actual or potential adverse events." In this context, a disaster is not necessarily a one-off event and may equally involve long-term changes and their consequences. Its causes may be either man-made or natural (all hazards approach).[36]

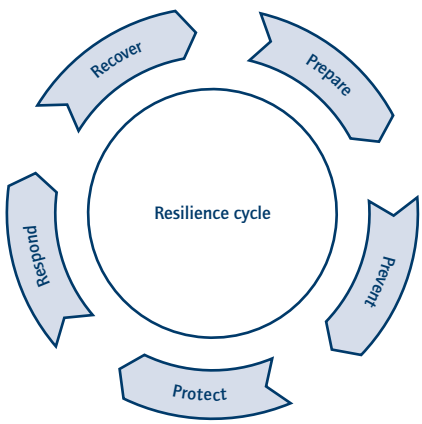
31 Kaufmann/Blum 2012, p. 240ff.
32 CSS Analysis 2009, p. 1
33 Tierney/Bruneau 2007.
34 Kaufmann/Blum 2012, p. 240ff.
35 Plodinec 2009, p. 7.
36 The National Academies 2012, p. 14.

In addition to the United States, the concept of resilience is also firmly established in security research in the UK. Leeds University's Institute for Resilient Infrastructure provides the following definition of resilience: "Resilience is the ability of a system to withstand disruption and continue to function. It is related to durability and performance to expected standards over time."[37] Although the Department for Management and Security at Cranfield University adopts a more detailed definition, it is still based on a holistic understanding of resilience:

> *"It suggests an ability of something or someone to recover and return to normality after confronting an abnormal, alarming and often unexpected threat. It is used alongside security to understand how governments, local authorities and emergency services can best address the threats from terrorism, natural disasters, health pandemics and other disruptive challenges. Resilience embraces the concepts of awareness, detection, communication, reaction (and if possible avoidance) and recovery. It also suggests an ability and willingness to adapt over time to a changing and potentially threatening environment."*[38]

In order to better understand such a wide-ranging concept and depict it in a concrete manner, Charlie Edwards' 2009 publication "Resilient Nation" borrows extensively from classical disaster management cycles.[39] Similarly, this study draws on both Edwards and disaster management cycles in order to develop a simple resilience cycle that provides an easily understood visual depiction of this complex concept (Figure 1). It comprises five resilience phases: "prepare", "prevent", "protect", "respond" and "recover". The first phase (prepare) involves making thorough preparations for disasters, especially in terms of early warning systems. By reducing the underlying risk factors it should be possible to prevent at least some adverse events from occurring in the first place (prevent). When an adverse event does nevertheless occur, the next stage is to ensure that physical and virtual protection systems operate flawlessly in order to minimise the negative impacts (protect). It is also necessary to provide rapid, well-organised and effective disaster relief. This requires the system to maintain its basic functionality as far as possible (respond). Once the actual adverse event is over, it is important that the system should be able to recuperate and learn the relevant lessons from what has happened, in order to be better prepared for future hazards (recover).

Figure 1: The resilience cycle



Source: Edwards 2009, p. 20, author's own illustration.

The resilience cycle was used to help develop the following working definition of resilience for the purposes of this study. This definition in turn provided a basis for the discussions that took place in the workshops:

37 University of Leeds 2013.
38 Cranfield University 2013.
39 Edwards 2009, p. 20; for more on disaster management cycles, see Stangl/Stollenwerk 2011.

"Resilience is the ability to repel, prepare for, take into account, absorb, recover from and adapt ever more successfully to actual or potential adverse events. Those events are either catastrophes or processes of change with catastrophic outcome which can have human, technical or natural causes."

The "Resilien-Tech" project's focus is on the applied aspects of the global concept of resilience, in particular the resilience of critical infrastructure. However, the social aspects are just as important as the technological aspects for creating resilient societies. Resilience can only be achieved by consistently combining technological and societal solutions.[40] Consequently, the two project partners, acatech and the Fraunhofer EMI, focused their research activities on both the technological and social dimensions, as well as on other factors, e.g. economic ones. All of these are key components of resilient societies. The study's focus is not on the theoretical social science discourse with regard to terminological definitions or semantic discussions of the precise meaning of individual elements of the holistic concept of resilience. Although we recognise the fundamental need for a classification of this type, the overview presented in this introduction is sufficient for the purposes of this study. The main body of the study will concentrate on formulating a series of strictly practical recommendations. This is in keeping with acatech's remit to provide advice to policymakers and the general public on key issues relating to the technological sciences, although, in view of the broad spectrum of topics encompassed by resilience, this advice will also extend to a number of wider issues. The findings of the Resilien-Tech project provide a scientific basis for research policy and security strategy decision-making.

This study presents the results of the Resilien-Tech project. In terms of its structure, it begins with an introductory chapter that describes the reasons for carrying out the project, elucidates the origins of the term "resilience" as used in a variety of different disciplines and postulates a working definition. Chapters 2, 3 and 4 go on to present the results of the expert workshops that were held in Berlin during 2013 and were attended by the leading national and international researchers in the field of resilience. Chapter 2 focuses on national approaches to resilience, while Chapter 3 looks at international approaches. Chapter 4 concentrates on resilience within companies and how businesses can contribute to increased overall resilience. Each individual chapter provides detailed definitions of resilience and explores various different aspects of the term. They also outline the ideas of the key research players, present research initiatives in the field of critical infrastructure protection and describe different national policies and strategies for achieving a resilient society. The chapters dealing with the national and international perspectives and with resilient businesses all conclude by identifying future challenges, tasks, research themes, trends and drivers. Finally, Chapter 6 formulates a series of recommendations for political, economic and societal decision-makers that are derived from the outcomes of the expert workshops. The intention is that these should inform future security research and security strategies so that they can help to build tomorrow's resilient society.

The 2005 London bombings demonstrated the value of the systematic incorporation of resilience into planning and implementation actions that is enabled by this approach. In the aftermath of 9/11, resilience had already been adopted by the UK government as a problem-solving strategy for dealing with crisis situations in the United Kingdom. Although the attacks still had a devastating impact, the careful planning and coherent and competent disaster relief provided in the immediate aftermath of the bombings – allied with Londoners' innate resilience – made it possible to prevent serious long-term damage to London, the UK as a whole and the people who live there.

40 Bara/Brönnimann 2011, p. 33; CSS Analysis 2009, p. 1.

2 RESILIENCE: NATIONAL PERSPECTIVES

GABRIEL BARTL, LARS GERHOLD, JOCHEN SCHILLER

2.1 GOALS AND STRUCTURE OF THE WORKSHOP "RESILIENCE – NATIONAL PERSPECTIVES"

As already described in the previous chapter, resilience is well-established within the field of security research in Germany. While the concept was originally adopted and developed mainly in the fields of psychology and ecosystem research, the Federal Ministry of Education and Research security research programme "Security Research – Research for Civil Security" played an important part in elevating resilience to one of the main goals of German security research.

Three different perspectives on resilience were addressed in the research project "Resilien-Tech – Resilience by Design: a strategy for the technology issues of the future". The first expert workshop focused on the national perspective.

It is self-evident that the national perspective does not exist in isolation from the international debate and is every bit as varied and multi-faceted as the field of resilience research itself. Within the overall context of the three "Resilien-Tech" project workshops, the primary goal of the first workshop was therefore to provide an interdisciplinary overview of the current resilience debate in Germany. The key question was what benefits could be delivered by engaging with the subject of resilience and what scientific findings could be harnessed to support policy-level implementation of the resilience concept in the field of national security research. In order to meet the primary objective of exploring the national debate on resilience, a conscious decision was made to employ a largely open workshop format using communicative and participatory workshop methods in order to facilitate an interdisciplinary exchange.

The key themes focused on during the workshop were the importance of critical infrastructures and the role of both policymakers and the public with regard to resilience. In addition to identifying future challenges for national civil security research, the aim was to engage in a detailed discussion not just of the technical aspects but also of the social dimensions, since these form an indispensable part of any holistic approach to resilience. According to Beckmann, resilience is often addressed primarily in terms of technology and infrastructure, a perspective that is far too narrow and sectoral.[41]

The workshop was held in Berlin on 20 and 21 February 2013. The Research Forum on Public Safety and Security (*Forschungsforum Öffentliche Sicherheit*) was responsible for planning and running the workshop and for choosing which experts to invite.[42] The Research Forum sets out to act as an interface between different disciplines and organisations involved in the field of public safety and security. It produces interdisciplinary and cross-discipline reports that provide a basis for formulating recommendations for policymakers and business as well as suggesting possible research topics. The Research Forum's partners include the Forum on the Future of Public Safety and Security (*Zukunftsforum Öffentliche Sicherheit e. V.*), a non-profit organisation that organises meetings held at the German Bundestag between stakeholders from business and the research community, practitioners and policymakers.

The workshop was attended by a total of 27 carefully chosen experts from a broad interdisciplinary spectrum of higher education institutions, research organisations and public authorities. It was chaired by Wolfram Geier, Head of the Directorate of Emergency Preparedness, Critical Infrastructure (CI) and International Affairs at the Federal Office of Civil Protection and Disaster Assistance (BBK).

The workshop was divided into five parts. It began by clarifying the key terminology and discussing the variety of different ways in which it is sometimes used, before moving

41 see Beckmann 2012, p. 5.
42 www.sicherheit-forschung.de [accessed 22. 01. 2014].

on to look at ways of reducing the misunderstandings that could potentially result from different terminological interpretations. After all, it is hardly likely that general terms such as "resilience" will be employed in exactly the same way in an interdisciplinary or cross-discipline context. Considerable emphasis was therefore placed on the joint development of a conceptual framework for resilience.

The five sections of the workshop can be summarised as follows:

1. Keynote addresses

The two keynote addresses provided a starting point for the development of a conceptual framework by presenting two contrasting points of view. Klaus Thoma (Fraunhofer EMI) and Wolf R. Dombrowsky (Steinbeis University Berlin) put the case for the technological science-based and social science-based approaches, although this is by no means to say that a single point of view prevails within either discipline. In fact, the presenters' different stances were largely due to the rationales and goals of their respective research backgrounds. The keynote speakers thus presented two different perspectives that provided participants with a concrete example of the wide range of concepts encompassed by the term "resilience".

2. Clarification of the conceptual framework

In the second part of the workshop, the diverse concepts covered by the term "resilience" were elucidated in greater detail. Guided by the chair, the participants drew up a chart that listed and structured the wide range of concepts and associations connected with resilience on one side and potential conceptual similarities and differences in people's perspective on resilience on the other. What does resilience mean and what are the dimensions that make up resilience as a theoretical construct? Is there a common denominator, do different disciplines share a common understanding of the term? Is the distinction between the technological and social science approaches useful or even necessary?

The discussion of these aspects was aimed at getting the experts to consider their own research field's understanding of resilience from a more abstract perspective, in order to facilitate an interdisciplinary exchange at the meta-level. The first day of the workshop thus laid the groundwork for the second day by providing a basis for understanding the different positions and approaches.

3. Interdisciplinary discussion

The main part of the workshop sought to address resilience from an interdisciplinary perspective. It was divided into three thematic blocks:

a) Critical infrastructure and technological requirements

Key questions: What does resilience mean in relation to critical infrastructure? How can resilient critical infrastructure (as distinct from current infrastructure strategies) be modelled and to what extent is this actually possible? Does the term "resilience" represent a holistic approach? If so, how can human beings and systems be integrated into this approach? What are the key indicators of resilience with regard to specific types of critical infrastructure?

b) Resilient citizens and the role of government

Key questions: What are the roles of the different actors, responsible agencies and communication structures in resilience? What constitutes a "resilient citizen"? How can we strike the optimal balance between government responsibilities and self-organisation by civil society? What form might be taken by possible protection concepts and strategies geared towards increasing the general public's resilience? How could communication between private and public actors be improved?

c) Trends and drivers – future challenges

Key questions: What future challenges and tasks will need to be addressed by safety and security researchers in connection with the concept of resilience? What are

the strategic issues and requirements that will need to be tackled by resilient strategies? How do different theoretical approaches relate to the concept of resilience?

The three thematic blocks thus covered three different aspects of resilience. The first fundamental aspect involved the modelling of resilient systems in connection with critical infrastructure. The second block introduced the social resilience dimension into the debate, together with the importance of two-way communication between government and the general public. Finally, the third block sought to identify future challenges. The discussions were facilitated by Jochen Schiller, Eckehard Schnieder and Carsten Felgentreff using a World Café format where each participant was invited to discuss and develop ideas for all the different themes.

4. Plenary discussion

The subsequent plenary discussion began with the three facilitators presenting a brief overview of the key outputs of their respective thematic blocks. All of the experts who took part in the workshop then had the opportunity to openly discuss the conclusions once more with a view to establishing the main points that should inform both future discussions and an interdisciplinary academic approach to resilience.

5. Overview

The workshop concluded with a brief overview, presented by the chair.

The following sections will describe the outputs of the individual blocks in terms of their themes and the arguments that inform them. An attempt will be made to relate them to the current academic debate on resilience, so that the individual arguments can be situated within the overall context.

2.2 NATIONAL PERSPECTIVES AND DIMENSIONS OF RESILIENCE

As already indicated in the brief outline of the workshop's format, a lot of emphasis was placed during its planning on enabling an in-depth discussion among the participants of the different theoretical approaches to the concept of resilience. This section will begin by describing how the concept of resilience is understood by different disciplines, something that the workshop was able to establish thanks to the wide-ranging research backgrounds of the national experts who took part in it. It will then present the different definitions and dimensions of resilience that formed a key element of the theoretical discussions throughout the entire workshop.

In order to build bridges between the individual disciplines, it is necessary to identify and describe the different ways in which they approach resilience. An understanding of these differences is central to paving the way for a holistic concept of resilience. This requires potential misunderstandings to be highlighted and different theoretical approaches to be clearly distinguished from each other. Without this groundwork, any attempt to develop strategies for coordinating the individual disciplines and formulate recommendations for policymakers will be doomed to failure.

In order to provide a basis for the discussion, the "ResilienTech" project partners produced the working definition of resilience described in the introduction to this study. This working definition characterises resilience as the ability to cope and recover, linking these qualities with the ability to adapt to adverse events. According to this understanding of the term, preparedness and planning are key to dealing with potentially dangerous scenarios as successfully as possible. As such, the working definition fundamentally agrees with the theoretical principles that underpin the resilience cycle, which was also discussed during the workshop (see 2.4.2).

2.2.1 NATIONAL PERSPECTIVES ON RESILIENCE: SELECTION OF EXPERTS AND THE APPROACHES TAKEN BY DIFFERENT DISCIPLINES

The way that the national experts were selected attempted to provide the best possible coverage of the entire spectrum of disciplines encompassed by the concept of resilience. Consequently, they were drawn from both the social sciences (e.g. political science, sociology, human geography) and the technological and engineering sciences (e.g. civil engineering, electrical engineering, IT). While most had a background in higher education, some also worked for government agencies and private companies.

In terms of the basic criteria used in the selection process, experts were invited to participate if they were responsible in some form or other for the design, implementation or control of a solution or if they had privileged access to information about groups of people or decision-making processes.[43] The aim of the workshop was therefore to provide people in senior positions with a platform for discussion that went beyond simply reporting on the current state of research. The use of discursive processes would enable participants to jointly explore their own perspectives and critically appraise opposing views, ultimately generating a new, common body of knowledge on the topic of resilience. Consequently, an explicit decision was taken to adopt an exploratory and open-ended approach to the workshop. It therefore began by looking at the organisational contexts represented by the experts, since the participants would all be influenced by the knowledge base and specific experiences, responsibilities and activities[44] associated with their organisations.

The composition of the expert panel reflected the division of the concept of resilience into the two "meta-fields" of social science-based and technological science-based resilience research. One of the workshop's goals was to identify similarities and differences in the way that resilience is understood and investigate if and how it might be possible to build bridges between the different perspectives. After all, if the concept of resilience is to be successfully leveraged in an interdisciplinary context, it will first be necessary to reach agreement on certain basic theoretical principles, not least because the existing approaches differ significantly in some respects. It was therefore important to describe and discuss the different perspectives on resilience in order to prevent any terminological misunderstandings.

The social science and technological science perspectives

Two fundamentally different perspectives emerged during the workshop. The following description of the characteristics identified by the experts during the workshop as being typical of the social science and technological science approaches to resilience is intended to provide an overview of this issue.

The social science perspective on resilience typically focuses on aspects such as demographic trends, social cohesion, the social repercussions of the growing complexity of global economic structures, etc.[45] Public perceptions also play an important role, for example in terms of analysing hazard mitigation strategies and assessing their potential implications for policymakers, or in terms of addressing the question of whether resilient cities are also safe and secure cities[46] and whether resilience will necessarily always have positive connotations. It is thus crucial to determine whether resilience can be a normative concept[47], since ultimately it is a question of "resilience of what and to what"[48]:

43 see Meuser/Nagel 2002, p. 7.
44 see ibid., p. 74.
45 see Global Risks Report 2013, pp. 21/30.
46 see Floeting 2012.
47 see Ibert 2013.
48 Cutter 2008, p. 603.

Ibert argues that the process of building something together causes us to lose sight of the underlying reasons for building it and the associated blind spots and normative orientations. Whilst this blindness does help to give us confidence in our actions, it in fact creates a false sense of security, since the consequences of those actions can quickly return to haunt those responsible for or in some way involved in them in unexpected ways.[49]

Furthermore, the view taken by the social sciences is that there is always a danger of the rationale for technological solutions becoming self-perpetuating, resulting in a lack of democratic legitimacy with regard to how they operate and what impacts they have. The sociological and political studies perspectives on resilience are supplemented by concepts found mainly in the field of human geography, where greater emphasis is placed on the environmental dimension (e.g. natural disasters).

The technological science perspective, on the other hand, revolves around the issues connected with material properties, hardware, software and programming. The focus is on concepts such as "smart" technology or whether slackness is better than tightness. Considerable emphasis is placed on prevention as a fundamental principle of engineering resilience. The question of how well technological systems are able to adequately represent the real world and whether there is a danger of technocratic aberrations remains unanswered.

The existence of interdependencies and conceptual overlaps between and within the social science, technological science and political facets of resilience is not only possible but is in fact the norm. For example, unintended technological phenomena can affect the social aspects of resilience. Likewise, when cascading effects are triggered within critical infrastructures, the unpredictability of mutual interactions forces us to ask whether the problem would be best tackled using worst-case scenarios, probable/improbable scenarios or some other method. Moreover, social factors such as intuitive risk assessments by the general public can hamper the implementation of technology-based resilience concepts. It is important to bear this in mind when using scenarios to forecast the probability of particular events and the damage they could cause. While scenario-based predictions are in principle a valuable tool, if we are to successfully walk the fine line between the advantages and dangers of using technical risk assessment methods it is nonetheless important to avoid falling into the trap of believing that they can provide us with control over actual events. During the workshop, participants explored the difference between the social science and technological science perspectives by attempting to identify the origins of these two opposite poles of the debate. The first pole is the technological approach to resilience. This is encapsulated in an understanding of the modern world as a world of interconnected data that generate their own interactions. It is then simply a question of controlling these interactions, although this does lead to an unnecessary increase in complexity. As Kaufmann puts it, the aim is not to reduce complexity but rather to develop more complex ways of exercising control.[50] The second pole, meanwhile, involves decisions made by human beings that are often based on gut instinct and are governed by very different rationales or emotions.

In summary, the national perspectives represented by the experts who were invited to participate in the workshop can be divided at the meta-level into social science approaches and technological science approaches, although the dividing line between these two perspectives is blurred and they should ideally be seen as the two opposite ends of a continuum.

Structural and functional preservation

However, it is not just at the interdisciplinary level that different conceptual perspectives exist – they are also found at an intradisciplinary level, where resilience can refer to

49 see Ibert 2013.
50 see Kaufmann 2013.

either the preservation of the system itself or of its functionality.[51] System preservation describes a static, structurally conservative understanding of resilience that is focused on protecting and restoring the system's structures. In this context, structures include both physical structures (e.g. infrastructure) and organisational structures. Functional preservation, on the other hand, is geared towards maintaining functionality. This does not necessarily require existing structures to be protected if other components are able to provide the same functionality. It thus involves a more dynamic approach. This ambivalence in the understanding of resilience finds expression in the two categories of engineering resilience[52] and ecological resilience[53]. Engineering resilience encompasses the principle of prevention, which involves an increase in the physical robustness of infrastructure or the introduction of enhanced monitoring systems. Ecological resilience, on the other hand, places greater emphasis on mechanisms for adapting to future problems and mitigating external shocks.

In this context, Holling speaks of the "two faces of resilience"[54]. While researching ecosystems, he was struck by the problems that characterised interdisciplinary communication between the two ecosystem research sub-disciplines of the biological sciences and the physical sciences:

> *"With the beginning of interdisciplinary efforts between the two fields, some of the fundamental differences between them are generating conflicts caused more by misunderstanding of basic concepts than by any difference in social purposes or methods."*[55]

Returning to the question of how the concept of resilience can be used in the field of security research, the workshop placed great emphasis on finding ways of reducing interdisciplinary conflicts and misunderstandings, an aspect that Holling clearly regarded as fundamental. Accordingly, in order to formulate a holistic concept of resilience for the field of security research encompassing a wide range of different disciplines, it is first necessary to undertake a detailed comparison and analysis of these two different perspectives on resilience. One of the workshop's priorities was therefore to provide people from different disciplines with an understanding of alternative perspectives on the concept of resilience. This is key to the important task of successfully bridging the gap between these different disciplines.

The workshop thus sought to determine where the participants would place their own perspective on the continuum that stretches between the two poles of ecological resilience and engineering resilience, as well as whether it is possible to reach a consensus on the fundamental pillars of a cross-discipline understanding of resilience. One of the main questions was therefore whether resilience can serve as a concept that bridges the gap between different disciplines and research fields, and if so, exactly how would resilience need to be defined in order for it to perform this function.

Holling's early work on ecological systems still treats resilience exclusively as an analytical category[56], i.e. as a static construct for describing ecosystems (system preservation as opposed to functional preservation). However, this approach presupposes that it is possible to effectively control system variability and predict the consequences of system errors. Holling responded to this problem by developing the category of ecological resilience[57].

---

51 see von Gleich et al. 2010.
52 see Pimm 1991.
53 see Holling 2004.
54 Holling 1996, p. 32.
55 ibid., p. 31.
56 see Holling 1973.
57 see Holling 1996.

The distinction between ecological resilience and engineering resilience has a number of profound implications.[58] For example, it raises the question of whether resilience should be understood as an analytical category or a normative concept.[59] The idea of a normative concept involves the formulation of target outcomes, whereas the understanding of resilience as an analytical category focuses in very general terms on reducing the probabilities of occurrence. It therefore lacks the normative connotations that are inherent in all targets, since the process of setting targets always involves negotiations that are shaped by the balance of power between the relevant players. Within the concept of ecological resilience, the mechanism of adapt-ability is key to enabling functional preservation, even with poorer quality individual components.[60] In general terms, the fundamental difference between engineering resilience and ecological resilience therefore lies in how they interpret the meaning of stability.

These two distinct academic interpretations of resilience are broadly reflected in the distinction between the social science and engineering science perspectives.[61] Ecological resilience involves a dynamic approach that actively attempts to cope with threats by focusing on functional preservation. On the other hand, Holling describes engineering resilience as an approach that consciously highlights the preventive aspects of dealing with threats and prioritises structural preservation over functional preservation. This distinction will be explored in more detail under section 2.3, using examples from the discussions in the workshop.

Since a consensus on the fundamental characteristics of resilience will be absolutely indispensable for future research projects, these different interpretations pose a challenge[62] when it comes to developing holistic problem-solving strategies. The Resilien-Tech project aims to address this challenge and ensure that the main aspects that should be included in a German perspective on resilience are communicated to policymakers.

The next section will begin by outlining various definitions of resilience and how they relate to the experts' associations with the term. It will then describe how the conceptual framework was developed during the workshop in order to more precisely define those dimensions of resilience discussed in the relevant literature that would appear to be indispensable for achieving an understanding of the different aspects and problems associated with the concept of resilience. The results of the workshop thus provide the basis for a more detailed analysis of how resilience is understood by different disciplines, while the literature on resilience is enriched through the participants' own personal expertise. This section will once again pay particular attention to the specific challenge of building bridges between different disciplines.

2.2.2 WHO OR WHAT SHOULD BE RESILIENT? WHAT ASSOCIATIONS DO PEOPLE HAVE WITH THE TERM? RESULTS OF THE ASSOCIATIONS MAP

The emphasis of different perspectives on resilience depends on a variety of factors. One fundamental question is who or what should be resilient. The various approaches to resilience differ in their response to this question, with the answer frequently depending on the scientific principles of the relevant discipline. Social scientists thus tend

58 see von Gleich et al. 2010, pp. 13 – 45.

59 The distinction between normative concept and analytical category is frequently used with regard to resilience and vulnerability, resilience being regarded as a normative concept and vulnerability as an analytical category (see. Fichter et al. 2010, p. 224).

60 see ibid., p. 28.

61 see ibid., p. 22.

62 Different perspectives on resilience also exist in the field of development theory. The modernisation theory interpretation is based on the assumption that systems, including social systems, become increasingly resilient thanks to the fact that they are constantly learning from experience. More reflexive approaches, on the other hand, question this cumulative increase in resilience, arguing that in times of change, past experience can, under certain circumstances, lose its relevance as time goes by.

to believe that human beings should be resilient, whilst engineers are more likely to associate the need for resilience with technological systems. Consequently, there is no consensus with regard to what needs to be made resilient. As Dunn Cavelty asks, is it the authorities? The socio-technical systems of our critical infrastructure? Their private and/or public operators? The technologies themselves? The city? The State? Society as a whole?.[63] The way in which these questions are answered can have very different implications for the stakeholders and was therefore one of the issues explored during the workshop. It is therefore important to distinguish between the different entities to which resilience can apply.

Ecological resilience: dynamic functional preservation

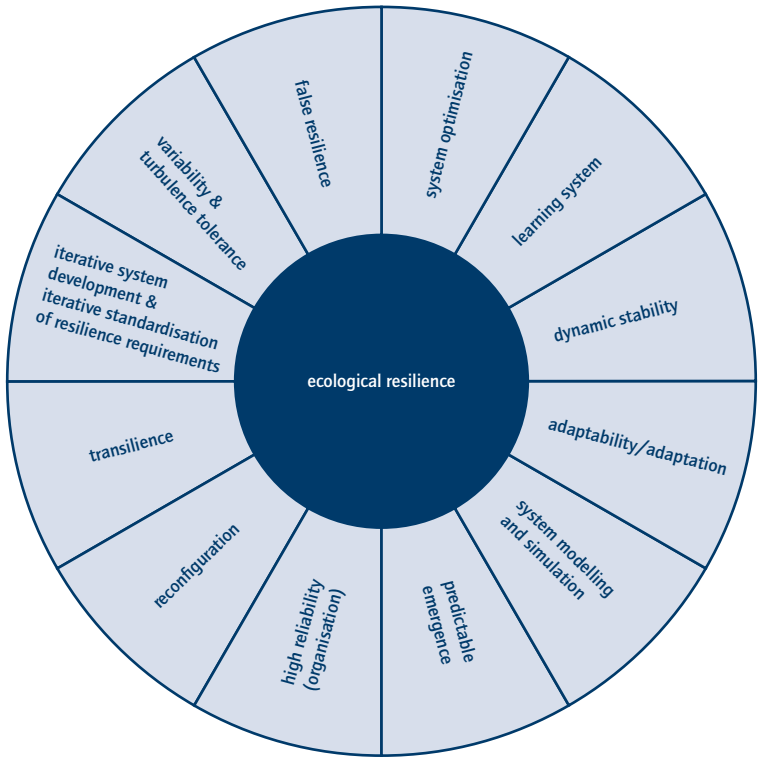
Systems are at the forefront of the perspectives on resilience that were introduced under section 2.2.1: resilience "reflects the capacity (i. e. the underlying mechanisms) of [eco]systems to maintain service in the face of a fluctuating environment and human perturbation".[64] According to this definition, resilience is the capacity to keep providing a service even in a changing environment: "Non-linear factors of influence interact dynamically and (re)produce a complex and multi-stable system that has not just one, but various dynamic states of equilibrium, or so-called steady-state equilibrium".[65] This approach thus involves what might be described as "dynamic stability"[66]. According to the ecological resilience perspective (see Fig. 2), resilient systems are systems that possess the properties of "adaptability" and "adaptation". As "learning systems", they not only incorporate "system modelling and simulation", but also include "reconfiguration" components that allow for the system's goals to be adapted to changing parameters. The underlying mechanism of this approach is to progressively improve the system through "iterative system development" and the "iterative standardisation of resilience requirements". When the experts came up with associations such as "variability" or "transilience" (in the sense of "development", "evolution" and "transformation") it pointed to them having a dynamic understanding of resilience focused on enabling systems to adapt to new requirements. It is the mode of anticipation that ultimately distinguishes this approach from narrower understandings of resilience that do not tend to include anticipation (see 2.3) of risks and hazards on the grounds that the relevant interactions are too complex to predict. According to this approach, however, resilient systems require "predictable emergence", which in this context refers to their ability to anticipate disasters.

The dynamic approach to coping with the challenges arising from future hazards can also be described as the property of "turbulence tolerance" which encapsulates the principle of fault tolerance: how can a technological system's functionality be maintained in the face of faulty inputs caused, for example, by system diversity? In this context, diversity can be tackled through "system optimisation that takes competing system properties into account". The aim is to configure a system's properties and incorporate them into a hierarchy in such a way that they do not block each other. Failure to do this could result in "false resilience", i.e. a form of flawed adaptation to external risks and hazards. In the context of false resilience, "high reliability (organisation)" is also important as a reliability parameter, e.g. in the event of inaccurate measurements. The problems associated with false resilience were subsequently revisited separately by the experts as one of the three priority themes of the World Cafés (see 4.1).

All of the associations with ecological resilience described above can be – and in many cases were – applied to technological systems. It is therefore apparent that the key to developing a holistic concept of resilience is to combine the two "faces of resilience". In other words, both technological systems and society should be resilient. The technological associations that came up in connection with ecological

63 see Dunn Cavelty 2013.
64 Brand 2005, p. 4.
65 Lorenz 2013, p. 8.
66 All the associations identified during the workshop are given in quotation marks and are translations of the original German terms.

Figure 2: Associations with ecological resilience identified by the experts during the "Resilience: National Perspectives" workshop



Source: Research Forum on Public Safety and Security.

resilience are a testament to the forward-thinking attitudes of some of the technology experts who participated in the workshop. They argued that we should think about resilience dynamically rather than advocating the perpetuation of the traditional planning and control approach[67].

Social resilience: participation and democratic negotiation processes

In view of society's nature as a dynamic project characterised by the mechanism of social change, the resilient approach to social systems broadly follows the same principles as ecological resilience: "From a social science perspective, the ecological resilience concept sensu Holling provides a common basis".[68] Nevertheless, in terms of functional units the focus is now on social factors, meaning that the ecological resilience perspective needs to be conceptually adapted to the idea of social resilience and its details modified accordingly. This section will describe the concepts encompassed by social resilience, a topic that was more relevant than ecosystems in the context of this workshop.

According to Adger[69], social resilience is the capacity of social groups or communities to cope with external disturbances and threats that have their origins in social,

67 see Kaufmann 2013.
68 Lorenz 2013, p. 8.
69 see Adger 2000, p. 347.

political and environmental change. This theoretical definition was endorsed during the interdisciplinary discussions (see Fig. 3). One of the associations that the participants in the workshop came up with was the "resilient society", while "cohesion" was identified as a basic mechanism of such a society. In addition, "diversity" was regarded as a key enabler of overall social cohesion, since homogeneous substructures within a society can hamper the cohesion of society as a whole. In this context, "voluntary work" and "bravery and courage" can be understood as examples of resources that help to strengthen social cohesion.

In a world characterised by "unpredictability" and complex interdependencies, another concept with a strong social component that is associated with resilience is "uncertainty competence". This expression was used to describe the ability to accept uncertainty as a fact of life and learn to cope with it. This view is supported by the literature. Dunn Cavelty states that to espouse resilience is to recognise that hazards can no longer be averted using conventional methods and risks can no longer be adequately analysed and minimised. In the age of resilience, there is no longer such a thing as national security – insecurity is the norm and disturbances in the shape of potential disasters are constantly anticipated.[70]

The "specification and selection of acceptance thresholds by society" is key to a society that is able to distance itself from the utopian dream of absolute security. It is essential for acceptance thresholds to be determined through a process of social negotiation in order to enable the establishment of "habitual patterns" – i.e. social routines for coping with uncertainty – that allow people to "feel comfortable" even in uncertain situations. In this context, resilience can be understood as a "factor that allows individuals to survive whilst also preserving the collective". This association can be interpreted as an "enabler" insofar as it constitutes an activation strategy that allows both individual freedom and the engagement of social groups to be planned and facilitated at the organisational level. This understanding of resilience is in some respects therefore similar to Adger's definition that was quoted at the beginning of this section.

It also became apparent during the course of the workshop that a distinction between social and strategic resilience could potentially help to tie down the concept of resilience more precisely. This would involve an understanding of social resilience as the more loosely structured realm of "community resilience", while strategic resilience would refer to the routine- and rule-based actions of the authorities (e.g. the police). However, this approach does result in tensions regarding who is empowered to take decisions in crisis situations – should decisions be taken by centralised administrative structures or decentralised coalitions of citizens at community level?

Overall, social resilience can therefore be regarded as similar to ecological resilience, since it is more concerned with changes of an organisational nature, as well as with the perceptions and culture surrounding security policy. Indeed, it is far from easy to draw a clear line between social and ecological systems – Lorenz, for example, talks of "social-ecological systems"[71], arguing that "[d]isciplinary approaches reach their limits"[72]. This also finds expression in the idea that innovation should be understood not only in technological terms, but also in broader, social terms, in the sense of regulatory frameworks, including stakeholder participation in decision-making or transparency in public communication culture[73]. Resilience thus has a wide range of social implications, some of which also highlight the dangers implicit in this concept. For example, one of the associations mentioned in connection with resilience was "vigilantism". This refers to a situation where the State regards itself as more important than the people and tries to impose a civic culture that supports its own interests.

70 see Dunn Cavelty 2013.
71 Lorenz 2013, p. 7.
72 ibid.
73 see Dunn Cavelty 2013.

Figure 3: Associations with social resilience identified by the experts during the "Resilience: National Perspectives" workshop

Source: Research Forum on Public Safety and Security.

Engineering resilience: strengthening structures

Although a large proportion of the participants' associations with resilience could be categorised under the dynamic concept of ecological resilience, a number of static characteristics were also associated with the term (see Fig. 4). These belong under the concept of engineering resilience and more or less reflect the following understanding of resilience:

> *"Resilience is the ability of systems to resist against external influences and themselves return to a well-defined state of equilibrium".*[74]

One of the associations most frequently cited by the experts was "robustness". Robustness refers to the "stability" of technological structures and evokes similar connotations to the association of "defiance"[75] or the material property of "elasticity", although this latter term describes a flexible form of robustness. Within this series of associations, "resistance" and "resistance to disruption" can also be seen as system properties that minimise the impact of disruption right from the outset. Unlike the dynamic approach to "system collapse", they are already built into the system design process ("resilience by design").

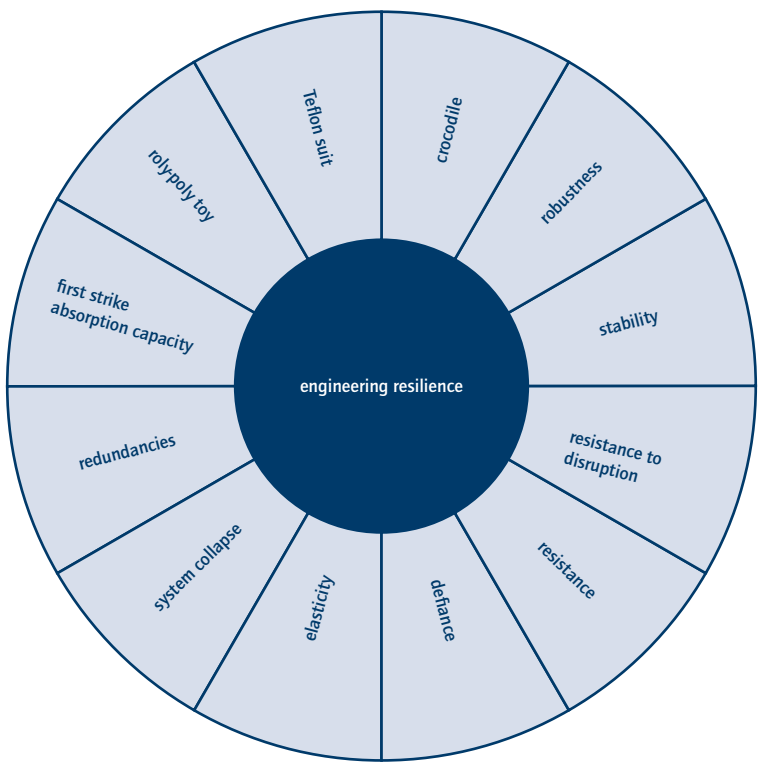
74 Lorenz 2013, p. 8.

75 The association "defiance" (Widerständigkeit in German) describes e.g. the capacity of the public to defy political decisions and should not be confused with the "ability to endure" (Widerstandsfähigkeit in German) of a technological system (the two terms are similar-sounding in German), although both associations do have structurally conservative connotations.

Another element of the engineering-based approach relates to "first strike absorption capacity", which is geared towards keeping a system's structure operational following an external shock. In order to create such a system, it is necessary to build in "redundancies" that could potentially compensate for the failure of different (sub)structures. In general terms, engineering resilience therefore operates according to the principle that a system should be able to return itself to its original state following a disturbance.

It is in this context that the traditional association between the engineering sciences and approaches based on creating stronger structures becomes apparent. However, this does not necessarily have to be the case, as demonstrated by the technology-related associations with ecological resilience. The key feature of the engineering resilience approach is its focus on the possible rather than on the probable. Accordingly, the probabilistic risk approach – based on the formula: probability of occurrence x damage = estimated risk – is replaced by an approach based on the lessons learned from experience. Ultimately, "resilience by design" refers to the

Figure 4: Associations with engineering resilience identified by the experts during the "Resilience: National Perspectives" workshop



Source: Research Forum on Public Safety and Security.

implementation in the engineering design process of what we have learned from experience. One major challenge that was identified in this context was how to integrate social complexity into a technological design process. This issue would go on to be addressed separately later in the workshop (see 3.2).

Metaphorical associations such as "roly-poly toy", "Teflon suit" and "crocodile" provided graphic descriptions of the engineering-based approach in the experts' own words. The clear difference between this approach and the ecological resilience perspective invites further discussion, since this fundamentally conservative interpretation implies a desire to be protected against and immune to any changes in the system's environment. As a result, it generally ignores the capacity of systems to learn and adapt, since this would involve changes to the system[76]. Clearly, an approach that is opposed to change and development must also reject any mechanisms that enable adaptation to new circumstances. However, there is absolutely no question that adaptability is in fact an important property for technological systems that operate in changing environments and should therefore be included in any holistic concept of resilience.

Up to this point, it has been demonstrated that, in general terms, the discussion of the concept of resilience can be approached from a social-ecological or a technological perspective. The attempt to develop an integrated perspective sometimes leads to resilience being understood as the capacity of people, social groups, systems or objects to compensate for damage that has already occurred and restore lost functionality, or the ability to respond flexibly to threats and prevent potential damage from occurring[77]. Although this is a more inclusive and integrated interpretation, it no longer allows for a clear distinction between social and technological systems. However, the associations map produced by the participants in the workshop highlighted a clear difference between these two approaches to the concept of resilience. There is disagreement not only regarding who and what should be resilient, but also with regard to the difference between the concepts of ecological resilience and engineering resilience. The distance that separates these two conceptual approaches was also apparent in the interdisciplinary discussions that took place during the workshop, as outlined in the following section.

2.2.3 THE MODE OF ANTICIPATION AND THE RESILIENCE CYCLE

Although there were many contrasting associations that could easily be assigned to one or other of the ecological resilience and engineering resilience approaches, the participants in the workshop had a far more equivocal attitude when it came to discussing whether or not the mode of anticipation should form part of the concept of resilience. This question of whether the anticipation of future developments and hazards can or should be included under the concept of resilience is crucial for the establishment of an interpretation that bridges the gap between the different disciplines. In order to properly understand this debate, it is necessary to draw a terminological distinction between anticipation and resilience in the narrow sense.

Anticipation and complexity

While, in the narrow sense, resilience means expecting the unexpected[78], anticipation operates on the principle that the future will replicate the past, so that we can prepare for it and prevent catastrophic impacts through timely intervention.[79] Wildavsky[80] regards resilience and

76 see Kolliarakis 2013.
77 see Bürkner 2010, p. 24.
78 see Felgentreff et al. 2012, pp. 70 – 73.
79 see Kreissl 2007, p. 12.
80 see Wildavsky 1993, pp. 305 – 319.

anticipation as two separate modes that are in fact based on different underlying assumptions. The difficult part is to determine whether and how concrete strategies for addressing unforeseen challenges and hazards such as 9/11 and Fukushima can be developed.

The burgeoning interest in resilience can to some extent also be interpreted as a response to an increasingly complex world where it is much more difficult to predict future events. Uncertainty about the relationships within technological systems and about possible future developments is a defining feature of a world characterised by unknown quantities. In the social science context[81], these trends can be described as the "modernisation of modernity". From a technological science perspective, meanwhile, the same phenomenon was described as follows by the workshop participants: "We are connecting more and more systems, increasingly with different half-lives."

In his keynote address, Wolf Dombrowsky also alluded to the problems associated with correctly anticipating future events and processes: "I can recall the first time that the chemists gave a presentation to the German Commission on Civil Protection explaining that autocatalytic processes were occurring in landfill sites which were spontaneously producing substances that we had never even heard of before." According to this view, systems are strictly limited in their ability to adapt to future events. It is true that global trends and problems such as urbanisation, natural disasters and terrorism – which led to the development of the engineering science perspective – can be seen coming and can even be substantiated empirically. However, we cannot predict which concrete challenges and impacts will accompany these changes at individual analytical levels. This is compounded by the fact that, as has already been alluded to, new constellations can develop in previously unknown ways, potentially resulting in risks.

Since this analysis applies to both social and technological systems, resilience should be consistently treated as a "holistic problem-solving approach". Factors such as health (ageing population), the environment (climate change, resource scarcity), communication (cybercrime), energy (desert solar power) and mobility (land, air and sea transport) should not be dealt with separately – resilience should be understood as an all-embracing problem-solving approach that provides a specific response to the problem of mutual interdependence which makes it so hard to predict future events.

However, some aspects of this view are contradicted by theoretical approaches such as the widely used "resilience cycle" model (see next section). These include anticipation as one of the fundamental components of their experience-based, cyclical systems which rely on analysing the past and subsequently optimising processes in order to meet future threats.

The field of security research is thus searching for a strategy that can provide ways of appropriately and satisfactorily coping with future events. In contrast to anticipatory methods that seek to predict the future and develop problem-solving strategies for dealing with expected damage, resilient strategies are, in the narrow sense, geared towards proactively coping with unexpected developments and events, although this approach can still take a variety of different shapes.

The high degree of complexity and global interdependence in today's world is also reflected in the relationship between globalisation and security, insofar as complexity is an attribute that is characteristic of the "new risks". It arises when the boundaries start to disappear between the temporal, physical, spatial and social dimensions[82], meaning that it is no longer possible for responsibilities to be clearly assigned. In this context, Beck talks of organised irresponsibility[83], an organisational problem that comes

81 see Beck/Bonß 2001.
82 see Kaschner 2008, pp. 63–95.
83 see Beck 2007, p. 11.

about as a result of communication failures between individual subsystems. The importance currently being attached to the concept of resilience can thus be seen as a response to the challenges posed by the "new risks". According to Wildavsky[84], complexity and interactions not only limit the value of anticipation but make it completely impossible. Nevertheless, technological approaches can still help us to predict future developments more accurately. There is no reason why we should not make use of scenario-based approaches and simulations, as long as we avoid the trap of believing that the predictions made using these methods are 100 percent accurate. It is, however, important to have the discussion about just how meaningful these approaches are, in order to ensure that we are realistic about the benefits and opportunities that technological solutions can provide.

The resilience cycle

The resilience cycle constitutes an attempt to provide an approximate representation of the time dimension involved in dealing with disasters and other security-relevant events. The number of dimensions in the resilience cycle varies depending on the theoretical perspective adopted. In the workshop, we used a version of Charlie Edwards' resilience cycle that had been adapted by the Fraunhofer Ernst-Mach-Institut (EMI)[85]. This resilience cycle contains five dimensions: "prevent" (avert danger), "protect" (cushion the impact of shocks and disturbances), "respond" (get up and running again), "recover" (adapt, adjust, learn) and "prepare" (be aware of dangers and take them into account) (see Figure 1).

The example of Hurricane Katrina was used to try and demonstrate how the resilience cycle can serve as an analytical tool for investigating major disasters. It is important to remember that our analysis was performed for illustrative purposes only and in no way claimed to be fully comprehensive. Nonetheless, three of the five resilience cycle dimensions received an entirely negative evaluation in connection with the disaster that devastated New Orleans and other parts of Louisiana. Serious failings were identified in the "prepare", "prevent" and "protect" dimensions, pointing to institutional and organisational neglect of both the pre- and post-event arrangements for catastrophic events.

In addition to basic criticism of the excessive use of cyclical models in academic publications[86], the discussions during the workshop also pointed out the problems associated with defining what constitutes the "normal state" that forms the basis of the cycle's structure and operation. Moreover, even if it were possible to come up with a definition of normality, this definition would not remain constant but would instead keep shifting in response to social change processes.

The cyclical model, however, to some extent lacks the ability to adapt to the complexities of social reality, even if the cycle is not chronologically closed. For example, the ability to learn and adapt plays a key role during the "recover" phase. However, the cyclical design of the model does not cater for aspects such as "discussing goals" or "changing goals", even though social negotiation processes should in fact underpin democratically legitimate policy decisions. The challenge of integrating widespread change processes and temporally variable social patterns of interpretation into the resilience cycle was therefore addressed by several of the workshop participants and identified as one of the challenges that will need to be met in order to further develop this approach.

84 see Wildavsky 1993, pp. 305 – 319.

85 Edwards' original cycle is structured somewhat differently and comprises the following phases: "preparedness", "response", "recovery" and "mitigation". The "prepare" dimension was added by the Fraunhofer EMI.

86 see Stoddard 1968.

The workshop also explored ways of drawing attention to the importance of society's "resilience competence" in order to raise public awareness of the likelihood of disasters occurring. The social science and humanities representatives suggested that we need to contemplate a new "culture of uncertainty"[87] in which we learn to cope with uncertainty by accepting that there can be no such thing as absolute safety or security. Uncertainty should therefore be regarded as a positive experience and challenge that forms an inherent part of our lives. Ultimately, this reinterpretation of uncertainty leads to the conclusion that it is necessary to take risks in order to foster innovation. However, this in turn requires risk-aware actors who are able to competently distinguish between different types of risk. The proposed "culture of uncertainty" that was discussed in this context postulates that controlled management of uncertainty is impossible and encourages people to proactively embrace the challenges associated with uncertainty. This allows them to preserve their freedom of action, rather than becoming bogged down in a defensive attitude that severely constrains society's ability to innovate.

The workshop also investigated the extent to which natural disasters on the scale of Hurricane Katrina are likely to occur in Germany and whether the cost of extensive preventive measures would in fact be justified over the long term. The discussion ended up fundamentally questioning the idea of a universal concept of resilience that can be implemented without regard to time and place. Indeed, some participants believed that the only logical approach is to adapt resilient strategies to e.g. the environmental, institutional, political and economic contexts at local, regional and national level. This opinion was also reflected in the association "define the context of the resilience debate" which was identified during the mapping out of the conceptual framework.

2.2.4 RESILIENCE AS THE "NEW SUSTAINABILITY"?

According to the definition included in the proceedings of the UN's Rio+20 conference, resilience is one of the pillars of sustainable development. In this context, sustainability is understood to include the environmental, economic and social dimensions. The seven priority areas for sustainable development are as follows: decent jobs, universal access to sustainable energy, food security, sustainable cities, access to clean drinking water, clean oceans and disaster-resilient societies. Resilience is thus regarded as one of the key components of sustainable development.

It remains unclear whether resilience really is a prerequisite for sustainability or whether the reverse may in fact also be true. Nevertheless, the concept is becoming increasingly important in the context of the sustainability debate. However, it is important to remember that sustainability and resilience are by no means one and the same thing. This was made clear during the workshop, where the conflicting goals of the two concepts were highlighted when one participant argued that the relationship between sustainability and resilience is not as free of conflict as people have tended to suggest in the past. Whilst agreeing with the view that sustainability needs resilience, they pointed out that resilience can require redundancy. In a sustainability debate focused on efficiency and energy flows, this begs the question of who is willing and able to pay for it and how much we are prepared to invest. And not just financially, but also in terms of the development of new types of energy and materials. Are we prepared to do all this just to achieve a small increase in resilience?

Accordingly, in a redundancy-based approach to resilience, the issue of how to pay for the technical solutions and innovations needed to increase resilience could lead to conflicts of interest, especially if we remember that resilience is just one of the seven key components of sustainable

87 For more details on the "culture of uncertainty", see the paper by Wolfgang Bonß in the series published by the Research Forum on Public Safety and Security 2012, pp. 100 – 106.

development. Of course, there are undoubtedly other strategies that quite rightly include resilience as a property of sustainability. It is therefore important to carefully study each individual case in order to ensure that the number of potential conflicts is reduced from the outset.

2.2.5 MEASURING RESILIENCE

Another central aspect addressed during the workshop was the measurement of resilience and the question of which methodologies should be used. How can we measure the resilience of technological systems or indeed entire societies? What are the pros and cons of the different methodological approaches? The workshop's associations map highlighted the problems involved in defining a "damage threshold", establishing an adequate "yardstick" for measuring resilience and the creation of appropriate "indicators". The association that described the need to find "time-based indicators for resilience" emphasised the importance of ensuring that resilience operates dynamically in both space and time.

It must be stressed that the current academic debate on measuring resilience is unable to provide a clear picture of which factors should be included and which should be excluded. The methodologies used to measure resilience are also problematic. How should we measure social cohesion as an indicator of resilience, for example? A whole host of different methodologies for measuring this indicator exist within the social sciences. And, far from being confined to the example of social cohesion, this problem applies equally to the entire spectrum of technical resilience indicators. Furthermore, even once the relevant aspects of resilience have been identified and the appropriate methodologies for measuring them selected, the third question that needs to be addressed concerns the relative weightings of these different aspects. In general terms, it is also important to investigate whether it is better only to use quantitative indicators or whether qualitative indicators may be preferable for certain purposes. If a mixture of quantitative and qualitative indicators is used, this can lead to problems regarding the compatibility of the different indicator categories. It is also necessary to decide whether absolute or relative resilience indicators should be used. With absolute indicators, the problem of how to define 'normality' rears its head once more, while relative indicators run the risk of only existing in a vacuum. However, relative indicators are at least able to record changes. Many people suggested that existing methodologies for measuring vulnerability could also provide a basis for measuring resilience.[88]

The literature often addresses the concept of resilience in the context of vulnerability. However, resilience and vulnerability describe different aspects of systems.[89] Although increased resilience reduces vulnerability, the reverse is not necessarily true: "It could [...] make the system more rigid and thus reduce resilience or it could use up resources that would be better employed for measures geared towards increasing resilience".[90] In some publications, resilience forms part of the methodology used to describe vulnerability, thereby demoting it to one among many sub-categories associated with vulnerability.[91] Consequently, resilience should not be understood as the opposite of vulnerability and by the same token indicators of resilience should not simply be the opposite of vulnerability indicators. Some of the basic methodological ideas for describing vulnerability could nonetheless provide a valuable source of inspiration.

In conclusion, resilience should not be regarded either as the opposite of vulnerability or as synonymous with sustainability. However, there is clearly a tendency for

88 see e.g. Susan Cutter's Social Vulnerability Index which is examined in more detail in the next chapter of this study.
89 see von Gleich et al. 2010, p. 37.
90 see ibid.
91 see ibid.

people to confuse these different concepts with each other. It is therefore incumbent on the relevant academic disciplines to point out their similarities, define their boundaries and pick out the specific properties of resilience. This will be essential both to enable further conceptual analysis and to address the question of how resilience can be implemented in practice.

2.2.6 CAN THE CONCEPT OF RESILIENCE BRIDGE THE GAP BETWEEN DIFFERENT DISCIPLINES?

It is clear from the workshop outputs presented so far that the different perspectives and conceptual approaches diverge significantly on certain points. As a result, it is difficult to find a standard, comprehensive definition of resilience that is sufficiently abstract to incorporate all the fundamental characteristics and properties associated with the concept whilst at the same time preserving its specificity.

However, in order to address the need for holistic solutions to interdependent global problems and threats it is essential that resilience should be used to bridge the gap between different disciplines[92]. The high degree of mutual interdependence between social, technological, economic, political and environmental factors calls for holistic concepts that address these individual factors as part of an overall system rather than treating them in isolation. In this context, resilience can be understood as what was described on the associations map as a "conceptual innovation for a new set of circumstances". This approach would thus be distinct from the narrower perspective of resilience engineering. The approaches of the individual disciplines and the way they see themselves can easily cause the complex interactions between different factors to be overlooked – the different disciplines pay only limited attention to these interactions, thereby inhibiting the potential for interdisciplinary approaches.

The thoughts outlined in this chapter highlight the challenges involved in finding the right degree of abstraction for an interdisciplinary concept of resilience whilst at the same time still ensuring that it provides a distinct definition of where the concept fits into the wider context. Notwithstanding these difficulties, it remains one of the main goals of the Resilien-Tech project to integrate the two concepts of dynamic ecological resilience and predominantly static engineering resilience at a new "meta-level". It is therefore necessary to investigate what the lowest common interdisciplinary denominator between the different approaches might be, as well as which aspects are common to both the technology-based and social science-based perspectives.

Given its exploratory nature, the national workshop made no attempt to come up with a clear and definitive answer to this question. Nevertheless, it was hoped that the outputs from all of the Resilien-Tech project's workshops would, in conjunction with the acatech syndication process, provide some initial ideas for further research in this area and help to identify questions that need further clarification. However, in order to develop a new, integrated concept it is first necessary to identify, analyse and discuss the strengths and weaknesses of current approaches. This is essential if we are to avoid falling into the trap of treating resilience as a panacea. As the associations map pointed out, if we neglect to perform a critical analysis of the different theoretical approaches, there is a danger that resilience could be reduced to nothing more than a "trendy concept" or "buzzword".

The "conceptual framework" developed by the workshop participants has already been described above. It contains some of the fundamental dimensions and conceptual distinctions associated with resilience and indicates where specific perspectives on resilience fit into the overall picture. As such, the conceptual framework can provide guidance in the search for commonalities and the analysis of structural relationships. A holistic concept of resilience does not allow for oversimplified

92 see Kaufmann 2012, pp. 109 – 131.

interpretations focused on one single aspect that claim to be applicable in all contexts. Instead, as has already been emphasised on several occasions, the concept of resilience must be geared towards the context in which it is used. Ultimately, what this means is that even the goal of adopting a holistic approach must be conceived in abstract terms, since this holistic approach only makes sense if it is understood as a flexible and adaptable concept.

2.3 RESILIENCE IN DIFFERENT FIELDS OF APPLICATION

As described in the previous section, resilience should be understood in terms of an integrated approach. Nevertheless, in view of the complex nature of the concept, it was felt that the workshop should take a closer look at some of its sub-themes. Interestingly, however, although the World Cafés were designed to focus on specific themes, the discussions tended to range beyond the confines of their formal topic – something that was also undoubtedly influenced by the interdisciplinary make-up of the participants. The common ground between the discussions in the different World Cafés thus provided compelling evidence of the holistic nature of resilience. The following sections will present the outcomes of the World Cafés.

2.3.1 RESILIENT SOCIETIES AND THE ROLE OF THE STATE

The first of the three World Cafés explored the characteristics of a resilient society and the role of the State. Its aim was to investigate what a society that claims to be resilient should look like and what role the State should play in helping to achieve this goal. Another issue at the heart of this theme was the importance of communication between government and the public and between private and public actors. It became apparent during the course of the World Café that it is necessary to draw an analytical distinction between the individual and collective levels. At the individual level, the discussion revolved around what makes a "resilient citizen", while at the collective level it focused on identifying the characteristics that make an entire society resilient. According to Lorenz[93], there are "three capacities of social systems (adaptive, coping, participative) that constitute resilience", each of which represents a "symbolic dimension of meaning". From a social science perspective, the meaning attributed to these three capacities of adaptation, coping and participation is therefore of fundamental importance. Adaptive behaviour, the ability to cope and participation are resources shared by resilient individuals and social communities. The significance of institutional and political structures and the nature of the relevant communication channels are also key drivers of social resilience. The following section will break down the outputs of the World Cafés based on these different aspects.

Resilient citizens and a resilient society

When discussing the individual-level question of what constitutes a "resilient citizen", it soon became apparent that the concept involves characteristics which at first sight might appear rather unrealistic. For example, resilient citizens would be expected to spend a lot of time at home, always have their emergency kit to hand and be aware of the potential problems that could affect the places where they live, work and spend their leisure time (e.g. an earthquake zone). Moreover, this knowledge would need to be constantly and actively updated with the latest information.

In addition, the features that constitute a resilient citizen would vary from one situation to another, rather than comprising a static concept made up of universal characteristics that always apply, irrespective of time, place and (cultural) context. Finally, when addressing the practical implementation of resilience as a normative concept, it is important not to overlook the influence of cultural context on people's values, attitudes and behaviour.

93 Lorenz 2013, p. 7.

In addition to the contextual influences, any attempt to establish a universal resilience strategy will be further complicated by subjective patterns of perception such as intuitive heuristics[94]. The way that different individuals perceive a threat can differ significantly across the population, meaning that there can also be substantial variations in people's individual preferences regarding the type of resilient strategies that should be implemented for society as a whole. In this context, it is also necessary to ask whether people have such a thing as a "disaster personality", with personality traits that are different to their "normal" personality. If so, it would be necessary to distinguish between human behaviour patterns in normal and crisis situations.

It became apparent during the discussion of the individual and collective analytical levels that the establishment of a resilient society requires social negotiation processes that define the relevant goals. The outcome of these processes should be the creation of a collective strategy that reconciles the diversity of attitudes that make up people's individual (safety and security) preferences. In other words, this is where a society needs to ask itself how it wants to live.

If we understand social resilience as "the capacity to come to terms or cope with unexpected or non-routine events", it becomes clear that it must be grounded in people's everyday reality. In other words, resilience should be something that people experience in their daily routines rather than a one-off response to a particular threat. Moreover, uncertainty and external change should be regarded not as secondary phenomena but as one of the key challenges[95]. To take the example of community resilience, the concept of making resilience relevant to people's everyday experience means e.g. recognising the importance of the local community level as an integrative mechanism for strengthening social solidarity. This ultimately raises the question of how and indeed whether solidarity in the guise of social cohesion can be managed politically (i.e. using a top-down approach) and how social disparities affect the cohesion of different groups at the community level. It is clear from this discussion that political decisions and social factors are inextricably entwined and cannot be analysed separately.

As far as the spatial dimension is concerned, smaller entities (e.g. municipalities) that promote solidarity and have relatively simple organisational structures appear to be better suited to implementing social resilience. This is because they strengthen empowerment and enable an approach that is more precisely targeted to the relevant context. However, this raises the question of whether the State would be willing to promote these decentralised organisational structures by devolving power to them (creating a bottom-up approach). One model for this approach could be provided by the organisational structures that exist in Austria, where there are specific people at regional level who can be contacted in the event of a disaster. Another alternative is the concept of "community resilience", as advocated in the UK context e.g. by Edwards, using the idea of the "Four E's": "Engagement, Education, Empowerment, Encouragement".[96]

The importance of participation

Participation – understood in a wider sense than mere political engagement – is a key resource in the context of social resilience. Edwards uses the term "voluntary effect"[97] to describe voluntary engagement in social affairs. Furthermore, the fact that communication is essential in order for participation to function properly became clear as soon as the discussion turned to the subject of a "culture of constructive dissent". Nevertheless, "Participation can also be challenging if its achievement is understood as a time-consuming communicative process based on accumulated experiential knowledge." Rather than favouring a purely

94 see Slovic 2000.
95 see Felgentreff et al. 2012, p. 71.
96 Edwards 2009, p. 80 f.
97 ibid.

consensus-based model, the participants believed that a society's capacity to embrace dissent and dialogue was fundamental to enabling an open debate. In this context, the ability to embrace dissent also manifests as fault tolerance.

Rather than following a top-down strategy, this approach seeks to integrate different viewpoints into a smaller framework. It once again exposes the communitarianism versus centralism power struggle that characterises the relationship between citizens and the State. This relationship has undergone a fundamental transformation – in a world characterised by growing uncertainty, citizens are increasingly expecting the State to deliver on its promise to protect them, something that might turn out to be the "illusion of the modern age". While on the one hand there are calls for people to take responsibility, the increased complexity of the relevant chains of events means that it is in fact extremely difficult to define these responsibilities clearly.

When the State is unable to keep its promise, the search for someone to blame causes people to question the State's raison d'être, i.e. the establishment of stability and security. In fact, however, this is a communication problem rather than a real phenomenon. As soon as citizens start expecting the State to be responsible for everything without being (politically and socially) active themselves, the relationship between the two becomes counterproductive – after all, there is a limit to how much protest a society can actually take. In other words, an understanding of modernity that believes everything to be controllable could be at the root of public dissatisfaction with the performance of the State. In view of this perceived loss of power and control, it is therefore necessary to investigate the extent to which complete control is actually needed.

There are two ways of interpreting the calls for increased public risk competence. The first envisages a scenario where well-informed citizens are able to participate in technology policy decision-making. However, there is a second interpretation that highlights the danger of both the State and businesses refusing to take responsibility for risks themselves, thereby devolving the burden of protecting against these risks onto the public.[98] Consequently, it is important to ask whether either of these alternatives is justifiable and realistic and if so, to what extent.

Education plays a central role as an individual resource and the key to participation. The participants in the World Cafés stressed the importance of teaching people the skills and knowledge needed to enable resilience right from the earliest stages of their socialisation. Under this approach, education helps to increase social resilience by helping people to help themselves.[99] The very act of addressing how society deals with risk in the pre-school, school and continuing professional development settings creates the basis for a resilient society. This does not mean that the State is passing the buck – rather, its role is to coordinate and facilitate communication between different stakeholders and channels.[100]

Roles, responsibilities and communication

The shift in and reinterpretation of the relationship between citizen and State also raised questions about the roles and responsibilities of institutional and political structures. In addition to providing a platform for public debate and ensuring that all members of society are able to participate freely, the participants also believed the State's role to include aspects such as the provision of services and indeed their suspension at such times as may be necessary in order to preserve their functionality. In the context of communication, it is also desirable to draw a distinction between the State and government. The State is, for example, responsible for civil defence. It was noted that in Germany, the relevant organisations (e.g. the Federal

98 see Kaufmann 2013.
99 see also the views of Rosanna Briggs in the second of the expert workshops organised by the Fraunhofer Ernst-Mach-Institut.
100 see Mayer 2013.

Office of Civil Protection and Disaster Assistance, BBK) still lack any kind of resilience strategy. Moreover, introducing one will be far from easy, since any serious attempt to implement the ideas that underpin the concept of resilience would require fundamental changes to current risk management practice.[101] Best practices from other countries could provide a valuable starting point for addressing this challenge. Accordingly, the next chapter of this study presents the results of the workshop on international perspectives on resilience that was organised and run by the Fraunhofer Ernst-Mach-Institut (EMI). The role of government, meanwhile, should be to communicate high-quality information to the public and to decision-makers, as well as to build the relevant (communication) structures.

However, communication with the public does not simply mean passing on information to citizens or indeed devolving responsibility onto them. Communication strategies should take account of differences between individuals, subjective variability in what people are prepared to accept and cultural specificities.

It became clear from this discussion that resilient communication structures should incorporate and strengthen the prevention aspect. Participants also believed that resilient communication structures could form one of the three pillars of an overarching civil protection and security strategy, alongside the existing pillars of emergency and risk communication. Improving communication between different generations in order to share people's experience and prevent it from being lost (e.g. the experience of the generation that lived through the war) is another possible means of strengthening resilience. The importance of adopting an approach that is relevant to people's everyday lives was stressed, in order to combat the danger of them being overwhelmed by information that is simply too much for them to process (e.g. doomsday scenarios). The tongue-in-cheek suggestion was made that resilience is in fact public enemy number one as far as the media are concerned, since a resilient society means that they will have fewer disasters to report on.

Measuring social resilience

The vulnerability debate could potentially provide a basis for devising methods of measuring social resilience, since numerous indicators for measuring vulnerability already exist (see e.g. Chapter 3.2.1, which describes Susan Cutter's SoVI project). However it is important to remember the conceptual differences between resilience and vulnerability that have already been alluded to in Chapter 2.5. These mean that the methodologies used for vulnerability cannot simply be transferred to resilience without first being adapted. One further difficulty is that the choice of indicators is highly dependent on our understanding of social resilience, i.e. on the type of threats and uncertainties we believe a resilient society should focus on (e.g. terrorism versus natural disasters). Superficially, this shouldn't matter if resilience is understood in terms of a holistic approach. However, when it comes to putting the conceptual ideas into practice – if not before – there is no getting away from the question of how the individual dimensions should be weighted in relation to each other.

The methodological problems connected with social resilience and the associated inaccuracies in how it is measured could potentially result in the real challenges being overlooked. In other words, there is a danger that strategies based on figures – and it should be stressed that this argument relates only to purely quantitative measuring techniques – could be based on flawed information. Edwards' theoretical ideas centred on the "Four E's" were mooted as one possible basis for an empirical analysis of social resilience, since they integrate social factors into a holistic approach.

In addition, one specific challenge associated with attempting to measure resilience is that it is a dynamic concept – the resilience of individuals and groups changes over the

[101] see Felgentreff et al. 2012, p. 70.

course of their lives and its meaning can also be modified by cultural influences. At the same time, it is important to prevent resilience from being relegated to the status of a variable construct that can be adapted to suit any interests, thereby making it little more than an alibi or label for completely different problems.

Summary

Overall, the concept of resilience poses a significant challenge for both society and the State. This is because while the pace of social change continues to accelerate, values still tend to be expressed as rather inert and static constructs. While there are growing calls for societies to increase their ability to adapt to new threats, it is necessary to investigate the extent to which this is actually possible without placing excessive demands upon their citizens.

In order to establish social resilience as a dynamic concept, it is therefore necessary to take into account the static characteristics of collectively shared values and norms. In addition, current social trends such as the rise in social inequality constitute an impediment to social cohesion, which is one of the main components of social resilience.

The participants identified a number of factors that are key requirements for a resilient society. For instance, members of the public should be given more opportunities and rights to participate, something that can be achieved by transferring power and responsibility from the State to smaller entities (local communities, individuals, etc.). In this context, Edwards talks of the "invisible role"[102] of government, a concept that he explains as follows:

> *"The role of central government in community resilience will always be limited. It will not be the main protagonist, a supporting actor or an extra – rather its role will be played out behind the scenes by a supporting cast of players who ensure the system is operating to the best of its ability."*[103]

In Edwards' concept of community resilience, the visibility of the State is limited – rather than acting as the main protagonist, it will be confined to a behind-the-scenes role. His perspective therefore focuses on strengthening civil society and civil protection through the inclusion of decentralised social actors.[104]

Trust is a key requirement for social resilience – so much so that Edwards describes it as one of the two fundamental pillars of resilience: "The politics of resilience is founded on two pillars: trust and dialogue"[105]. Trust in political institutions strengthens people's desire to participate and prevents conflicts between government and the public.[106] In a resilient society, it is also essential that people should trust each other. The connection between trust and social cohesion becomes readily apparent in this context, since social cohesion is heavily influenced by people's trust in their democratic institutions.[107]

Seen in terms of resilience, the fact that trust in political institutions and social cohesion are both currently declining forces us to ask whether we are not in fact getting further and further away from the key characteristics of a resilient society. On the other hand, a holistic resilience debate has the potential to move these trends higher up the agenda again by analysing how social processes and a society's vulnerability in the event of a crisis exert a mutual influence on each other.

---

102 Edwards 2009, p. 80.
103 ibid.
104 see also Mayer 2013.
105 Edwards 2009, p. 22.
106 see ibid.
107 see ibid., p. 60.

2.3.2 RESILIENCE AS A STRATEGY FOR PROTECTING CRITICAL INFRASTRUCTURE

The second round of World Cafés focused on the meaning of resilience in relation to critical infrastructure. The aim was to discuss how and to what extent resilient critical infrastructure can be modelled. Participants would also explore whether the concept of resilience is underpinned by a cohesive, holistic approach and, if so, how human beings and systems can be integrated into this approach. The priority of this World Café was, moreover, to identify the key indicators of resilience for specific types of critical infrastructure. In other words, its focus was on how best to implement resilience in a critical infrastructure setting.

According to the definition adopted by the workshop, infrastructure is regarded as critical if its failure results in significant harm to the common good. This definition is very close to the interpretation of critical infrastructure proposed by the German Federal Ministry of the Interior (BMI)[108].

When participants tried to rate how critical different types of infrastructure are, it became clear that the definition of criticality is heavily dependent on which underlying indicators are used. In other words, the term "critical infrastructure" can encompass a variety of different features. For example, while the US definition of critical infrastructure includes schools, the German one does not. In view of this context-sensitive variability in the definition of criticality, the participants decided to begin by identifying indicators of infrastructure criticality before moving on to discuss which measurement values can be considered critical or non-critical.

Indicators of infrastructure criticality

In order to help identify indicators of criticality, an analytical distinction was drawn between the actual damage caused by the failure of a critical infrastructure on the one hand and the system's technical structure on the other. This was done to avoid falling into the trap of simply assuming that there is always a top-down, causal relationship between the failure of a technological system and the resulting social impacts.

The level of damage can be measured using both quantitative and qualitative methods. The limitations of purely quantitative indicators are illustrated by the fact that they are of limited value for assessing the damage caused when a person dies[109]. The public perception of damage also plays an important role. For example, the impact on public opinion of someone dying from *E. coli* poisoning is disproportionately high, while people who die in road accidents barely impinge upon the public consciousness at all anymore.

The distinction between functional and structural preservation was felt to be key to determining the criticality of a technological system. In the case of the transport system, for example, its function is to transport goods and people whilst its structures include motorways and rail networks. Functional preservation therefore involves maintaining the service (in this instance, transport) provided by the infrastructure. In this context, resilience equates to "risk management as part of an ongoing process", while "service level compliance" – which is another of the associations identified in the conceptual framework – can act as an indicator of resilience.

Dynamic modelling of technological systems also needs to take account of the fact that the initial conditions under which a system is created themselves form part of the system, i.e. if these parameters change then the system will no longer be optimally configured. In terms of how the technological challenges are addressed, there is a fundamental danger that the design of resilient systems will be based on past experience rather than on future needs. Roadmaps

[108] see the BMI's KRITIS strategy 2013.
[109] for more on this, see Viscusi/Aldy 2003, pp. 5 – 76.

that describe e.g. physical limitations (the limitations of using battery-operated devices, for example) can help to gain a better understanding of the complexity of technological infrastructure systems.

From a technical point of view, infrastructure systems are composed of nodes and edges. However, the nodes themselves should not be regarded as critical – it is the values measured at these nodes that determine criticality. It is also necessary to decide what the appropriate level of protection is and whether or not it is affordable. The fact that the level of protection can be influenced by organisational factors is illustrated by the way in which electrical grid outages increased following grid deregulation and privatisation.

In the functional preservation approach, damage can be described as a relative loss of functionality resulting from the impairment of a node or edge. However, the exact extent of the damage cannot be easily assessed by a cost-benefit analysis. In addition to nodes and edges, other traditional infrastructure research criteria include factors such as density and centrality.[110] Robustness, redundancy and resources for enabling infrastructure innovation are further core elements in the discussion of technological systems' properties. Very few dynamic indicators have hitherto been identified for measuring the resilience of critical infrastructure. This is in spite of the fact that the dynamic aspect – e.g. how things change over time – should be absolutely fundamental, since the time it takes to restore the system is a key factor, particularly in terms of networking and interdependencies. In order to enable the principles of resilience to be applied to critical infrastructure, greater emphasis should also be placed on system properties such as early detection, prevention and proactivity (as opposed to a purely reactive approach).

Threats as future eventualities

Since threats are things that might happen in the future, the measures designed to protect critical infrastructure also need to be focused on future eventualities. This poses the problem of how to model different types of disturbance in the context of unknown future scenarios. It is therefore necessary to investigate the extent to which engineering solutions can be used to cope with unforeseen threats and disasters. The following suggestions were made in this regard:

1. A scenario-based approach, employing scenarios with far-reaching consequences such as an "electrical blackout situation". In this scenario, the challenge is to restore electricity to a given number of people in a given area within a given period of time. Protection goals and strategies are formulated based on a detailed study and analysis of the consequences of the scenario. These could take the form of lists containing sequences of actions and instructions for operators to follow in the event of a blackout.

2. The use of simulation models to study e.g. the impact of disasters on the connections between electricity grids and IT networks, so that impact assessments can be produced. The degree of abstraction employed in this system modelling is key. It is therefore necessary to decide how much analytical effort should be invested in different categories of error, since the more a system deviates from its state of equilibrium, the more abstract the instructions for how to respond become. This is even more of a challenge for open, dynamically modelled systems, insofar as it is necessary to define both a desired degree of deviation (dynamic functional preservation) and a critical degree of deviation (where functionality can no longer be maintained as a result of the disturbance).

3. Proposed solutions should be independently verified by two groups of experts. This would involve the two groups repeatedly anatomising the proposed solution to the point where it can no longer be deconstructed any further. At this stage, the remaining core proposal should be identical in both groups and any weaknesses should have

[110] see Tierney/Bruneau 2007.

been eliminated. It will now be a resilient solution and can provide a basis for rebuilding the system step by step. If the two groups fail to arrive at a (common) core proposal, other proposed solutions will need to be developed.

While the first proposal does include the public, the simulation approach should be investigated to assess whether it is in fact possible to simulate the decisions of decision-makers and individuals, particularly in view of the fact that individual decisions in extreme situations are often made on an emotional rather than a rational basis. Simulation models frequently ignore the difficulty in identifying and accurately simulating patterns of emotional behaviour, preferring to assume that individuals' actions will be governed by the rational decisions of "homo economicus". Moreover, the hugely complex nature of the interdependencies and interactions between people and systems forces us to question whether collective effects can or indeed should be simulated. In this context, it is also necessary to distinguish between the two analytical levels of human beings and technological systems, in order to take account of the top-down implications that have already been alluded to. Since simulations cannot be developed on a purely theoretical basis, it is important for any resilience simulations to draw on the lessons learned from practical experience.

In the third proposal, the deconstruction and analysis of old systems and their underlying principles (such as the horse and carriage) that might at some point reach their limits of their own accord (rather than as a result of external – e.g. economic – factors) reflects a dynamic approach to resilience. This is a characteristic that probabilistic approaches are incapable of. It was however stressed that attempting to anticipate the unimaginable – for instance the Chelyabinsk meteor (although people were in fact aware that it was theoretically possible) – can lead to the danger of creative potential and problem-solving strategies being blunted. As one of the workshop participants put it, the attempt to control the uncontrollable leads to a loss of imagination and a decline in people's ability to find their own way out of dangerous situations.

Under this approach, human beings are absolved of responsibility. One of the issues touched upon during the World Cafés was that in other countries human beings tend to occupy a far more central position in the debate. In Germany, on the other hand, people's capacities and ability to help themselves tend to be underestimated as a core component of social resilience, compared to technological systems. This analytical problem – whereby too much attention is paid to the technological system itself as opposed to the actual disturbance or the people affected by it – came up on several occasions. It highlights the danger of simply treating the human factor as an "add-on" to technological systems in the context of critical infrastructure. Moreover, it is at the root of the criticism of a high-tech bias in the majority of resilience strategies developed in the field of security research[111].

Summary

In summary, it became clear during this World Café session that the social and technological issues are closely intertwined. While technological systems do have a role to play in increasing resilience, the role of human beings in controlling these systems tends to be underestimated. Their operators should therefore be provided with clearer guidelines. In addition to the problem of communication, it is also necessary to address the issue of organisation (e.g. bottom-up versus top-down, deregulation versus State control) and to create clear structures and well-defined responsibilities. In conclusion, when debating an appropriate and technically feasible level of protection, it is important not to lose sight of the system's users and the actual social problems it is supposed to address. British urban planner Cedric Price posed the following question: "Technology is the answer, but what was the question?"[112] The goal should be to make sure that this question no longer applies.

[111] see Dunn Cavelty 2013.
[112] Price in Mathews 2007.

2.4 FUTURE CHALLENGES AND TASKS

The goal of the workshop was to identify and document the future challenges and issues that the field of security research will need to address when dealing with the concept of resilience. The results of the third World Café, which focused specifically on this theme, are outlined below.

The importance of the concept of resilience for future challenges

It is the demands of our 21st century society that make the concept of resilience so relevant. Changing economic circumstances, the dependent nature of our electricity supply and the trend towards individualisation are among the factors that are leading to a loss of control that can no longer be compensated for by technological solutions alone. Systems are becoming more complex, interdependent and networked and this inevitably results in a certain degree of uncontrollability and unmanageability.

Uncertainty is hence a defining characteristic of the modern age and is accompanied by a real or subjective loss of control. Any attempt to control future events from the present day runs the risk of creating a control illusion – by relying solely on anticipated scenarios, technological solutions and human behaviour models, we fail to take into account the possibility of low-probability events that could nonetheless have major repercussions (black swans, unknown unknowns). It will therefore be important always to define the scope of future resilience strategies, stating the extent of what they are able to achieve, the context in which they can do so and the limitations and obstacles.

The key to selecting resilient strategies thus lies in the vulnerability of the target state "resilient society", even if this cannot be easily, comprehensively and universally specified.

Goal conflicts/goal definition

One of the principal future challenges is to define the goals that describe the target state of a "resilient society" that is capable of regaining control by identifying the main drivers that cause control to be lost.

However, Chapter 2.3 has already highlighted the issues involved in anticipating future states – the challenges associated with global and systemic threats and hazards are often connected to their unpredictability and the fact that they cannot be planned for in advance.

Consequently, the resilience debate must recognise the fact that although increasing a society's resilience will involve the normative formulation of defined goals, these will never be fully attainable. While there are undoubtedly many scenarios and predictable developments where "what if" strategies can help to prevent damage, these are no substitute for flexible and creative response strategies when scenarios unfold in an unexpected manner.

When resilience is stipulated as a target function – be it in a research project or as part of a policy strategy – it is always essential to specify the conditions under which it is expected to occur. Failure to do so will mean that there is no framework for evaluating the strategy's success and will lead to goal conflicts between different actors such as the local authorities and the public. Goal conflicts can also arise when resilience is approached from an economic perspective, since an efficient and profitable business strategy may sometimes be at odds with a strategy that is resilient.[113] Moreover, in situations characterised by conflict arising from social inequality, it makes little sense to define restoration of the "initial state" as a goal, since not all the stakeholders will be equally keen for the preservation of current living conditions or maintenance of the status quo to be a protection goal of the resilience strategy.

[113] see also the outputs of the third expert workshop that was run by KPMG AG.

Finally, the choice of a target state also possesses a political dimension, since in order to create a more resilient society it is necessary to make people follow certain guidelines. Who decides what these guidelines should be is an open question that should be discussed as part of a comprehensive communication process.

Communication

In order to prevent goal conflicts, it is important to devise a communication strategy that informs and raises awareness without spreading paranoia. Secrecy and the development of resilience strategies behind closed doors should be avoided at all costs. One crucial aspect of communication is to ensure a dialogue between stakeholder groups with regard to the goals that resilient strategies should pursue, since different groups may have different goals. The dialogue should be transparent and to the point and should facilitate participation. This will help to actively engage the public and prevent an exclusive focus on "making the system immune to external threats".

Guiding strategy

If resilience is to serve as a leitmotif or guiding strategy for technological, social and political development, it will be necessary to define the relevant target states through a negotiation process that includes the whole of society so that roadmaps can be formulated for decision-makers. This process can begin by identifying the key drivers that have an influence on the attainment of the target states in different sociocultural, technological, economic, environmental and political areas. In the past, the tendency has been to define target states in negative terms, i.e. people have tended to focus on what they do not want (e.g. which types of damage should be avoided). It is harder to come up with more positive definitions that emphasise redundancies and buffers as elements of a guiding strategy, since although relevant to technological systems, they are less so for social systems.

One reason why it is difficult to formulate positive guiding strategies is that resilience to some extent needs to be understood as a "moving target", meaning that just one overarching strategy is not enough. When it comes to tackling threats and protecting against disasters, every single problem and solution requires a strategy that has been modified for the specific conditions in question.

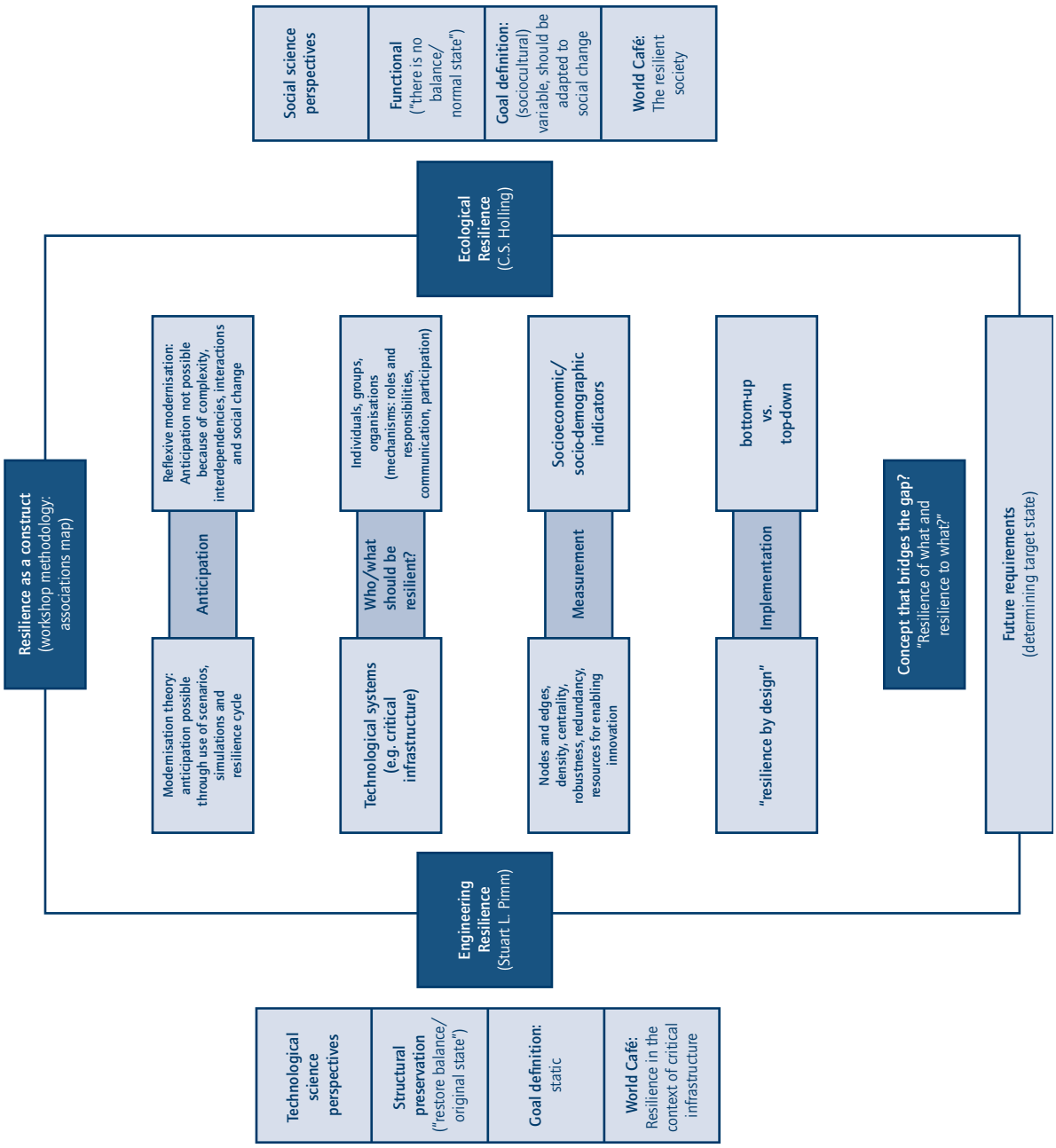
Resilience should therefore be understood and implemented in terms of a "toolkit approach", whilst any recommendations made to decision-makers should emphasise their limitations and the fact that they are confined to a specific target. Protection goals and levels of protection should be based on the outcomes of negotiation processes informed by the guiding strategy.

2.5 CONCLUSIONS

The workshop "Resilience – National Perspectives" sought to facilitate an interdisciplinary discussion on the subject of resilience with the aim of identifying ideas for a holistic concept of resilience capable of bridging the gap between different disciplines (see Fig. 5). It was established that there is a clear need for such a concept in view of the numerous interdependencies that exist between technological and social systems. As such, any holistic approach must bridge the gap between these two opposite ends of the spectrum. The trick will be to find a way of integrating the two conceptual approaches of engineering resilience and ecological resilience. Whilst the former focuses primarily on engineering questions (e.g. critical infrastructure), the latter tends to be employed to address the issues associated with a resilient society. Both approaches can learn valuable lessons from each other that will benefit their respective fields of research.

For example, the engineering concept of robustness – i.e. the ability to resist – could also constitute an important

Figure 5: Resilience as a concept that bridges the gap between different disciplines



Source: Research Forum on Public Safety and Security.

characteristic for societies seeking to oppose illegitimate regimes. Indeed, the purely adaptive measures that would tend to be favoured by the social resilience perspective could have disastrous consequences if applied to the context of an illegitimate regime. Conversely, adaptability is in certain circumstances undoubtedly a desirable feature for technological sub-components and systems, since it allows them to be employed more flexibly. Robust but rigid structures can be difficult to adapt owing to their lack of dynamic components. In addition, the goals of technological systems should not be permanently fixed, since they need to be capable of responding to new social challenges and developments.

Rather than exclusively applying engineering resilience to technological systems and ecological resilience to societies, in a holistic approach the focus should be on the interactions between technological and social systems. The key question is how well a resilient critical infrastructure can perform in the face of a given threat to society. It is also necessary to turn this question around and ask whether society is capable of absorbing the impact of critical infrastructure failure. Consequently, it is clear that the two poles cannot be considered in isolation of each other and there is nothing to be gained from splitting resilience into two separate conceptual approaches that exist side by side but are completely unconnected. An approach that bridges this gap is therefore essential, if nothing else to prevent the duet between the engineering and social science perspectives from being discordant. If we do not integrate these two perspectives, there is a danger that technological innovations will fail to win public acceptance and will therefore be unable to function efficiently.

In the societal context, the mode of anticipation is a mechanism that people have always used to cope with their everyday lives. However, in our complex, boundariless postmodern societies, the future can only be anticipated up to a certain point. It is important to remember this, so that we do not overestimate what we are capable of. To believe that we can anticipate future events with complete accuracy would if anything have the effect of making us less resilient.[114]

While anticipation does play a more significant role in relation to technological systems, here too it is important to avoid falling into the trap of believing that everything is fully controllable. Failure to do so could not only result in the wrong measures being implemented but could also influence public perception of risks in a way that would be detrimental to society's resilience. While anticipation in the shape of scenarios and simulations is indispensable for technological systems, it is important to ensure that the scenarios are dynamic in nature, i.e. they should not be defined too rigidly. This could be achieved by integrating dynamic elements (ecological resilience) into the modelling of technological systems.

Rather than blithely overestimating technological systems' ability to provide adequate protection against complex risks, it is necessary to place greater emphasis on human capabilities. In the context of critical infrastructure, it is important that people should not simply be treated as an add-on to technological systems. Instead, an approach should be adopted that provides the structures needed to strengthen public participation and people's ability to help themselves. The State should act as a kind of organisational framework that works with citizens in the interests of society. The fact that disasters can sometimes actually have the effect of increasing resilience was demonstrated by the way that people helped each other out during the most recent floods in Germany in 2013. This example provided a graphic illustration of the importance of social cohesion. However, this very social cohesion is increasingly being undermined, not least by the failure of policymakers to adequately address growing social inequality. Security research therefore needs to place greater emphasis on investigating the social dimensions in order to ensure that we do not continue to rely exclusively on technological

[114] see Lorenz 2013, p. 12.

systems to provide us with an adequate level of protection. Failure to do so will result in a disconnect between the social and technological approaches. Paul Valery encapsulated the discrepancy between these two approaches in the question "Can the human mind master what the human mind has made?"[115]. An integrative concept of resilience that combines the social and technological approaches and prevents them from drifting too far apart is thus undoubtedly the most sensible way of tackling future threats and hazards.

All these abstract theoretical constructs and ideas need to be put into practice through concrete strategies at the implementation level, where it is necessary to draw a distinction between scientific knowledge in the shape of large volumes of data and policy strategies (knowledge versus action). Finally, in addition to asking who should be responsible for resilience and how they should deliver it, we above all need to decide exactly what it is that we want to make resilient.

The following table summarises the key lessons learned from the workshop:

Table 1: Lessons learned from the first workshop

LESSONS LEARNED	CONTENT
1. Resilience as a holistic approach	Formulation of an integrative, holistic concept of resilience that combines the ecological resilience and engineering resilience approaches and prevents the social and technological dimensions from drifting too far apart (one practical example would be the involvement of several experts from the social sciences and humanities in the design of new technologies).
2. Identification of categories for a holistic concept	A holistic concept should address in detail the categories of anticipation, who/what should be resilient, measurement and implementation, since these are the key dimensions that shape different perspectives on resilience.
3. Measuring resilience	The methodology used for measuring resilience should include both quantitative and qualitative (measurement) techniques. In addition, it may prove useful to base the methodology on existing measuring techniques (such as the Social Vulnerability Index) and combine it with them.
4. The normative and reflexive approaches	In order to prevent goal conflicts, it is necessary to introduce a reflexive element into the understanding of resilience as a normative concept. It is of course necessary to establish normative criteria in the field of applied security research. However, it is important to ensure transparency with regard to the actors who establish these criteria and what their intentions are. For instance, the resilience of a social system cannot be a value in itself. Ultimately, different sets of values are involved that cannot be evaluated on an ad hoc basis.
5. Participation and democratic legitimacy	Opportunities to participate based on a bottom-up, decentralised approach are essential, e.g. to facilitate community-based decision-making. This approach follows Edwards' understanding of the pillars of resilience: "The politics of resilience is founded on two pillars: trust and dialogue". According to this interpretation, participation is an instrument for ensuring the democratic legitimacy of technological developments. In this context, education is a key component of participation.
6. A critical assessment of the mode of anticipation should be undertaken	While we should of course make use of the available technology, we must avoid the trap of believing that we can control everything. The extent to which we are able to anticipate future threats is limited. This is because interdependencies are increasing and boundaries are disappearing, creating an increasingly complex world where it is no longer clear who is responsible for what.
7. The relationship between resilience and sustainability must be defined	We need to define and discuss the relationship between resilience and sustainability. For example, there are certain situations where resilience requires redundancies. It is therefore necessary to check whether these redundancies are at odds with the sustainability principle of (e.g. economic) efficiency. This will allow potential conflicts to be identified as early as possible.

[115] Paul Valery in Bauman 2000, p. 1.

3 RESILIENCE: INTERNATIONAL PERSPECTIVES

BENJAMIN SCHARTE, DANIEL HILLER, TOBIAS LEISMANN, KLAUS THOMA

3.1 RESILIENCE – THE TERM, THE CONCEPT AND ITS PRACTICAL VALUE

Academic terms and concepts are all very well, but ultimately they are just fine-sounding words. Resilience is one such concept. It is a buzzword with its origins in developmental psychology and ecology that has now found its way into the field of security research. In the US, the adjective "resilient" is blithely used by the media – without the slightest theoretical understanding of its meaning – to describe everything from dogs to sports stars, terrorists and even mould.[116] A trawl of the Web reveals that the term "resilience" has been invested with huge significance and is now being indiscriminately touted as a successor to that ultimate millennium buzzword "sustainability". Its meaning has been expanded to include pretty much everything one could imagine.[117] In contrast to its straightforward adjectival use in the media, in Germany it is a concept that has remained confined within the ivory tower of social science theory, being batted back and forth in the debate between political scientists and sociologists. So what are we to make of resilience? What good is the concept to us? And how can it be usefully employed both at a policy level and in disaster protection and prevention practice?

The preceding chapter on the "national perspectives" has shown that discussion of resilience in Germany is confined mainly to the realm of social science theory. However, this is of little practical use to people on the ground, be they civil defence workers, first responders, architects, or just ordinary members of the public. People fighting for their lives in the face of freak storms, unprecedented flooding, or a terrorist attack that the authorities failed to prevent do not stop to think about the boundaries of the concept or its semantics. They may well be able to survive the disaster thanks to a well-built embankment, excellently trained and equipped first responders, a close-knit community or a timely and accurate advance warning. However, they couldn't care less about which of these measures was mainly responsible for saving them. All that matters is the outcome. It is the combination of several perfectly coordinated measures that in fact makes it possible to minimise the damage caused by adverse events, and this is the key feature of resilient societies.

Of course, this isn't the whole story. Even in Germany, it is not only the academics in their ivory towers who discuss and show an interest in resilience. For example, the fact that the Federal Ministry of the Interior, which is responsible for civil protection, is a member of the Multinational Community Resilience Policy Group[118] is a clear indication that resilience has now become part of civil protection practice in Germany too. Nevertheless, Germany could learn a great deal and benefit enormously from taking a closer look at the wide range of research initiatives and practical projects that are currently being undertaken under the heading of resilience in Europe and North America.

However, the previous chapter also highlighted the importance of starting by reflecting on the scope and limitations of different terms and concepts. It is first necessary to establish a common language before all the relevant actors can work together productively and constructively on innovative solutions for the resilient societies of the future. If society is to succeed in meeting the manifold challenges of the complex, interconnected world that we live in today, it will be necessary to integrate the technological, legal, economic, political and social aspects into a single, symbiotic system. Different ideas and approaches to delivering this ambitious goal can be found in the research programmes and policy

116 Abramson 2010; Filkins 2010; Sacks 2006; Smith 2013.

117 Zolli 2012.

118 This multinational working group is composed of top officials from the civil protection authorities and ministries of countries such as the US, Israel, Canada, the UK, Singapore and Germany. The group meets once a year to hold informal discussions about national resilience strategies, implementation programmes and strategies for establishing and increasing community resilience.

initiatives of various countries around the world. The UK and the US have undoubtedly led the way in this area. In the aftermath of 9/11, the shocking realisation of their own vulnerability and the recognition of a continuing threat to their security led both countries to begin systematically researching resilience, incorporating it into government programmes and implementing it in a real-world setting.[119] Researchers, policymakers and practitioners in Germany can learn from their experience, thereby avoiding needlessly making the same mistakes, adopting good ideas and best practices and engaging actively so that they too can contribute their own experiences and ideas to resilience theory and practice around the world.

This chapter is based on the outcomes of the expert workshop "International Perspectives on Resilience", the main aim of which was to look at the resilience strategies that are already being implemented in selected countries. The workshop also sought to gather information on other interesting questions, for example: What methods exist for quantifying resilience? In the view of the experts, what are the main unanswered questions in the field of resilience research? Which areas require further research? In a high-tech world where complexity is increasing at an almost exponential rate, what are the most promising resilience strategies, i.e. the ones that are likeliest to be sustainable in the long term? In order to ensure that the contributions to and outcomes of the workshop were both academically rigorous and practical in nature, we invited some of the world's foremost experts in this field. These included researchers such as Susan Cutter, Wolfgang Kröger and Jon Coaffee, as well as practitioners such as Rosanna Briggs (an emergency planner at Essex County Council) and Erik Thomassen of the Norwegian Directorate for Civil Protection and Emergency Planning. This meant that the concept of resilience could be approached from a number of completely different perspectives, ranging from the societal aspects addressed by Susan Cutter's "Social Vulnerability Index" to the technical specifications and requirements of a resilient energy supply and the crucial role of education in a disaster prevention and protection setting.

It is already clear from the above that, just like the national perspective, the international perspective on resilience is also characterised by a variety of different themes and approaches. However, it soon became apparent that the common denominator shared by every single research project and practical implementation of the concept of resilience is their focus on safety and security, protection and public preparedness for all kinds of adverse events. All the experts agreed that resilience to negative events, whatever their exact nature, involves minimising potential or actual damage to people's physical and material well-being. As such, resilience is a property of society and its subsystems (e.g. critical infrastructure) that is essential to sustainable development. On the other hand, it proved more difficult to reach a consensus regarding the best and most sustainable way of achieving this goal, which aspects merit special attention and the point where an acceptable or good degree of resilience can be said to have been achieved. Consequently, what common ground does exist is just the starting point for a whole host of different research topics, practical examples and ideas, all of which could prove extremely valuable to the "Resilien-Tech" project and its final recommendations. The expert workshop provided an opportunity for these to be examined in greater detail.

The workshop took place in Berlin on 15 and 16 May 2013. It was organised and run by the Fraunhofer Institute for High-Speed Dynamics, Fraunhofer Ernst- Mach-Institut (EMI). In total, more than 30 national and international experts took part in the workshop, which was facilitated by German broadcaster ZDF's southern Europe correspondent, Michael Bewerunge. The workshop was attended by researchers and practitioners from Germany, France, the UK, the Netherlands, Norway, Austria, Switzerland and the US. This chapter will be divided into four sections in order to properly reflect all the themes that were presented and

[119] see 3.3.1 and 3.3.2, as well as Trachsler 2009, p. 2.

discussed during the workshop and provide an accurate picture of the international perspectives on the concept of resilience. Following these introductory remarks, it will begin with an overview of seven different research initiatives that are heavily focused on resilience, two from the US, two from the UK, two from Switzerland and one from France. This section will primarily draw on the ideas and themes that were addressed by the researchers during the workshop and included in their slide presentations. Some additional information will also be provided in the shape of quotations taken from the works of these authors. The chapter's third section will describe a small number of selected examples of policy initiatives in the area of resilience. These include the implementation of the concept in government documents, a practical strategy for increasing resilience in the field and an initiative that addresses how government can guarantee the resilience of critical infrastructure. This will be followed by a fourth section that will present a final overview of the international perspectives on resilience in the form of "lessons learned", i.e. the findings of the selected research initiatives and practical examples that could be of value to the German resilience community. It is not the goal of this chapter to provide a status report containing an exhaustive description of every single academic and government initiative relating to resilience. Instead, the aim is to add value to the "Resilien-Tech" project by outlining a targeted selection of particularly interesting research projects and implementation strategies that can be used to help develop concrete and meaningful recommendations for decision-makers in government, business, the research community and civil society.

3.2 RESILIENCE RESEARCH – INTERNATIONAL PERSPECTIVES

This section will analyse the research initiatives of seven different researchers and institutions whose work will provide the substance of the international perspective on resilience in the "Resilien-Tech" project. The individuals and institutions in question are Susan Cutter of the University of South Carolina, the United States National Research Council, Charlie Edwards of the UK's Royal United Service Institute, Jon Coaffee of the University of Warwick, Wolfgang Kröger and Timothy Prior of the ETH Zürich and Christian Sommade and Léo Muller of France's Haut Comité Français pour la Défense Civile.

3.2.1 SUSAN CUTTER, USA – THE SOCIAL VULNERABILITY INDEX (SoVI)[120]

Susan Cutter is a Professor of Geography at the University of South Carolina whose main interest lies in the topics of vulnerability and resilience. Cutter explicitly argues that vulnerability – and in particular social vulnerability – should not be understood as the polar opposite of resilience. Just because certain characteristics or circumstances make a person especially vulnerable to adverse events doesn't mean that they necessarily lack resilience. Cutter's interpretation of resilience and vulnerability is similar to the definition of resilience given in the introduction to this study, where it is described as the "ability to defend oneself against actual or potential adverse events, prepare and plan for them, cope with and recover from them and continuously improve one's ability to adapt to them." This instantly makes it clear why vulnerability and resilience cannot be regarded as two sides of the same coin – and at the same time why it is absolutely essential to recognise the vulnerability of certain sectors of society, certain locations, etc. It is only once these factors have been recognised that policymakers, disaster management experts, urban planners, etc., can identify vulnerable groups and take the measures needed to increase their resilience. Factors such as age group and ethnicity show little variation, while income levels and employment type only vary at the individual level. The elderly, children, people with physical and mental disabilities and the poor and unemployed are all particularly vulnerable and should receive special assistance from the State in the event of a disaster. To define resilience

[120] A useful overview of the SoVI concept can be found in Cutter et al. 2003.

as the opposite of vulnerability would be to say that these people cannot become resilient, or at least that they can only do so if they experience a major change in their social status. However, if resilience is defined as a holistic strategy for increasing the ability of society and its subsystems to cope with adverse events, then both decision-makers and, even more importantly, the people affected by the disaster themselves have the opportunity to increase their own resilience, however vulnerable they may be. For this to be possible, it is necessary to be able to establish as accurately as possible in advance of any adverse events who the vulnerable people are and how and why they are vulnerable. This is exactly what Susan Cutter's SoVI sets out to do.

Cutter and her team rather succinctly define vulnerability as the "potential for loss".[121] The fundamental question that they sought to address was why the same natural disaster can cause completely different types of damage in different social and geographical contexts. Cutter cites the impact of Hurricane Sandy by way of example. In strictly meteorological terms, it was by no means one of the worst storms in history. However, it caused huge damage in the highly urbanised and heavily populated area where it made landfall. While the fact that Cutter et al. only look at natural disasters means that their perspective is narrower than the wider understanding of resilience used in this study, this in no way diminishes the value of the SoVI index. The index was developed in response to the observation that the social aspects of vulnerability had traditionally received too little attention compared to the biophysical and infrastructure aspects, and that no comparative studies of the social vulnerability of different locations existed at that time. In order to define social vulnerability, the SoVI draws on Cutter's "hazards of place model". Risk (the likelihood of a hazardous event) interacts with mitigation (measures to lessen risks or reduce their impact) to produce the "hazard potential". This is then accentuated or moderated by the geographical context and the social fabric of the place in question. The geographical context determines biophysical vulnerability, while the social fabric determines social vulnerability. The combined scores provide a means of measuring the vulnerability of specific locations.[122] The SoVI only addresses the social aspects of vulnerability.

There is a relatively high degree of consensus within the social sciences regarding Cutter et al.'s assessment of the major influences on social vulnerability. These include a lack of resources such as information, knowledge and technology, limited access to political power and representation, a lack of social capital, age and limiting health conditions. However, there is less agreement with regard to the specific indicators that should be used to measure these factors. Age, gender, ethnicity, socioeconomic status and mental and physical disability are all potentially valuable indicators, while special groups such as non-native speakers, the homeless, transients and tourists may all be particularly vulnerable. However, there are also some circumstances where this may not be the case – for example, tourists are less at risk of losing all their worldly possessions than local residents. Other possible indicators include the quality of dwellings or infrastructure.[123] It is not easy to decide on a purely theoretical, a priori basis which of these indicators are suitable for measuring the factors alluded to above in order to accurately describe the social vulnerability of specific places and social groups. Cutter et al. therefore approached the development of their Social Vulnerability Index from the opposite angle. They employed a factor analytic approach to identify obviously relevant indicators (referred to as variables by Cutter et al.) based on the empirical data of several field studies of the various impacts of natural disasters on different locations. These variables were then used to explain the differences. Originally, more than 250 variables for social vulnerability were collected. The use of statistical techniques such as testing for multicolinearity[124] among the variables

121 Cutter et al. 2003, p. 242.
122 Cutter et al. 2003, p. 243 f.
123 ibid., p. 245, see also pp. 246 – 249 for an overview of the relevant potential influences on social vulnerability discussed in the literature.
124 A phenomenon in multivariate regression analysis, where two or more explanatory variables are highly correlated, meaning that their individual influence on the variable that they are being used to explain can no longer be identified. See Stock, J./Watson, M. 2012, Chapter 6.7.

allowed this number to be reduced to 85. Further statistical tests allowed the total to be whittled down to 42 variables on which a detailed factor analysis was subsequently performed. This resulted in the identification of eleven factors that explained 76.4 percent of the variance – i.e. the differences in the impact of the same disaster on different locations. These were multidimensional factors that incorporated 32 of the variables. The eleven factors were used to produce a map of social vulnerability in the United States. The unit of analysis was the 3,141 counties in the United States, while the data for the variables was drawn from the U.S. Census.[125] In other words, aggregated rather than individual, personal data were used. On the one hand, this can be viewed as a positive insofar as it ensured that the individual rights of the people affected were not violated. At the same time, however, it is also true that the relatively coarse resolution of the county level clearly requires significant refinement for the purposes of local disaster management – if not to the individual level then at least to the level of local aggregated data. Furthermore, the available data and underlying theory mean that the SoVI is a relative measure of social vulnerability. Specific places can only be rated as more or less socially vulnerable than other specific places or a predefined average.[126]

Following criticism of the SoVI by some sociologists, the factors relating to physical infrastructure were removed from the index, despite their high explanatory power. This decision was also partly due to the fact that the relevant data were not available at local level. Moreover, certain variables became unavailable as a result of changes to the U.S. Census. Nevertheless, it proved possible to replace these with new variables that could still be obtained from the census data, such as family structure, access to a car, etc. From a theoretical perspective, these can also be important determinants of social vulnerability. An updated version of the SoVI has now been produced. In its current incarnation, it comprises 30 variables that combine to produce a total of seven components (see Table 2) which account for 72 percent of the variance in the data.[127] In the absence of a sound theoretical basis for differentiating between them, all the variables are assigned the same weighting. In other words, each variable accounts for 1/30 of the total social vulnerability score.[128]

The map in Figure 6 was produced by applying the SoVI to the county level in the US. Counties are divided into three groups where the least vulnerable 20 percent (in relative terms) are shown in blue and the most vulnerable 20 percent are shown in red. This provides a useful initial overview of the areas that may require extra government assistance and attention in the event of a natural disaster. On its own, however, this tool is far less valuable than it would be if taken together with additional data on biophysical vulnerability. During the workshop, Cutter cited a study of the parts of New Orleans that were flooded as a result of Hurricane Katrina. In those areas where extreme flooding coincided with high levels of social vulnerability, the percentage of people who returned once the flooding had subsided was significantly lower than in socially and/or biophysically less vulnerable parts of the city. Of course, it is of particular interest to perform this type of analysis before the occurrence of an adverse event rather than after it. The index can thus once again be seen to be highly pertinent to the definition of resilience used in this study. In conjunction with data that accurately describe biophysical vulnerability, the results obtained from the SoVI can be directly employed in three of the five phases of the resilience cycle[129]. They can thus provide a basis for strengthening the resilience of societies and their subsystems. In the Prepare phase,

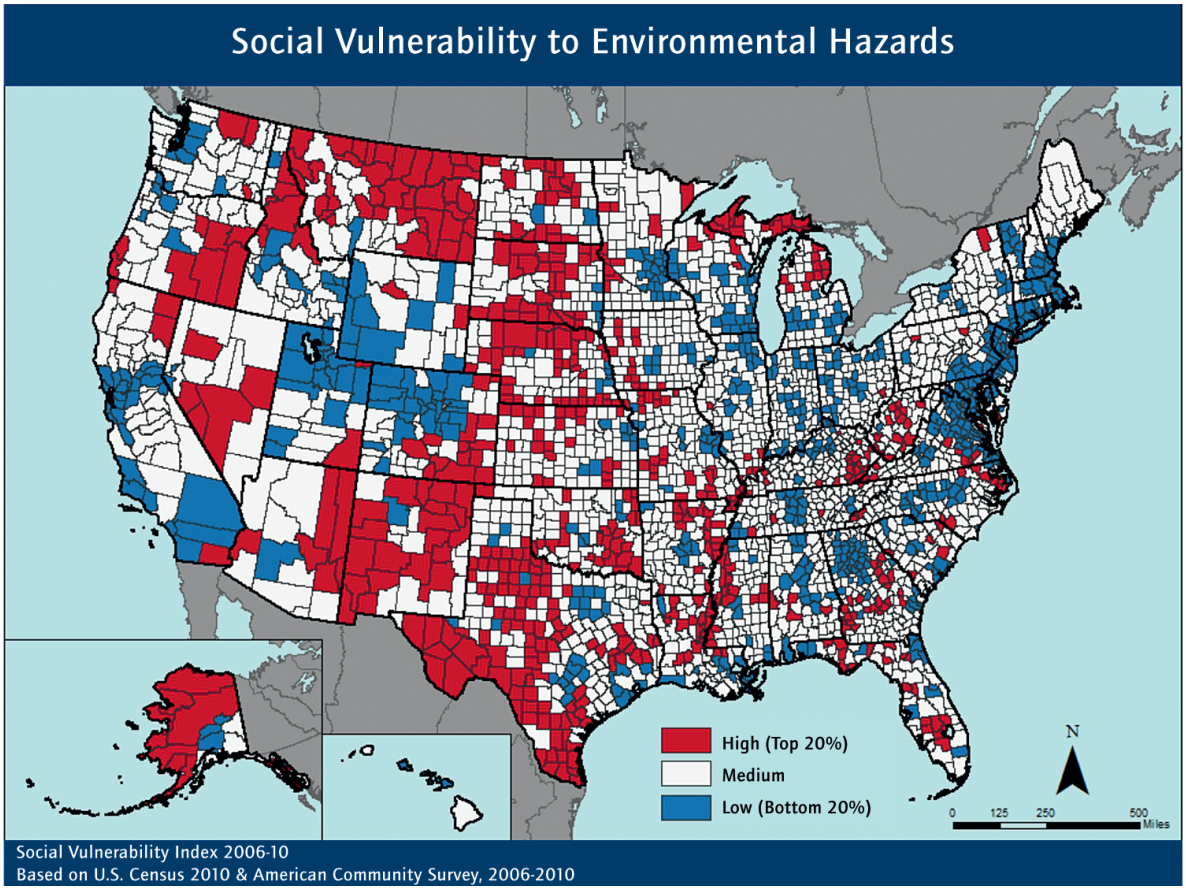
125 Cutter et al. 2003, p. 249ff.
126 ibid., p. 254.
127 HVRI 2013b.
128 Cutter et al. 2003, p. 254.
129 The resilience cycle is described in detail in the introductory chapter of this study. It comprises five phases: Prepare, Prevent, Protect, Respond and Recover. In the interests of clarity, this model consciously simplifies the real-life resilience cycle which is characterised by parallel phases with multiple branches. However, this complexity is still taken into account in the analysis.

Table 2: Explanatory power and composition of SoVI components

COMPONENT	CARDINALITY	NAME	% VARIANCE EXPLAINED	DOMINANT VARIABLES	COMPONENT LOADING
1	+	Race (Black), Class, Poverty	17.45	QBLACK	0.736
				QFHH	0.853
				QCVLUN	0.692
				QPOVTY	0.766
				QED12LES	0.667
				QNOAUTO	0.647
				QFAM	−0.794
2	−	Wealth	15.69	QASIAN	0.692
				PERCAP	0.730
				QRICH200K	0.810
				POPDENS	0.607
				MDGRENT	0.790
				MDHSEVAL	0.852
				QNONURBAN	−0.563
3	+	Age (Elderly)	12.98	MEDAGE	0.914
				QAGEDEP	0.774
				PPUNIT	−0.672
				QRENTER	−0.623
				QSSBEN	0.801
4	+	Ethnicity (Hispanic)	9.34	QHISP	0.687
				QFEMLBR	−0.669
				QEXTRCT	0.598
				QNOHLTH	0.728
5	+	Special Needs	6.73	QNRRES	0.628
				QMOHO	−0.454
				HOSPTPC	0.586
6	+	Ethnicity (Native American)	4.94	QNATAM	0.798
				QESL	−0.488
				QNOAUTO	0.489
7	+	Service Employment	4.45	QSERV	0.821
		Cumulative Variance Explained	**71.56**		

Source: HVRI 2013c.

Figure 6: Social Vulnerability Index results for the US



Source: HVRI 2013b.

they can help to identify areas with particularly high social vulnerability, allowing more efficient deployment of scarce resources for contingency measures and awareness-raising among the social groups in question. In the Protect phase, a similar identification process also enables efficient resource allocation, so that the highest possible increase in overall social resilience can be delivered for a given level of resourcing. This is because, all else being equal, the deployment of suitable protection technologies in areas whose inhabitants are at high risk of losing their lives and/or property in the event of a disaster is likely to have a greater impact than in areas where the damage caused by a disaster would be

expected to be significantly less severe.[130] Moreover, during the Recover phase, i.e. once the adverse event is over and society is trying to get back on its feet as quickly as possible, the results obtained from the SoVI can also help with the implementation of a smart recovery strategy that attempts not only to improve infrastructure but also to reduce social vulnerability as much as possible.

The Social Vulnerability Index developed by Cutter and her team has thus provided an exceptionally valuable tool for US resilience theory and practice. However, it will only offer similar benefits to decision-makers and security researchers in Germany if it can be shown to work equally well in different cultural contexts. The fact that versions of the SoVI that have been adapted to work with the data available in the relevant regions have already been used in countries such as Norway, Portugal and Indonesia suggests that it should be transferrable to the German cultural context. Moreover, the Hazards and Vulnerability Research Institute is continuously refining the Social Vulnerability Index and has plans to incorporate additional variables at a finer resolution, such as the number of homeless people, drug prescriptions and social capital data.[131] As yet, no version of the index has been developed for Germany. Given the obvious usefulness of this tool, it would appear to be worth investigating whether the corresponding metrics can be developed for Germany and whether their use there would be acceptable. While the SoVI could be directly implemented and adapted to the German context, it could also provide a blueprint for indices designed to measure different aspects of social vulnerability at different levels and different resolutions. In addition to the social aspects addressed by the SoVI, there is a particularly urgent need for technology-oriented metrics as part of a resilience-based strategy.

3.2.2 THE NATIONAL ACADEMIES, USA – DISASTER RESILIENCE: A NATIONAL IMPERATIVE

The National Academies of the United States are non-governmental academies of science that do not have links with any political party. Their role is to advise policymakers and government on current scientific and technological issues and problems of national importance. The National Academies comprise the National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine. The three academies' members are drawn from among the most distinguished researchers in their respective fields. The fourth organisation that belongs to the National Academies is the National Research Council, which acts as their operational arm and is tasked with undertaking research initiatives.[132] As such, it was responsible for the study entitled "Disaster Resilience. A national imperative", in which a team of researchers investigated ways of increasing the United States' resilience to natural disasters. In 2011, the financial cost to the US of the damage caused by natural disasters came to 55 billion dollars, without even attempting to calculate the cost of the 600 lives that were also lost. This led to the launch of a large-scale study of resilience to investigate how this damage could be significantly reduced going forward. It was believed that increased social resilience would be an appropriate means of pursuing this aim. The study's goals were as follows:

1. To define the concept of National Resilience and its implications for the United States.

2. To establish concrete goals, baseline conditions, performance criteria and metrics for resilience.

3. To describe the current state of knowledge about resilience.

[130] A purely economic interpretation might challenge this assumption by arguing that wealthy people have more to lose than poor people, meaning that it makes more sense to deploy protection technologies in relatively prosperous areas. However, since natural disasters, terrorist attacks, etc. pose a threat to human life, this would mean weighing up the value of a human life against economic goods. As a result, this type of approach would appear to be morally indefensible, at least for policymakers, if not for insurance companies.

[131] HVRI 2013.

[132] The National Academies 2012.

4. To outline the gaps in the research and obstacles that need to be addressed to increase resilience to adverse events.[133]

These goals closely match the goals of the "Resilien-Tech" project, suggesting that the results of the National Academies study should be carefully scrutinised to see whether they contain any ideas that could contribute to the debate in Germany, and if so, to what extent.

"Decisions by communities, states, regions, and the nation regarding whether or not to invest in building resilience are difficult. If building the culture and practice of disaster resilience were simple and inexpensive, the nation would likely have taken steps to become more resilient already."[134] In other words, building resilience is neither easy nor cheap. Nevertheless, a number of current trends mean that it is absolutely essential to do so. There is no doubt that adverse events will continue to occur in the future. The geographical vulnerability of US society is increasing as a result of a growing population and in particular the rising number of people living in southern and coastal areas that are at high risk from natural disasters such as droughts and hurricanes. At the same time, failure to modernise the country's ageing critical infrastructure has meant that it is already starting to fail of its own accord, posing a threat to the supply of essential commodities to the population. Moreover, this creaking infrastructure is no longer suitable for meeting the growing challenges of the 21st century. In many cases, it is forced to operate outside of its original physical performance parameters and is therefore extremely vulnerable even to minor disturbances.[135] The discussions during the workshop made it clear that the same thing could also be said of some parts of Germany's critical infrastructure.[136] In addition, infrastructures such as State schools and the healthcare system are facing major financial problems owing to the growth and ageing of the US population. This in turn means that they will be significantly more vulnerable to extreme events, particularly since they too are affected by the much-cited general trend towards greater complexity and interconnectedness and the resulting increased risk of cascading effects. Furthermore, try as we might to prevent them, risks will always be a part of our lives and it will never be possible to eliminate them completely. The National Academies also cite climate change and the decline of natural "defences" against extreme weather events as further reasons for why it is so important to increase resilience.[137]

In pursuit of these goals, the study initially sets out to establish exactly what is meant by resilience. The authors agreed on the following definition: resilience is the "ability to prepare and plan for, absorb, recover from or more successfully adapt to actual or potential adverse events."[138] The striking resemblance between this definition of resilience and the one used in the "Resilien-Tech" project is no coincidence. In addition to the work of Charlie Edwards (see 3.2.3), Jon Coaffee (3.2.4) and the Swiss Center for Security Studies (3.2.6), the German definition owes a particular debt to the results of the National Academies study. The Americans also use an all hazards approach, according to which adverse events include not only natural disasters but also terrorist attacks, serious instances of organised crime or large-scale industrial accidents. This being said, their findings are almost exclusively based on the analysis of natural disasters such as Hurricane Katrina and their impacts. The researchers do not believe this to be a problem – as far as they are concerned, a key feature

133 ibid., p. 1, 9ff.
134 ibid., p. 11.
135 ibid., p. 11.
136 This point was discussed at length during the "National Perspectives on Resilience" workshop (see Chapter 2). Germany needs roadmaps that reliably describe the physical limitations of technological systems and their maximum capacity.
137 The National Academies 2012, p. 11f.
138 ibid., p. 12.

of resilient societies is their ability to maintain their critical functions or at least restore them as quickly as possible, irrespective of the specific nature of the adverse event (see also the example cited by Gerald Galloway in Chapter 3.2.6). All efforts are geared towards minimising the human and economic impacts of disasters[139] and this is exactly what the characteristics of a resilient nation allow it to do for its citizens. The National Academies describe this in terms of a vision for the year 2030:

- In a resilient nation, a "culture of resilience" exists throughout society, from individuals to the highest levels of government.
- Information on risks and vulnerability is transparent and easily accessible to all.
- Investments and policy decisions with regard to preparedness, mitigation, response and recovery have significantly reduced the human and economic costs of adverse events.
- Regional and local community coalitions are well organised and able to provide support before, during and after a disaster.
- Recovery after disasters is smooth and rapid and includes funding through private capital.
- The average per capita cost of disasters to the U.S. has been declining for a decade.[140]

Transforming the United States into the resilient nation described above in the space of less than two decades will be a huge challenge. Among a whole host of other measures, it will require high and sustained investment in the modernisation of critical infrastructure systems. These will need to be upgraded using innovative and advanced technologies in order to meet the needs of the 21st century. Strategies for increasing resilience should therefore form a fundamental part of the design process of these technologies. Everything that engineers do will have to be rethought in terms of resilience engineering. It will also be necessary to incorporate the core principles of resilience into building codes and other relevant rules, regulations and laws.[141] The pay-off of investing in critical infrastructure resilience is especially high.[142] The National Academies study cites a report by the Multi-Hazard Mitigation Council which found that for every dollar spent on pre-event mitigation related to earthquakes, wind and flooding, about four dollars were saved in post-event damages. By helping to mitigate the damage caused by natural disasters, terrorist attacks or industrial accidents, resilience engineering provides long-term benefits to society.[143] Most of these benefits – i.e. the human lives saved through appropriate prevention, protection and preparedness – cannot be quantified in financial terms. But even those aspects that are financially quantifiable demonstrate that resilience is not just an expensive add-on and must form a fundamental part of future engineering strategies.

The National Academies study frames six recommendations that are outlined in Table 3. The first recommendation concerns the establishment of a systematic database, that documents all types of adverse events on a statistically comparable basis. The systematic compilation and analysis of all this information in a single database allows cost-benefit analyses to be performed so that the case can be made for investing in measures to increase resilience. The second recommendation comes under the heading of a risk management strategy. Since risks cannot be completely eliminated, it is necessary to develop tools to ensure that when adverse events do occur, the damage they cause can be kept to a minimum. This can involve both structural and nonstructural measures. In effect, the third recommendation amounts to the implementation of the second recommendation within communities. Alongside the federal resilience measures that apply nationwide and are mostly derived from the risk management strategy

139 ibid., p. 14.
140 The National Academies 2012, p. 12.
141 The National Academies 2012, p. 13.
142 For more on the business case for resilience, see also the ideas of Jon Coaffee in Chapter 3.2.4.
143 The National Academies 2012, p. 13.

described in the second recommendation, community resilience coalitions should also be established to focus on the local specificities that could constitute obstacles or opportunities in terms of the creation of resilient communities. Recommendations four and five – Organising Principle and Cooperation & Assessment – describe measures that can be taken by the government and federal agencies to make the United States more resilient as a whole. Resilience as an organising principle means that federal government should have an overarching vision of a resilient nation so that it can communicate resilience as a goal in all areas of government and society.[144] In their sixth and final recommendation, the National Academies call for the development of a National Resilience Scorecard. No suitable methods yet exist for measuring the resilience of societies and their subsystems.[145] This is hampering efforts to systematically identify the weaknesses that need to be addressed, evaluate investment costs in terms of their financial benefits and determine how individual measures affect society's resilience. Any successful method of measuring resilience will need to incorporate the all hazards approach, work with systems of different types, sizes and purposes, and integrate all the different dimensions of the concept of resilience. The National Academies argue that this can only be done through a combination of indicators from all the different areas involved in resilience.[146]

During the workshop, Alexandra Eide and Lauren Augustine presented their "Resilience Equation" which provides an excellent overview of the areas that need to be addressed in order to create resilient societies. Figure 7 illustrates how the resilience equation operates in theory and in practice. According to this approach, resilience can only be achieved through a combination of engineering, physical science, protection of critical infrastructure, social science, various aspects relating to public health and good governance. Should the resilience mechanisms in one of these areas fail, society will be unable to respond resiliently to adverse events. Like Susan Cutter, Eide and Augustine chose to use the example of Hurricane

Table 3: National Academies' recommendations for a resilient nation

RECOMMENDATION	DETAILS
1. Database	Establishment of a database that documents all types of adverse events on a statistically comparable basis, allowing cost-benefit analyses to be performed
2. Risk Management Strategy	The design and implementation of risk management strategies including structural measures (resilient building methods, upgrading of existing structures, building codes, etc.) and nonstructural measures (geographical aspects, risk communication, early warning systems, insurance, tax incentives, etc.)
3. Community Resilience Coalitions	The establishment of Public-Private Partnerships and other coalitions with key local organisations in order to increase community resilience through vulnerability analyses, risk communication, resilience engineering of critical infrastructure, etc., all of which should be geared towards the specific local circumstances
4. Organizing Principle	Incorporation of the concept into all the relevant government documents at federal level, resilience as an organising principle
5. Cooperation & Assessment	The relevant agencies should assess their own contribution to the nation's resilience, cooperation should be promoted between the responsible agencies
6. Resilience Scorecard	A combination of technological and social indicators should be developed that together provide a means of measuring systems' resilience, thus allowing different systems to be compared

Source: The National Academies 2012b, pp. 3 – 10, authors' own summary.

144 The National Academies 2012, pp. 3 – 8, for more on the topic of the organising principle, see also Coaffee's observations in Chapter 3.2.4.

145 See also Chapters 3.2.6 and 3.2.7. While there are a number of promising approaches to measuring resilience, there is as yet no consensus on which methods are best.

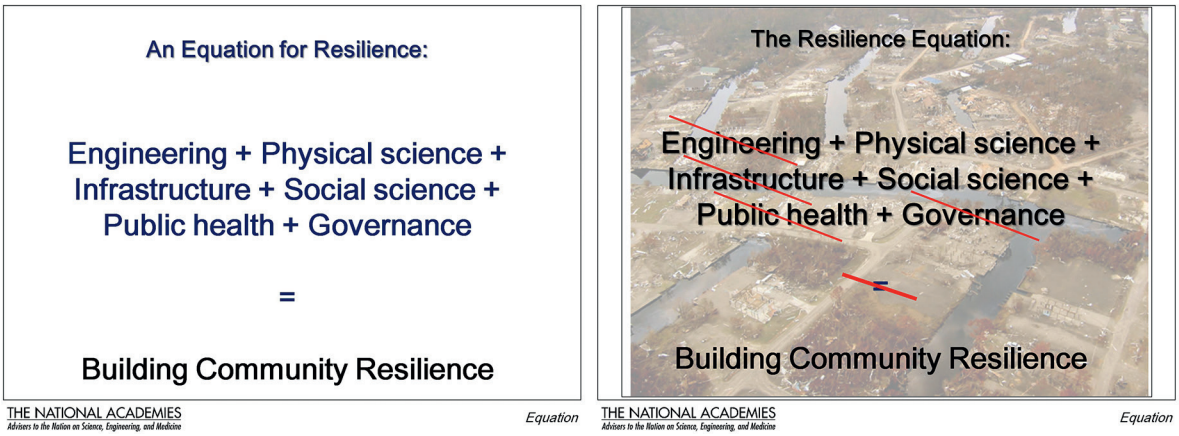
146 The National Academies 2012, p. 10. For more on the issues connected with measuring resilience, see also Chapters 3.2.5, 3.2.6 and 3.2.7.

Katrina. In this case, the early warning systems actually functioned correctly, since the data obtained by physical scientists meant that there was in fact sufficient information about the storm's nature and intensity as well as its likely path. Furthermore, government agencies also had accurate data about social conditions within the city, its demography, the distribution of its inhabitants and the differences in their vulnerability to adverse events. According to Eide and Augustine, however, all the other parts of the equation were not adequately covered and this is why the hurricane ultimately had such a devastating impact. In summary, they argue that a resilient society can only be established by paying equal attention to all the different dimensions, from governance aspects to social science methodologies and the research and development of cutting-edge engineering technologies that incorporate resilience engineering principles. The German resilience debate can benefit enormously from this all-embracing understanding of the concept of resilience and its detailed recommendations for individual areas of society. The outputs of the "Resilien-Tech" project therefore incorporate many of the National Academies' findings.

3.2.3 CHARLIE EDWARDS, UK – RESILIENT NATION

Charlie Edwards is Director of National Security and Resilience Studies at the UK's renowned Royal United Service Institute (RUSI). Before joining the RUSI think tank, he also played a leading role in the development of the UK's CONTEST counter-terrorism strategy which is based on a holistic understanding of resilience. This is, for example, apparent in its chapter headings, which refer to the individual phases of the resilience cycle (with the exception of the Recover phase). The Executive Summary also sets out an unmistakably holistic vision, outlining a counter-terrorism strategy that does not rely exclusively on measures such as increased surveillance. Instead, it addresses all the different phases of terrorism.[147] During the workshop, Charlie Edwards introduced the key ideas contained in his publication "Resilient Nation". The document begins by outlining Edwards' observations on the status quo in an increasingly complex environment, with reference primarily to the UK. He talks of a "brittle society" that has not yet actually broken but which could easily be completely destabilised even by small disturbances. Interconnectedness and complexity could result

Figure 7: The resilience equation in theory and in practice as illustrated by Hurricane Katrina



Source: Presentation by Eide/Augustine at the workshop "International Perspectives on Resilience", Photo right: ©NOAA Remote Sensing Division.

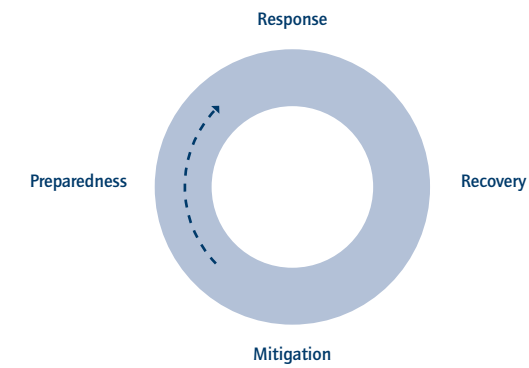
147 HM Government 2011, pp. 3, 9 – 15.

in catastrophic cascading effects and the collapse of the entire system, even if only a small part of the system were to fail.[148]

This is particularly true of the nation's critical infrastructure, more than 85 percent of which is now owned by private, profit-oriented companies. Water, energy, food and other important services are now supplied by the private sector rather than the State. It is therefore vital that the private sector should have a vested interest in guaranteeing security of supply – in other words, it is necessary to make the business case for resilience. Edwards also points out that, paradoxically, people in the UK have never been safer as individuals. They have never been healthier or wealthier and have never had so many tools to help them live better lives. At the same time, however, people's individual fears, complicated lives and high expectations mean that society as a whole feels that it is more at risk than ever.[149] Resilience is key to combatting these risks – later on in the document, Edwards describes how disasters still occur frequently, despite the fact that we live safer lives overall[150]. Edwards understands resilience to mean more than simply the ability to bounce back after a disaster. If the concept of resilience as a characteristic of societies and individuals is to be of any use in addressing the challenges of the future, then it will need to incorporate aspects relating to learning and adaptation.[151] Edwards summarises his understanding of resilience in the following definition: "The capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity."[152]

Based on this definition, Edwards developed a social resilience cycle made up of four stages – mitigation, preparedness, response and recovery (see Fig. 8). As already mentioned in the introductory chapter, Edwards' cycle forms the basis of the resilience cycle used in the "Resilien-Tech" project. Some of the key ideas in our definition of resilience are derived from Edwards' work which is thus hugely relevant to the resilience debate in Germany. This is especially true because Edwards' definition of resilience is neither static nor reactive, criticisms that have both been levelled at the way the term has been interpreted in some quarters in Germany. The close similarity between Edwards' ideas and the definition of resilience used in the "Resilien-Tech" project becomes abundantly clear if we take a look at the four stages of his resilience cycle:

Figure 8: Charlie Edwards' Social Resilience Cycle



Source: Edwards 2009, p. 20.

- Mitigation: this stage is essentially the same as the Prevent and Protect phases of the resilience cycle used in this report. It involves measures geared towards preventing adverse events (as far as possible) together with protective measures that limit the negative impacts of disasters.
- Preparedness: this involves measures for anticipating disasters such as early warning systems, evacuation and emergency plans, threat analyses, emergency exercises and raising awareness about the potential dangers.

148 Edwards 2009, p. 25ff.
149 Edwards 2009, p. 16.
150 ibid., p. 35.
151 ibid., p. 10.
152 ibid., p. 18.

– Response: actions taken during and immediately after a disaster. The focus here is on saving lives and minimising damage. This stage relates primarily to the role of the professional and voluntary emergency services as well as the first people who happen to be present at the scene of a disaster.
– Recovery: rebuilding and restoring a community after a disaster. This stage involves learning from the past rather than simply returning things to their previous state.[153]

During the workshop, Edwards highlighted five characteristics of a resilient nation:

1. An awareness of the risks and dangers that exist and an understanding of their potential impacts.

2. Clear responsibilities and interoperability in the event of a disaster.

3. Close and reliable cooperation between the responsible agencies before, during and after an adverse event.

4. Clear and consistent legislation and regulation on the management of adverse events.

5. Transparency, as well as economical and efficient use of the huge volumes of data and information that are available in the age of big data.

Based on his definition of the concept of resilience and the properties of resilient societies, Edwards concludes his study by recommending implementation of a set of measures that he refers to as the "four Es" – engagement, education, empowerment and encouragement. These are intended to help the UK become a resilient nation.[154]

Engagement is used by Edwards to describe a new level of communication between central government, local authorities, emergency planning officers, the emergency services, etc. and the public. Rather than simply passing on information unilaterally, this involves effective on-the-spot engagement with the people directly affected by disasters. The second E, which stands for education, is in a similar vein. Education is key to the establishment of a resilient society. Every single member of society should, as far as possible, have a basic knowledge of the relevant threats and risks and of how to behave in the event of a disaster, as well as a more specific knowledge of the factors that are relevant to them personally (e.g. geographical factors). Practical examples of how this measure can be implemented already exist e.g. in Essex (see 3.3.2). If people are already well educated about the threats and risks as well as how to behave in the event of a disaster, then they are ready for the third E, which is empowerment. By this, Edwards means measures that enable the people affected by a disaster to take action themselves in order to minimise its negative impacts. One way of doing this can be to arrange emergency planning exercises, especially at local level. The last E stands for encouragement and relates to the more psychological aspects of empowerment. The idea is to encourage members of the public to become actively engaged, thereby contributing to society's overall resilience.

Edwards' conclusions provide valuable material both for the general debate on resilience in Germany and for the specific recommendations of this study. If a society is to become resilient, then so must its citizens. The State can help them do this through engagement, education, empowerment and encouragement. Edwards' four Es describe how this can be achieved in practice. Edwards also made a rather surprising observation during the workshop which could provide a valuable insight for the debate in Germany – he argued that many things actually work extremely well during a disaster. People come to each other's help, early warning systems do

153 ebd., p. 19ff.
154 Edwards 2009, p. 80ff.

what it says on the tin and embankments hold back the flood waters, to name but a few examples. The mere act of talking about the things that work well – without, of course, becoming complacent – is in itself a way of increasing a society's resilience by strengthening its belief in its own abilities.

3.2.4 JON COAFFEE, UK – THE INTERPLAY BETWEEN PHYSICAL AND SOCIO-POLITICAL ASPECTS OF URBAN RESILIENCE

Jon Coaffee is one of the world's foremost experts on the subject of urban resilience. He is Professor in Urban Geography at the Centre for Interdisciplinary Methodologies at the University of Warwick and also runs the web site www.urbanresilience.net, which serves as a platform for sharing research findings and practical examples on the topic of urban resilience. In the blog that appears on this web site, he also addresses e.g. the economic aspects of resilience. He discusses the idea of employing a "dual-use" strategy with regard to measures for increasing resilience. For example, he looks at how structural robustness can provide a defence against both terrorist attacks and natural disasters such as flooding, a feature that can be used as a compelling marketing tool for the relevant buildings or locations. He also explores the idea that measures to boost resilience could result in lower insurance premiums, creating a win-win situation for insurers and policyholders. While the cost of being insured would fall for the latter, the former would also benefit from having to pay out lower average sums on a less frequent basis. This contrasts with the strategy usually adopted by insurance companies, which is not to provide any cover at all for unforeseeable major adverse events in high-risk areas, something that poses a huge problem for people living in coastal areas or flood plains, for example. Another idea that could contribute to the business case for resilience would be to appeal to the social responsibility of private-sector companies. It might be possible to get them to act in a resilience-aware manner through a combination of public pressure and their desire to protect their good name. However, according to Coaffee, this approach runs the risk of lacking transparency and being inherently unsuccessful. Coaffee distinguishes between these three "carrot approaches" and the "stick approaches" enforced by the State, i.e. legislation and regulation. While on the one hand compulsory measures can be criticised for failing to make a genuine business case, excessive bureaucracy means that they are in any case rarely implemented. According to Coaffee – and the United Nations Office for Disaster Risk Reduction, which provides the basis for much of his arguments[155] – in the future cities and regions will inevitably start using resilience as an offensive marketing strategy for attracting investment. In an age characterised by growing vulnerability, resilience may thus offer indirect economic benefits, since businesses will be likelier to locate to and invest in areas that are safer and more secure. This will have the knock-on effect of increasing tax revenue, providing government agencies with funds that can be invested in resilience.[156]

But what exactly does investing in resilience mean? According to Coaffee, the concept of resilience developed as a response to the fatalistic view of a high-risk society. Coaffee argues that a large part of what makes resilience attractive has to do with the fact that it is a positive-sounding term. These positive connotations make it significantly easier to sell the underlying concept to policymakers and explain it to the public, rather than constantly reiterating the growing number of hazards, threats, vulnerabilities and problems to which we are all exposed. National Academies representative Lauren Augustine made a similar case during the workshop. Coaffee, however, also delivers a critique

155 In 2013, the United Nations Office for Disaster Risk Reduction published the third edition of its Global Assessment Report on Disaster Risk Reduction, entitled "From Shared Risk to Shared Value: The Business Case for Disaster Risk Reduction". Coaffee uses the report as a basis for discussing how a business case can be made for the wider urban resilience approach. URL: http://www.preventionweb.net/english/hyogo/gar/2013/en/home/download.html [accessed: 17. 12. 2013].

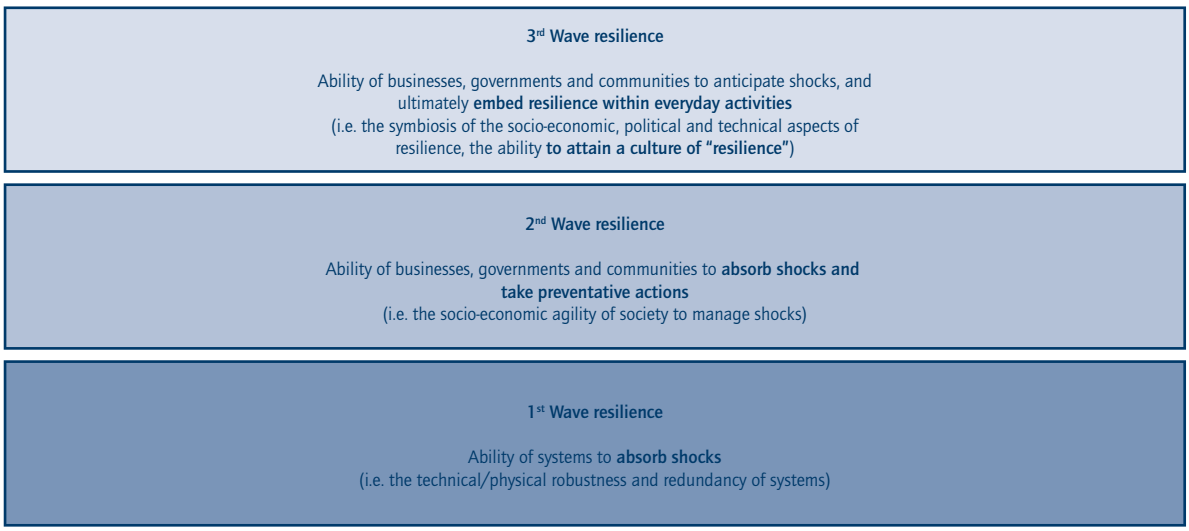
156 Coaffee 2013.

of the term "resilience". What matters to him is the underlying concept. He argues that the decision to use the word "resilience" is politically motivated, meaning that although it may be the term of choice today, no-one knows what we will use to describe the same concept in a few years time. The German debate can take Coaffee's ideas in this regard one step further – the fact that the German term "Resilienz" is an English loan word that is virtually unknown outside of a small community of researchers means that it can be imbued with positive connotations that can themselves help to increase society's resilience. This is in keeping with what Edwards refers to as the need to talk about the things that work well.

Whilst the term's semantic import is all well and good, it is of course the content of the underlying concept that really matters. According to Coaffee, this has evolved from a purely reactive understanding of resilience as the technical robustness and redundancy of systems to an all-embracing interpretation that gives equal weight to the socioeconomic, political and technological aspects (see Fig. 9). Resilience has thus become a kind of organising principle for government policy initiatives, incorporating planning, prevention, holistic threat management, response measures, increased subsidiarity and greater utilisation of modern technologies and data analysis techniques. Moreover, the evolution of the concept does not stop here.

Coaffee believes that a "fourth wave" of resilience is imminent. In the future, the State will no longer be solely responsible for society's safety, security and well-being. Resilience will also need to be promoted at local level through the engagement and empowerment of citizens. Instead of the State using regulation and legislation to create resilience, the emphasis will be on a more

Figure 9: Jon Coaffee's model of the evolution of the concept of resilience



Source: Presentation by Jon Coaffee at the workshop "International Perspectives on Resilience", see Coaffee 2013b.

cooperative approach. Local resilience in local communities will be created by local actors to serve their own local interests – with professional support from government agencies. Coaffee uses the term "responsibilisation" to describe this trend towards citizens taking on greater individual responsibility.[157] His understanding of resilience thus clearly has a lot in common with the ideas outlined in Charlie Edwards' "Resilient Nation". In addition to this focus on the local level, Coaffee also identifies a trend towards the development and marketing of smart technological solutions. As well as phenomena such as big data, software algorithms, sensors and digital technologies, the use of software to record different aspects of our everyday lives and crowdsourcing, this also includes the establishment of intelligent operations centres such as those currently being promoted by companies such as IBM.[158] One example cited by Coaffee during the workshop is predictive crime analysis, which is already being used by some police departments in the US. Data analysis techniques make it possible to predict where crimes are likely to occur, allowing police resources to be deployed more efficiently and effectively. Nevertheless, Coaffee believes that so-called smart technologies are also accompanied by a variety of ethical, moral and legal pitfalls. He describes this approach to increasing urban resilience as "black box urbanism". While the advantages of the technology may be indisputable, there is an urgent need to address unanswered questions about who controls it and who its main beneficiaries are.

In summary, Jon Coaffee recognises and clearly describes both the risks and the major opportunities that are implicit in the concept of resilience. His emphasis on the local aspects of resilience and citizen empowerment at local level could provide a valuable input to the debate in Germany. The term "responsibilisation" is also something that the German debate should analyse and discuss. Equally important were the thought-provoking ideas on the subject of unknown unknowns that he expressed in connection with exceptional, unexpected events such as 9/11 and the Japan tsunami in March 2011, the impact of which was dramatically exacerbated by unforeseen cascading effects. The question he raised in this regard was whether societies should even attempt to prepare for black swan events, given that their unpredictability – particularly in terms of the damage they cause – might require a disproportionately high level of investment.[159]

Coaffee also discusses the connection between the concepts of resilience and sustainability, claiming that "Resilience is the union of sustainability and security, with the former redefined by the latter."[160] While there are undoubtedly those who might wish to challenge this statement, the basic idea that Coaffee is addressing here is extremely important: it is impossible to make a case for resilience without also including sustainability as the central paradigm of social development in Germany. Both goals – a resilient society and sustainable development – must be addressed together. Studies carried out as part of the "Resilien-Tech" project have shown that genuinely sustainable development cannot occur without resilience. It is thus impossible to overstate the importance of resilience as a key component of sustainability (see also 3.4).

3.2.5 WOLFGANG KRÖGER, SWITZERLAND – A RESILIENT CRITICAL ENERGY INFRASTRUCTURE

Since mid-2011, Wolfgang Kröger has served as the Executive Director of the ETH Risk Center in Zürich. While the ETH Risk Center investigates questions that are also addressed

157 Coaffee discusses this idea in detail in: Coaffee et al. 2009, pp. 230–240.
158 IBM 2013.
159 Strictly speaking, it is logically impossible to make explicit preparations for unknown unknowns, since by definition these are events that nobody knows about until they occur. However, it is possible to make general preparations for disasters of all types. These may subsequently help to successfully cope with adverse events that were not initially predicted.
160 Coaffee et al. 2009, p. 262.

by the field of resilience research, it looks at them from a risk-based perspective.[161] Kröger's presentation to the workshop concentrated on the security of Europe's energy infrastructure. He used this specific example to illustrate his views on the concept of resilience in general. The goal of Europe's energy infrastructure networks is to supply society with secure, sustainable and affordable energy. Security refers to the quantity and quality of energy available at any given time. Kröger was able to use the example of our energy supply to vividly illustrate two trends that have already been alluded to several times in this study: the increased vulnerability and growing complexity[162] of the critical infrastructure required for our society to function smoothly. Table 4 lists the major power outages that have occurred in recent years, showing that these blackouts are actually far more common than people realise. According to Kröger, the general public in Europe is completely unaware of just how likely a lengthy, widespread blackout really is. Moreover, the causes of the blackouts are indicative of the fact that systems are becoming more and more complex. Kröger cites the example of a blackout in November 2006 that affected some 15 million households in western Europe. The outage was traced back to the planned disconnection of part of the grid and was ultimately caused by a number of different, interconnected, mutually exacerbating factors, some of which were technical (power grid overload), some of which were natural (high winds), some of which involved human error (inattentive operators) and some of which were organisational (networked system). A major blackout can thus be triggered by relatively minor problems. Kröger argues that this is in part due to the fact that we often use our systems outside of the parameters for which they were originally designed.[163] This means that while terrorist attacks or natural disasters are no longer even necessary to paralyse a system like our energy supply, the damage that they cause to an already vulnerable system can be catastrophic.

Kröger uses networked system modelling techniques to describe the complexity of modern infrastructure and evaluate its vulnerability. These models must be capable of capturing the local interactions between a wide range of interconnected components which combine to create the global system behaviour. They should also be able to cater both for normal operating conditions and for a broad spectrum of exceptions caused by different types of adverse events. Kröger contends that traditional methods based on reductionism and causal chains struggle to cope with these requirements. Nevertheless, Kröger employed a heuristic, model-based approach to simulate the Swiss electricity grid and how it responds to disturbances. The Swiss grid comprises 242 nodes (power plants, substations, consumers) and 310 edges (high-voltage power lines). Simulations were performed both for targeted attacks on important nodes and for random edge failures. The results indicated that the grid would become unstable in the event of targeted attacks on the most important nodes, but did not identify cascading effects as a major threat. The researchers found that the system had unexpectedly large safety margins. Kröger believes that the next stage in modelling this kind of complex system could be to employ agent-based techniques to stochastically simulate all the system's components in order to describe the behaviour of the entire system without resorting to predefined scenarios or system states. The take-home message as far as Germany is concerned is that in order to understand complex systems and take the right measures to increase their resilience, it is necessary to employ innovative modelling approaches using modern network- or agent-based techniques.

The complexity of today's critical infrastructure forms the backdrop to Kröger's definition of the concept of resilience. Resilience can be understood as "the ability of a system or a system-of-systems to resist/absorb initial adverse effects of a disruptive (shocking or creeping) internal or external event/force (stressor) and the time/speed at which it is able

161 ETH Risk Center 2013, 2013b.
162 For more on the term complexity, see also e.g. Al-Khudhairy et al. 2012, p. 574ff.
163 The National Academies 2012, p. 11.

to return to an appropriate functionality/equilibrium." As can be seen from Figure 10, this interpretation of resilience has a lot in common with those of Cutter, the National Academies, Edwards and Coaffee. Although his definition is informed by a technological science perspective, Kröger does not restrict it to the aspects of robustness and redundancy. Instead, he argues that in addition to achieving the fastest possible recovery from a shock, the focus of resilient strategies should also be on adapting, learning and transforming in order to ensure that this recovery is as sustainable as possible. Resilient systems should not only be able to bounce back to their original condition[164] in which they were able to perform an important function for society to at least an adequate standard. Instead, thanks to their inherent ability to keep developing, they should be capable of improving their performance and reducing their vulnerability to future adverse events. In Kröger's view, adverse events include not only one-off disasters but also the creeping decay that affects critical infrastructure as it gets older. In general, he does not believe the physical, technological systems that comprise critical infrastructure to be important in themselves. All that matters is the function

Table 4: Significant major power blackouts in recent years

BLACKOUT		LOSS [GW]	DURATION [H]	PEOPLE AFFECTED	MAIN CAUSES
Aug. 14, 2003	Great Lakes, NYC	~60	~16	50 million	inadequate right-of-way maintenance, EMS failure, poor coordination among neighbouring TSOs
Aug. 28, 2003	London	0.72	1	500,000	Incorrect line protection device setting
Sept. 23, 2003	Denmark/Sweden	6.4	~7	4.2 million	Two independent component failures (not covered by N-1 rule)
Sept. 28, 2003	Italy	~30	up to 18	56 million	High load flow CH-I, line flashovers, poor coordination among neighbouring TSOs
July 12, 2004	Athens	~9	~3	5 million	Voltage collapse
May 25, 2005	Moscow	2.5	~4	4 million	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0.2	~3	200,000 passengers	Non-fulfilment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug. 14, 2006	Tokyo	?	~5	0.8 Mio households	Damage of a main line due to construction work
Nov. 4, 2006	Western Europe (planned line cut off)	~14	~2	15 Mio households	High load flow D-NL, violation of the N-1 rule, poor inter-TSo coordination
Nov. 10, 2009	Brazil, Paraguay	~14	~4	60 million	Short circuit on key power line due to bad weather, Itaipu hydro (18 GW) shut down
March 11, 2011	Northern Honshu	41	days		Grid destruction by earthquake & tsunami/ supply gap

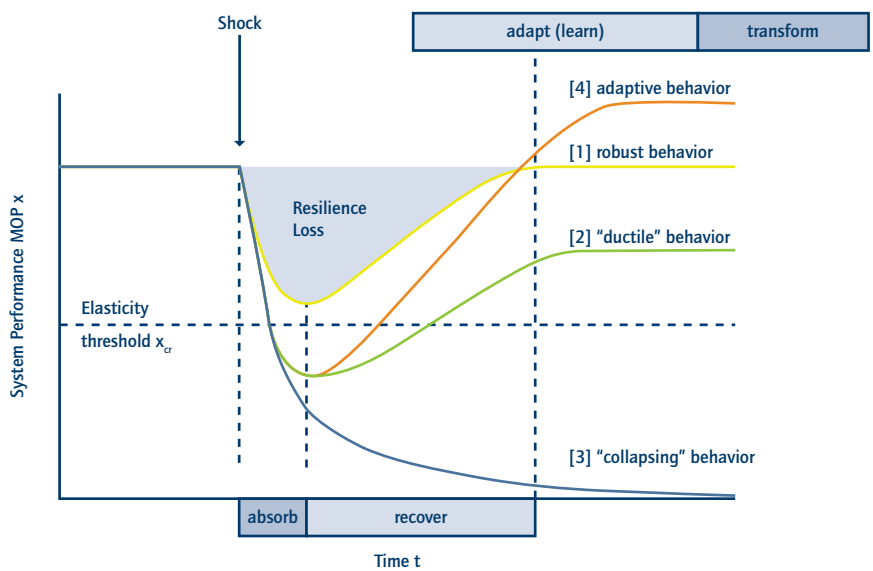
Source: Presentation by Wolfgang Kröger at the workshop "International Perspectives on Resilience" plus author's amendments, see e.g. Kröger 2011, p. 70.

164 This corresponds to the purely technological definition of resilience, see the introductory chapter to this study.

that the infrastructure performs for society. For example, the function of electricity remains the same irrespective of whether it was generated by a hydroelectric, wind-powered, coal-fired or nuclear power plant. The differences that do matter concern its cost, sustainability and security. Depending on what we mean by security, our definition of resilience can be purely technological or can be extended to include socio-technical systems. According to Kröger, the best way of creating resilient critical infrastructure that continues to perform its function for society even in the face of adverse events is to employ socio-technical solutions that integrate and attach equal importance to the technological, economic, social and legal aspects.

Kröger understands resilience as part of the overall concept of vulnerability. We have consciously chosen not to adopt this approach in the "Resilien-Tech" project, preferring instead to use the definition of vulnerability developed by Cutter for the SoVI index. Nevertheless, Kröger has a number of useful ideas that can enrich the resilience debate in Germany. These remain valid even if resilience is not interpreted within the overall context of vulnerability. For example, he repeatedly stresses the need to raise public awareness of the fact that adverse events can and do occur, often causing serious damage. Kröger's emphasis on awareness building is shared by other researchers, including Edwards. Of course, the very act of informing the public

Figure 10: How resilient and non-resilient systems respond to a shock



Four essential patterns, (1) absorbing a shock without collapsing, (2) recovering from a shock to gain structure, functions and essential feedback loops again, (3) adapting through self-organization and learning, and (4) eventually transforming into a different system by altering structures, functions and feedback loops.

Source: Presentation by Wolfgang Kröger at the workshop "International Perspectives on Resilience".

about potential risks and threats also involves shattering the illusion that they live in a completely safe and secure "zero-risk society".

Resilience can be increased through functional, technological redundancy. However, Kröger raises questions about whether we can justify the cost of expensive redundancy measures to safeguard the functioning of technological systems. In view of the fact that financial resources are limited and bearing in mind the conflicts that sometimes arise regarding the efficient use of scarce resources, he makes the case for creating smart redundancies, e.g. at the software rather than the hardware level. As far as the phenomena of complexity and automation are concerned, he does not believe either to be positive or negative in itself, arguing that it is simply a case of striking the right balance. Both too much and too little complexity are to be avoided. Too little complexity leads to inefficient systems that do not function optimally because they fail to leverage the benefits that can be achieved through networking. However, too much complexity can create unmanageable systems that no-one understands and which can thus no longer be meaningfully controlled or used. A level of complexity where everything is connected to everything else is thus also undesirable. For instance, Kröger specifically argues that for reasons of security the public Internet should under no circumstances be used for the critical functions of key infrastructure.

There is no doubt that automation and the replacement of human systems by technological ones can have a positive impact thanks to the greater average reliability of technology. However, in unforeseen one-off situations, only human intelligence and improvisation are capable of rapidly resolving apparently out-of-control situations thanks to our ability to be creative and think out of the box. These are abilities that routine-bound technological systems have (hitherto) been unable to develop to the required degree. This is one of the reasons why Kröger believes that it is essential for the latest scientific discoveries, technologies and models to be implemented in resilient systems. He also argues that it is only possible to achieve resilience by constantly adapting to external change and responding to it in an appropriate – potentially even proactive – manner.

In summary, Kröger believes that the concept of resilience has great potential, but also contends that it requires further development, particularly with regard to the protection and security of critical infrastructure. This is especially true because hardly any techniques currently exist for adequately quantifying or measuring resilience. The ability to quantify resilience is essential so that the resilience of different systems can be compared, allowing them to be more easily optimised. Kröger emphasises that there is still much work to be done in this area, a view that is explicitly endorsed by the authors of this study as far as the German context is concerned.

3.2.6 TIMOTHY PRIOR, SWITZERLAND – POTENTIAL PROBLEMS WITH THE CONCEPT OF RESILIENCE AND ITS MEASUREMENT

Timothy Prior is head of the "Risk and Resilience" research team at the ETH Center for Security Studies (CSS) in Zürich, which investigates aspects of social and technological resilience in the context of disasters and crisis situations. His presentation to the workshop focused on the issue of measuring resilience. His purpose in asking whether resilience can be measured – and if so how – is to find an objective measurement of resilience which, whilst primarily applicable to infrastructure, can also function in the context of society as a whole. This would allow the actors responsible for different areas to efficiently optimise the resilience of the area under their control through benchmarking, learning from others and the deployment of targeted measures. This is a premise that Prior shares with Kröger and indeed with the many other researchers who are investigating ways of measuring resilience. The Swiss emergency planning

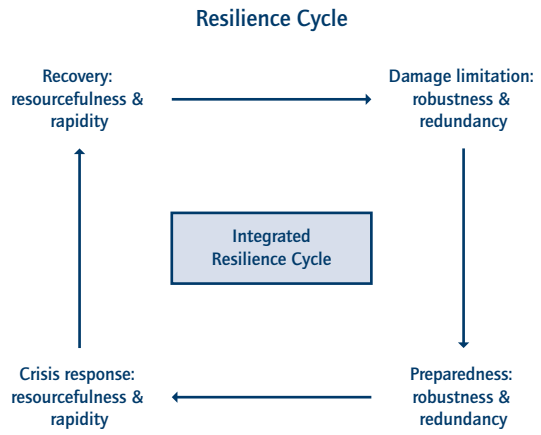
authorities already use the concept of resilience in their plans for protecting critical infrastructure – during the workshop, Kröger alluded to their definition of resilience, which is very similar to his own. The problem, however, is that there is as yet no objective way of determining whether critical infrastructure is resilient and if so to what extent. Prior made the telling point that it is in fact extremely difficult to measure resilience.

Also of interest to the debate in Germany are the findings of a study that were published in a recent article by Prior and Florian Roth in the "Journal of Strategic Security". In an age of growing globalisation and in recognition of the fact that it is increasingly hard to predict when adverse events will occur and how serious they will be, Prior and Roth propose that cities should adopt a double-track strategy. Firstly, cities must improve their capacity to plan for risks and potential adverse events that they would previously not have taken into account. To this end, they should strengthen cooperation between the different emergency planning authorities and other relevant experts. Moreover, the use of advanced system modelling techniques postulated by Kröger can help to identify vulnerabilities so that the appropriate counter-measures can be taken. The second part of the strategy addresses what happens once a disaster has occurred. Preparedness and good planning notwithstanding, it will still not be possible to prevent or even predict every adverse event. However, cities can still (re)act resiliently in the event of an unforeseen major disaster. This requires flexible response strategies that help to activate the potential of the community and the responsible authorities without – as far as possible – being tied to specific types of disaster.[165] One example of this type of resilience was cited by Gerald E. Galloway during the workshop. It involved a major flooding event in a small US town situated near a nuclear power plant. Because of the town's location, regular disaster exercises had been carried out and residents were conscious of the risk that a disaster – albeit a very different type of disaster – might occur. Consequently, when the floods occurred it proved possible to rapidly pool the resources of the two hospitals which were kept open thanks to a robust backup electricity supply. The upshot was that not a single human life was lost as a result of the flooding.[166] This once again highlights the importance of two particular points for the resilience debate in Germany. Firstly, it is absolutely key for the public to be aware that adverse events can and do occur. And secondly, regular rehearsal of what to do in the event of a disaster not only creates this awareness, but also gives people the belief that they are well equipped and prepared to cope with any type of disaster. And the mere fact of believing means that they are to some extent better able to do so.

In addition to Prior's ideas, the work of the CSS at the ETH Zürich is also of great interest to the "Resilien-Tech" project. The Center's analyses and descriptions of various concepts informed much of the content of this study's introductory chapter. In particular, our working definition of resilience owes a substantial debt to the work carried out by the CSS: "Resilience aims to increase the general ability of technological and social systems to endure and regenerate." It is the "capacity of a system or society to cope swiftly with an unexpected disaster or crisis and restore functionality and performance as rapidly as possible."[167] This definition of resilience, which was published in the "CSS Analysis in Security Policy" series, contains many of the concept's key points. The CSS has also developed its own resilience cycle (see Fig. 11) which is similar to the one based on the work of Charlie Edwards that is used in this study. It comprises the four stages of preparedness, crisis response, recovery and damage limitation. The resulting "R4 Framework" features different combinations of the qualities of Robustness, Redundancy, Resourcefulness and Rapidity. These four characteristics are a trademark of highly resilient societies.

165 Prior/Roth 2013, p. 68.
166 The National Academies 2012, p. 28, 2012b, p. 8.
167 Trachsler 2009, p. 1.

Figure 11: The resilience cycle of the Center for Security Studies at the ETH Zürich



Source: Trachsler 2009, p. 2.

Like in Germany, however, the 2009 CSS Analysis found that the concept of resilience has not yet been fully leveraged in Switzerland. This is due to the lack of a common understanding of the term which is consequently only used as a vague way of referring to "a society's basic capacity to overcome a crisis".[168] As a result, in 2011 the CSS carried out an analysis of current international perspectives on the term and concept of resilience. The subsequent report, entitled "Risk Analysis. Resilience – Trends in Policy and Research", addresses almost the same objectives as the "Resilien-Tech" project, albeit within a more limited remit. The focus of the study was to produce a descriptive overview of government programmes and how they use and understand the concept of resilience, together with ideas and projects on measuring resilience.[169] The countries included were the US, the UK, Australia, Canada, Germany, Singapore and Israel.[170] The approaches to measuring resilience came mainly from the US, with one each from Israel and France.[171]

The study found that the US, the UK, Australia, Canada and Germany share a very similar understanding of resilience. There are striking similarities to the definition of resilience used in this study. On the other hand, both Singapore (where resilience is viewed as a desirable national "ideology") and Israel (where the focus is exclusively on counter-terrorism and there is no interest in the all hazards approach) have a completely different approach to resilience.[172]

The study's authors, Corinne Bara and Gabriel Brönnimann, found that the various methods of measuring resilience that they examined could not be compared with each other, since the units of analysis, indicators, methodologies, data and goals of the different indices were all completely different. There was once again a clear difference between approaches that are more concerned with critical infrastructure resilience and those that aim to investigate community resilience. However, since a society's resilience can only be increased if all the relevant social factors work together – as demonstrated by the National Academies' resilience equation and in several other places in this study, it is in principle extremely difficult to find suitable indicators for measuring the resilience of individual subsystems.[173] It is, on the other hand, possible to measure the robustness of energy supply networks or the social vulnerability of communities and social groups. These measurements can provide a basis for implementing measures to increase robustness or reduce vulnerability, both of which can improve society's resilience as long as the effects that the complex interconnectedness of different systems has on efforts to increase robustness or reduce

168 Trachsler 2009, p. 3, own translation.
169 Bara/Brönnimann 2011, p. 5f.
170 ibid., pp. 8 – 24.
171 ibid., pp. 26 – 31, for more on the approach of France's Haut Comité Français pour la Défense Civile, see 3.2.7.
172 ibid., p. 25.
173 Bara/Brönnimann 2011, p. 32f.

vulnerability are recognised and taken into account. Other problems with measuring resilience include difficulty in accessing the relevant data, the question of whether resilience is more a behaviour than a state, the key aspect of adaptation and learning – how do we gauge whether the system's new state after a disaster is better or worse than the previous status quo? – and the fact that resilience also emerges from the relationships between subsystems, meaning that resilient subsystems do not necessarily create a resilient overall system and vice versa.

However, despite all these problems, Bara and Brönnimann do not argue that the search for appropriate indices for measuring resilience should simply be abandoned. Instead, they propose taking a step back and making greater use of inductive methods to gain a better understanding of the features of individual societies that comprise resilient behaviour. Examples where it is obvious from the affected system's response that it possesses a high level of resilience should be systematically investigated in the form of case studies in order to identify common factors that could be responsible for the system's resilient behaviour.[174]

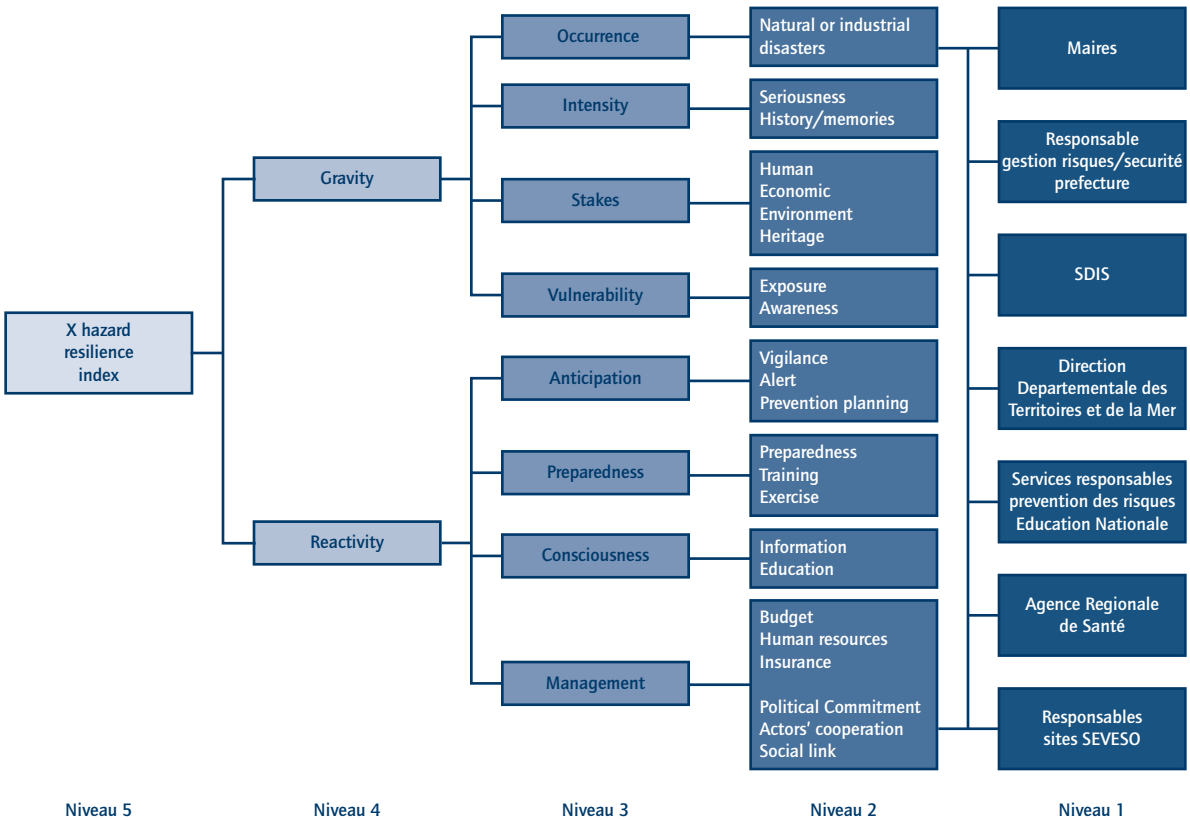
3.2.7 CHRISTIAN SOMMADE & LÉO MULLER, FRANCE – TERRITORIAL RESILIENCE INDEX

Christian Sommade and Léo Muller of the Haut Comité Français pour la Défense Civile (HCFDC) gave a presentation to the workshop on the HCFDC's Territorial Resilience Index. The Index, which is based on the outcomes of a pilot study, aims to provide information on those aspects of resilience that can be realistically measured. Now employed as the HCFDC's Executive Director, Sommade has 25 years' previous experience in the security and defence industry where his work focused mainly on CBRN defence and crisis management. Muller led the HCFDC study that developed the Territorial Resilience Index. The HCFDC is an independent think tank headquartered in Paris that conducts research on security issues and resilience. It also acts as platform for dialogue between its elected members, experts, industry, members of the public and infrastructure operators.[175] In addition to conferences, Webinars and monthly breakfast debates in the French Senate on global and civil security issues, the HCFDC also offers year-round 250-hour courses on "Resilience and Societal Security".[176] The HCFDC also awards the "Pavillon Orange pour la Sauvegarde des Populations" (Orange Flag for Public Protection) to towns, cities and communities that fulfil the relevant criteria. The data are obtained via an online questionnaire comprising 350 questions. One of the key criteria is the extent to which the town or community has formulated and implemented local civil defence plans.[177]

The goal of the Territorial Resilience Index project that was presented at the workshop is to develop a pilot index for the region of Brittany. The project is funded by the French Ministry of Ecology and Sustainable Development. Brittany was chosen for the study because it is at high risk from natural disasters and industrial accidents.[178] The aim of the index is to measure territorial resilience, i.e. the societal resilience of a given geographical unit. The HCFDC researchers define societal resilience as follows: "Means and actions a society uses at the collective and individual level in order to be able to prevent and withstand disasters and aggressions of all kind with the less damage on the functioning of the society [sic]. It would also permit society to adapt or reconstruct itself. It implies risks and threats awareness, prevention and preparation planning, straightness of the behaviours, psychological strength and sense of general interest." The Territorial Resilience Index is a qualitative way of measuring the impact of

174 ibid., p. 34ff.
175 UNISDR 2013.
176 HCFDC 2013b.
177 HCFDC 2013.
178 Bara/Brönnimann 2011, p. 28.

Figure 12: Structure, variables and indicators of the Territorial Resilience Index



Source: Presentation by Sommade/Muller at the workshop "International Perspectives on Resilience", © HCFDC.

an adverse event (natural disaster or industrial accident) on the people, economy, environment and cultural heritage of a particular region. To this end, the index was developed by studying existing plans and programmes in the areas of emergency planning, risk management and risk communication, available types of insurance cover for this kind of damage, etc. Eight societal resilience variables were identified and various indicators were chosen to measure them.[179] Figure 12 depicts the structure of the Territorial Resilience Index. An online questionnaire provided the basis for establishing the values of the 20-plus indicators. This data was obtained from the relevant local stakeholders, e.g. local mayors and emergency planning officers. The online questionnaire systematically structures what are at first sight rather disparate factors, ranging from the seriousness of past disasters to emergency planning budgets and disaster exercises and training. This approach does mean that the quality of the data used for the Territorial Resilience Index is dependent on the subjective evaluations of local leaders. Nonetheless, the methodology subsequently employed by Sommade and Muller's team

[179] ibid., p. 28f.

constitutes an extremely interesting approach to measuring resilience that could prove valuable to the debate in Germany. Once the individual values for the different indicators have been collected, they are grouped together under the eight variables that have already been alluded to. These variables are Occurrence, Intensity, Stakes, Vulnerability, Anticipation, Preparedness, Consciousness and Management. The first four are then combined under the category of Gravity, while the last four are grouped together under Reactivity. The scores for all the different indicators are added together (maximum score 100, minimum 0) to allow gravity and reactivity scores of between 1 and 5 to be derived. The final step is to compare these two scores. If the reactivity score is higher than the gravity score, the entity in question can be said to be resilient to adverse events. If the scores are equal, then the entity is capable of coping with known hazards but lacks the resources and buffers to successfully withstand unforeseen threats. If the gravity score is higher than the reactivity score, the entity has little or no resilience to adverse events and the impact of any disasters is likely to be extremely serious. The Territorial Resilience Index expresses these qualitative predictions as a score between 5 (very resilient) and 1 (not resilient) for each of the three types of hazard included in the study (meteorological, geological and industrial hazards). The definition of a score of 4 (resilient) is particularly unusual. If the reactivity score is one point higher than the gravity score, then the entity in question is rated as resilient, while it is rated as very resilient if it is two points higher. However, if the reactivity score is three or even four points higher than the gravity score, the entity is only rated as resilient rather than very resilient. This rating system is based on a very revealing insight. Some towns or communities that have hardly been affected by adverse events in the past have low vulnerability vis-à-vis future disasters and would probably suffer very little human and economic damage or other impacts if a disaster did occur. If they nonetheless also have a very high reactivity score, then they are obviously not making optimal use of the available resources. Rather than resilience simply requiring sufficient resources to be deployed, it is thus also important that these resources should be deployed in the correct manner. Given that the HCFDC approach sets out to measure resilience to specific hazards, in some communities a score of 4 could indicate that they may be concentrating on the wrong hazard and that it would be more effective to redirect their resources elsewhere.[180]

One major advantage of this complex approach to measuring resilience is that it provides an absolute yardstick. The people who fill out the online questionnaire are asked to evaluate the risks, procedures, budgets, etc. in their own administrative unit, without reference to the scores of any other units. This means that it is possible to assess the resilience of individual units independently of the larger statistical population. However, as described above, this advantage is offset by the subjectivity of the data. For instance, the likelihood of a forest fire occurring in a particular region could be assessed completely differently by two different people. In fairness, the fact that it is experts who are asked to score the indicators as opposed to lay people with no experience in this area means that this criticism is only partly justified. Moreover, the Territorial Resilience Index provides an innovative approach in its implementation and systematic scoring of different dimensions of the concept of resilience. The Index includes evaluations of the damage caused by past adverse events, assesses vulnerability, appraises the at-risk (human, economic, cultural and environmental) factors and evaluates preparedness measures, risk communication and the resources available for civil defence. The fact that a qualitative approach is used means that the researchers can compare the different dimensions by asking the opinions of the local stakeholders, notwithstanding all the problems that this approach entails.

[180] At first sight, it might appear that this is at odds with the "holistic" approach to resilience that is characterised by the capacity to withstand and adapt to any kind of adverse event. However, while some general counter-measures are equally applicable to natural disasters, terrorist attacks, industrial accidents, etc., protection against specific threats such as flooding obviously also calls for additional measures that are different to those needed to protect against a chemical factory explosion, for example. As such, resilience also implies the capacity to take the right measures in the right place at the right time.

Overall, the Territorial Resilience Index can be considered a promising method for measuring resilience. It will be possible to address some of its methodological and scientific shortcomings during the remainder of the project. Furthermore, these shortcomings need to be weighed up against the huge benefits that this approach to measuring resilience can deliver in certain situations. Whilst this does not make the criticisms any less valid, it does constitute a strong argument for nevertheless continuing to use the Territorial Resilience Index in spite of them. Having demonstrated its value in the pilot project, the hope is that the Index will be extended to the whole of France.[181]

3.3 RESILIENCE POLICY – SELECTED EXAMPLES OF GOVERNMENT RESILIENCE STRATEGIES

This section will outline three examples of how a holistic approach to resilience has been implemented in government policies and official documents as well as assessing the extent to which they can act as a model for Germany. The three examples are the US Presidential Policy Directive 21 on "Critical Infrastructure Security and Resilience", the initiatives undertaken by Rosanna Briggs at Essex County Council in the UK – including a brief overview of the relevant UK resilience strategies – and the work of Erik Thomassen at the Norwegian Directorate for Civil Protection.

3.3.1 USA – PRESIDENTIAL POLICY DIRECTIVE 21: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

In February 2013, the White House published Presidential Policy Directive 21 on "Critical Infrastructure Security and Resilience." Presidential Policy Directives (PPDs) are an instrument used by the US President to promulgate his decisions on national security matters.[182] The majority of PPDs are not published owing to the sensitive nature of their content. PPD 21 is complemented by PPD 8 on "National Preparedness", which addresses resilience to all types of hazards.[183] PPD 21, on the other hand, focuses specifically on the resilience of national critical infrastructure. Its goal is to establish a national partnership to guarantee the security, functionality and resilience of critical infrastructure in the US: "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. [...] U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency."[184] In PPD 21, the White House describes the general responsibilities that fall primarily under the remit of the Department of Homeland Security (DHS), as well as assigning concrete tasks to the DHS and providing it with guidelines on how to proceed. The document also lists the individual critical infrastructure sectors and the Sector-Specific Agencies (SSAs) that are responsible for them, as well as providing definitions of the key terms.[185]

PPD 21 defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[186] The striking similarity to the National Academies' definition shows that, in the US, research findings relating to the concept of resilience directly inform official government documents. This impression is reinforced by the use of an all hazards approach for describing the potential hazards and adverse events facing critical infrastructure. PPD 21 defines hazards as any

181 Bara/Brönnimann 2011, p. 28f.
182 FAS 2013.
183 The White House 2011, p. 1.
184 The White House 2011, p. 2.
185 ibid., pp. 1 – 12.
186 ibid., p. 12.

conceivable adverse event – from natural disasters, acts of terrorism and industrial accidents to organised crime, cyber-attacks, pandemics and sabotage. It furthermore defines critical infrastructure as infrastructure so vital to the United States that any impairment of its functionality would have a debilitating impact on "security, national economic security, national public health or safety, or any combination of those matters".[187] It is essential to ensure that critical infrastructure is resilient in order to prevent this type of damage from occurring. The responsibility for so doing is shared by a variety of government agencies at federal, state, local, tribal and territorial levels – chief among them the DHS –, as well as the owners and operators of the relevant infrastructure.

PPD 21 also assigns specific roles and responsibilities to each of these agencies and to various ministries such as the Department of Justice. The DHS has a coordinating role that involves monitoring the activities of the Sector-Specific Agencies and coordinating their work. The responsibilities of the DHS and/or the Secretary of Homeland Security include the following:

> *"[T]he Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure."*[188]

In their respective sectors, the SSAs are responsible for cooperating with the DHS, collaborating with the critical infrastructure operators, implementing disaster management measures should an adverse event occur, carrying out specific vulnerability analyses and acting as the official point of contact for their sector. Other Federal Departments are also attributed specific responsibilities – for example, the Department of State is responsible for ensuring the resilience of critical infrastructure located outside the borders of the United States, while the Department of Justice, including the Federal Bureau of Investigation (FBI), takes the lead on counter-terrorism and the Department of the Interior is accountable for the resilience of national monuments such as Mount Rushmore.[189]

After defining the respective responsibilities, the White House goes on to describe the strategic imperatives that make PPD 21 necessary in the first place. These are 1) to refine and clarify the relationships within the Federal Government that are key to strengthening critical infrastructure resilience, 2) to enable efficient information exchange between the responsible agencies by identifying baseline data and systems requirements and 3) to implement an integration and analysis function to enhance future decision-making regarding the development of critical infrastructure.[190] In order to address these strategic imperatives, PPD 21 sets out six actions to be implemented by the DHS within the specified timeframes:

1. Description of the responsibilities and relationships within the DHS and across the Federal Government related to national critical infrastructure security and resilience. This should include a description of the roles and functions of the two new National Critical Infrastructure Centers[191] that are to be established (within 120 days of PPD 21 coming into force).

187 The White House 2013, p. 11f.
188 ibid., p. 3.
189 The White House 2013, p. 4ff.
190 ibid., p. 2, 6f.
191 One for physical infrastructure and another for cyber infrastructure.

2. Analysis of the existing public-private partnership model in the critical infrastructure sector and recommendations for improving its effectiveness (within 150 days).

3. Identification of baseline data and systems requirements to enable efficient information exchange between government agencies (within 180 days).

4. Development of a situational awareness capability for critical infrastructure. This should enable detection of vulnerabilities, threats, potential cascading effects, etc., as well as allowing this critical information to be disseminated as rapidly as possible to the emergency services, thereby helping to save lives and maintain the system's functionality (within 240 days).

5. Update to National Infrastructure Protection Plan (within 240 days).

6. Formulation of a "National Critical Infrastructure Security and Resilience R&D Plan" detailing the research and development investments required in order to make the United States' critical infrastructure resilient (within two years).[192]

The content of the sixth action that PPD 21 requires the DHS to perform is of particular interest to the "Resilien-Tech" project. This is because it is also the remit of "Resilien-Tech" to develop recommendations for policymakers regarding how the concept of resilience can be incorporated into future security research programmes and implemented in a resilience by design approach. PPD 21 stipulates that R&D should be promoted with regard to highly specific topics in the area of critical infrastructure. These include researching the resilient design and construction of critical infrastructure and enhancing existing modelling techniques through new research initiatives in order to simulate and investigate the impacts of adverse events on critical infrastructure, particularly in terms of cascading effects. In addition, support is to be provided to initiatives that incentivise investment in cybersecurity and resilient critical infrastructure design. Finally, R&D should also help to support and expand the strategic guidance role of the DHS.[193] These aspects of PPD 21 demonstrate that the US is some way ahead of Germany in terms of the implementation of resilience in specific government documents and the actions derived from them, for example strengthening support for R&D in the field of critical infrastructure resilience. As far as the debate in Germany is concerned, it is thus important to underline the necessity of incorporating similarly concrete recommendations into future government programmes, in order to ensure that R&D investment can subsequently be targeted at the relevant needs.

3.3.2 ROSANNA BRIGGS, UK – ESSEX, BUILDING COMMUNITY RESILIENCE WITH CHILDREN

Rosanna Briggs is Deputy Head of Civil Protection and Emergency Management at Essex County Council in the UK. All of the activities carried out by the Essex Civil Protection & Emergency Management Service (ECPEM) are based on the 2004 UK Civil Contingencies Act[194], details of which are outlined below. The fact that the UK as a whole is now the undisputed world leader with regard to the implementation of the holistic resilience approach in government programmes and guidelines for coping with all types of adverse events can be traced back to the Civil Contingencies Act. Since the Act came into force, there have been a variety of government documents and actions aimed at increasing the resilience of society in the UK. Even a small and by no means exhaustive overview of these documents is enough to provide a useful idea of what has been done. The UK government has bought into the holistic resilience approach as the right strategy for

192 The White House 2013, p. 8ff.
193 The White House 2013, p. 8.
194 Parliament of the United Kingdom 2004.

successfully coping with all types of adverse events and is now looking at ways of putting it into practice. In addition to critical infrastructure resilience, great importance is also attached to creating community resilience and to ensuring business continuity in the event of a disaster. The key documents include the following:

- A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010
  Increasing the UK's resilience to adverse events is one of the eight key national security tasks outlined in the National Security Strategy.[195]
- Sector Resilience Plan for Critical Infrastructure 2010
  This report documents the vulnerability, current status, existing measures to increase resilience and further work needed for all critical infrastructure sectors in the UK, from water and energy to financial services.[196]
- Community Emergency Plan Toolkit, 2011
  This document is a guide designed to help people produce Community Emergency Plans with a view to increasing community resilience.[197]
- CONTEST. The United Kingdom's Strategy for Countering Terrorism, 2011
  The concept of resilience underpins the UK's counter-terrorism strategy. This document addresses all the different stages connected with terrorism, including its origins in the radicalisation of disillusioned young people, technical measures for preventing attacks and reducing their impact, first-class training for the emergency services and raising awareness among the public for situations where attacks cannot be prevented.[198]
- Keeping the Country Running: Natural Hazards and Infrastructure. A guide to improving the resilience of critical infrastructure and essential services, 2011
  A general overview of the concept of resilience in the context of critical infrastructure, as well as of the UK's critical infrastructure and how it can be made resilient.[199]
- Preparing for Emergencies: Guide for communities, 2011
  A guide and resource for local leaders, explaining how community resilience can be increased, what it means and what its benefits are.[200]
- Strategic National Framework on Community Resilience, 2011
  A national strategy describing how community resilience should function at a local level.[201]
- The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world, 2011
  Resilience to cyber attacks is one of the Cyber Security Strategy's four strategic goals to be accomplished by 2015.[202]
- A Summary of the 2012 Sector Resilience Plans, 2012
  An update of the 2010 sector resilience plans for critical infrastructure. Owing to their sensitive nature, the details of the plans are classified and unavailable to the public. However, this can in itself be seen as a security measure that enhances resilience.[203]
- National Risk Register of Civil Emergencies. 2013 Edition
  An overview of the threats and hazards facing the UK. The Register provides leaders with a tool to help them prepare for specific potential threats.[204]

195 HM Government 2010, p. 33.
196 Cabinet Office 2010, p. 5ff.
197 Cabinet Office 2011, p. 2.
198 HM Government 2011, pp. 3, 9-15.
199 Cabinet Office 2011b, p. 5ff.
200 Cabinet Office 2011c, p. 2f.
201 Cabinet Office 2011d, p. 3.
202 Cabinet Office 2011e, p. 8.
203 Cabinet Office 2012, p. 4.
204 Cabinet Office 2013.

– How prepared are you? Business Continuity Management Toolkit
  A guide and resource for implementing business continuity measures in enterprises.[205]

These documents and plans are produced by different government agencies, for example the Civil Contingencies Secretariat[206] and the Centre for the Protection of National Infrastructure (CPNI).[207] There are also various regional and local government organisations that are pursuing resilience strategies, for example the London Resilience Team[208] with its London Strategic Emergency Plan[209] and indeed the Essex Civil Protection & Emergency Management Service with its Essex Resilience Forum (see below).[210] All of these documents have their origins in the Civil Contingencies Act.

The Civil Contingencies Act was passed by Parliament in 2004 in response to the impact on the UK of what came to be known as the "three Fs". The three Fs refer to the protests surrounding sharp hikes in the price of fuel and the associated knock-on effects in the year 2000 (fuel crisis), the floods that hit the UK in the same year (flooding) and the foot-and-mouth outbreak in 2001 (foot-and-mouth disease). These events led to the recognition within the UK government that its current emergency planning provisions were obsolete and unsuitable for modern civil defence initiatives. This eventually resulted in the Civil Contingencies Act being passed three years later. The Act is divided into two parts. The first part addresses local emergency planning arrangements and responsibilities, while the second concerns the special emergency powers granted to the emergency services during the most serious emergencies in order to ensure that they are able to respond efficiently, effectively and rapidly.[211] The Civil Contingencies Act defines an emergency as an event that threatens serious damage to human welfare or the environment, or phenomena such as war and terrorism which pose a general threat to national security. The first part of the Act relates to events confined to a restricted local area within the United Kingdom, whereas in the second part, the term "emergencies" only refers to events capable of causing damage at regional level or above.[212]

The first section of the Civil Contingencies Act serves as a guideline for the relevant actors at local level. It defines clear responsibilities and assigns the tasks that the different actors must perform in the event of an emergency. To this end, it divides the actors into Category 1 and Category 2 responders. Category 1 relates to the core responders in the emergency services and government who have a direct role to play in all types of emergencies. These include the police, fire service and ambulance and healthcare services, as well as local authorities, mayors and county council officers.[213] The Civil Contingencies Act requires these actors to perform a variety of different duties, including the establishment of local resilience forums:

– assessing the risks and analysing threats at local level,
– producing and implementing emergency plans,
– producing business continuity management plans,
– informing the public about risks, hazards, how to behave in the event of an emergency, preparedness measures, etc.,

205 HM Government, n.d., p. 4.
206 Gov.uk 2013.
207 CPNI 2013.
208 The London Resilience Team 2013.
209 The London Resilience Team 2010.
210 ERF 2013.
211 Cabinet Office n.d., p. 2; Parliament of the United Kingdom 2004, pp. 1f, 12.
212 ibid., p. 2f.
213 ibid., p. 7.

– sharing information with other local responders,
– cooperating and coordinating with other local responders,
– providing business continuity management advice and assistance to businesses and voluntary organisations (local authorities only).[214]

Category 2 responders are mainly critical infrastructure operators such as energy providers, water and telecommunications companies, airport and public transport operators, etc.[215] They will only be impacted by adverse events of a certain scale if the disaster affects their own particular sector. Their duties are therefore confined to co-operating and sharing relevant information with the other relevant responders.[216]

The first part of the Civil Contingencies Act is of far greater practical relevance to "normal" emergencies than the second part. Of the seven duties that this part of the Act attributes to local responders, Rosanna Briggs' contribution to the workshop focused on the public information aspect. According to Briggs, a key part of building community resilience is to raise public awareness of the relevant hazards and risks. In her view, it is especially important to target children and young people. As a result, ECPEM has carried out two EU-funded projects to develop teaching materials and methods aimed at raising awareness among schoolchildren of all the things that could happen and how best to respond to them. The suitability of these materials and methods was then tested on site in schools through a series of four case studies. Briggs found that the children's knowledge of the risks and of how to behave in the event of an emergency increased significantly and that they also passed this knowledge on to their parents and other family members. Furthermore, extensive media coverage of the studies ensured that their findings reached an even wider public audience. Concerns that the specific teaching content might cause panic or fear among the young people proved to be unfounded. After the successful completion of the EU-funded projects, Briggs continued to develop her methods for training and educating children and young people about the risks of disasters and the correct way to behave before, during and after an emergency. A web site has recently been launched at http://www.whatif-guidance.org, featuring games, jigsaws, books and other simple learning materials regarding how to behave in the event of a disaster.[217] This focus on educating and training children and young people would appear to be an extremely promising strategy. Briggs herself demonstrated its potential by highlighting the difference in the attitudes of children and adults. While adults will tend to say "If only I could …", children will ask "What if …?". The experience of Essex County Council only serves to underline the fact that systematic public awareness-raising from an early age is also important in a German context.

3.3.3 ERIK THOMASSEN, NORWAY – RESILIENCE AS A FUNCTION OF GOVERNANCE

Erik Thomassen is Head of the Analysis Unit at the Norwegian Directorate for Civil Protection (dsb). The dsb reports to the Norwegian Ministry of Justice and Public Security and is responsible for cross-sectoral coordination of government initiatives in the fields of safety and security. The main duties performed by Thomassen's group are the production of the annual Norwegian National Risk Assessment and of vulnerability analyses of Norway's critical infrastructure. During the workshop, Thomassen gave a presentation on the Norwegian government's approach to and implementation of the concept of resilience. He defined a resilient society as "a society with decentralized responsibility focusing

214 Cabinet Office n.d., p. 3f.
215 ibid., p. 8.
216 ibid., p. 4.
217 The "Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)" (Federal Office of Civil Protection and Disaster Assistance) is already pursuing a similar strategy, e.g. through the web site http://www.max-und-flocke-helferland.de [accessed 14.12. 2013].

on reducing the impact of 'tight couplings'[218] in order to maintain basic production and services under all kinds of circumstances." The concepts of governance, functions and maintaining functionality are key to his understanding of resilience. Thomassen understands governance as actions that can be taken by governments and government agencies to encourage society to become resilient by decentralising responsibility. The functions that he is alluding to involve the supply of essential goods and services to the public. For example, critical infrastructure is only critical to society because of the functions it performs. According to the Norwegian understanding of resilience, maintaining functionality in the face of adverse events is thus the key characteristic of resilient systems. One way of achieving this is via redundancy, an approach also advocated by Perrow for preventing normal accidents in complex systems.[219] Since government is itself unable to perform most of the functions that are critical to society, its role must be to ensure that private owners and operators of critical infrastructure are fully aware of their responsibilities and to provide them with support in the fulfilment of their duties. The first step is to clarify which functions are critical and who provides them. The approach taken by the Norwegian government is that infrastructure is considered critical if its failure would threaten the critical social functions of society. Social functions are critical if their failure would prevent essential social needs from being met. These essential social needs are food, water, energy, security, etc. Since the term "security" in particular is not specific enough to allow concrete actions to be derived from this approach, the dsb undertook a study to identify critical social functions, some of which are fulfilled by the private sector (food, drinking water, heating, etc.) and some by the State (national security, law and order, etc.). The dsb uses the resulting list as a basis for carrying out reviews and audits to assess the resilience initiatives undertaken by the individual departments of the Norwegian government and the agencies that report to them. The goal of all these efforts is to ensure that business continuity measures[220] are initiated by companies and measures to increase resilience are also taken by the State. In terms of their content, Thomassen highlighted the issue of redundancy during the workshop, as already mentioned above. With regard to the specific area of critical infrastructure – something that is not really included in most of the areas that fall under the government's responsibility, such as national security, the democratic rule of law, etc. – he concludes that the role of government and government agencies is to produce regulations, ensure that they are complied with and set targets.

3.4 LESSONS LEARNED – STEPS FOR CREATING A RESILIENT SOCIETY

In late May 2013, just two weeks after the workshop "International Perspectives on Resilience" had brought together some of the world's foremost experts on resilience in Berlin, Central Europe was hit by some of the worst floods in its

218 The term "tight couplings" is taken from sociologist Charles Perrow's seminal 1984 work "Normal Accidents. Living With High Risk Technologies" (see Perrow 1999). Perrow uses a series of case studies, including the accident at the Three Mile Island nuclear power station in March 1979, to analyse how the complexity of technological systems leads to system failure and accidents. Perrow can be accused of having a pessimistic view of the potential of technological development (Whitney 2003, p. 1ff). He argues that the complexity of technological systems such as nuclear power stations makes them inherently vulnerable. Tight couplings – i.e. close linkages between the individual parts of a system, resulting in a high risk of "contagion" in the event of a disturbance – mean that total system failure is inevitable at some point. They are roughly equivalent to the cascading effects referred to in this study. Since the system failure is both unforeseen and unforeseeable in terms of its specific nature, the responsible actors are unable to respond adequately to it, thereby further hastening the system's collapse. Perrow refers to accidents caused by tight couplings and complexity as "normal accidents" – in his original work, he argued that this type of accident is impossible to prevent (Rijpma 1997, p. 16). He would subsequently look at ways of creating more stable systems using decentralisation, redundancy and robustness, although he himself considered such measures to be inelegant and contrary to the principles of engineering (Perrow 1999b, p. 150ff).

219 Perrow 1999b, p. 150ff.

220 Business continuity is discussed in detail in Chapter 4 of the Resilien-Tech study.

history. In Germany alone, eight people lost their lives and hundreds of thousands suffered damage to their property, while the Munich Re Group put the total financial cost at over twelve billion euros.[221] The almost unprecedented scale of the flooding was thrown into focus when the water level of the Danube at Passau passed 12.5 metres for the first time in 500 years.[222] Coming as it did right in the middle of the "Resilien-Tech" project, this extreme flooding event provided a dramatic illustration of the fact that a holistic strategy for coping with disasters of this kind is just as important in Germany as anywhere else in the world. Recommendations for policymakers based on a better understanding of the concept of resilience could help to significantly reduce the death tolls and financial, social and environmental cost of future natural disasters, terrorist attacks, industrial accidents and other extreme events. The floods brought home the fact that minimising the impact of these events on the well-being of those affected – through prevention, preparedness, protection, appropriate crisis response measures and learning the right lessons from the past – is at the very heart of the question of what makes a resilient society.

This chapter has sought to provide answers to this question by carrying out a thorough review of international perspectives on the concept of resilience. The research initiatives and practical examples of leading experts that were described in sections 3.2.1 to 3.2.7 and 3.3.1 to 3.3.3 also addressed a number of additional, subordinate questions: What kind of resilience strategies are already being implemented in selected countries? What approaches have been developed for quantifying resilience? What do the experts regard as the main unanswered questions in the field of resilience research? What are the areas where further research is required? In view of the near-exponential growth in the complexity of our high-tech world, what are the most promising resilience strategies, i.e. the ones that are likeliest to be sustainable over the longer term? It is clear from this candid look at the different research programmes and practical initiatives that are being undertaken under the banner of resilience in Europe and North America that the German resilience community of researchers, practitioners and policymakers can benefit enormously from the experience and ideas of its international counterparts.

Each of the previous sections concluded by picking out the most important, innovative or unusual ideas and approaches from the different projects and outlining their potential value to the debate in Germany. The next section will summarise these findings in the form of nine lessons learned. The main aim of the "Resilien-Tech" project is to produce practical recommendations that can be incorporated into future research programmes and strategies in Germany. The lessons learned that are outlined below range from the repeatedly emphasised importance of adopting a holistic approach to resilience to the need for resilience engineering and the conclusion that resilience should always form an indispensable key component of sustainable development. These lessons complement the findings of Chapters 2 and 4. Taken together, they can provide a basis for formulating direct, concrete and meaningful recommendations for decision-makers in government, industry, the research community and civil society.

1. The Resilience Equation: resilience as a holistic concept

The first lesson to be learned from the international perspectives on resilience was in fact also the starting point for the "Resilien-Tech" study: resilience is a holistic concept geared towards improving the ability of societies to keep functioning, adapt, endure and learn in the face of all types of adverse events. This holistic approach is the key benefit that resilience can provide in the context of security research. The question, however, is exactly what is meant by a holistic approach. All of the research programmes and practical examples examined in Chapters 3.2 and 3.3 highlighted the holistic dimension of resilience. Despite the genuinely

221 Badische-Zeitung.de 2013, FAZ.NET
222 Guyton 2013.

different backgrounds, methodologies and theories of the various researchers and practitioners, they all agreed on one thing: irrespective of what the best way of achieving this goal may be, resilient societies are characterised by the fact that they do everything possible to minimise the human, economic and environmental cost of adverse events. This requires appropriate and coordinated measures to be researched, developed and implemented across all the stages of the resilience cycle. It is precisely this aspect that is central to a holistic understanding of resilience. Instead of drawing an artificial distinction between technological, social, economic and other solutions, the key is to explore all of the most promising avenues and combine them in an integrated fashion. This understanding of resilience already underpins government policy and research programmes in countries such as the US, the UK and Switzerland. The resilience equation developed by the researchers from the National Academies provides an excellent overview of the areas that must be addressed in order to create a resilient society. The equation states that resilience can only be achieved through a combination of engineering, physical science, protection of critical infrastructure, social science, various aspects relating to public health and good governance. Should the resilience mechanisms in one of these areas fail, society will be unable to respond adequately to adverse events.

2. A national resilience strategy: establishing resilience as an organising principle

At a policy level, the holistic understanding of resilience requires the development of a national resilience strategy. This is the second lesson learned. In keeping with the recommendation given by the National Academies in their US study, it is necessary to consider how we in Germany can communicate the idea of resilience as a kind of organising principle that constitutes one of the goals of all areas of government and society. Since the way resilience is implemented at community level must take account of local specificities, government cannot simply ordain resilience by statute. Instead, it should develop a long-term strategy and detailed plans for researching, developing and implementing measures to create or increase resilience. The UK government has bought into the holistic resilience approach as the right strategy for successfully coping with all types of adverse events. Documents such as the Sector Resilience Plan for Critical Infrastructure, the Community Emergency Plan Toolkit and the Strategic National Framework on Community Resilience are a testament to the UK's efforts to put this overarching strategy into practice. In view of the potential benefits that it has to offer, a serious assessment should be undertaken to establish whether this routine incorporation of resilience – as defined in this study – into government documents and policies could in future also be rolled out in Germany. Resilience could constitute the underlying principle of all future research initiatives, particularly in the field of applied, solution-oriented security research. This would allow innovative ideas and approaches to be identified more rapidly and effectively, gaps in the research to be plugged and the potential value-added that individual solutions contribute to the overall resilience of society to be reliably evaluated. The remaining lessons learned outlined below can thus primarily be understood as topics and fields where further research and development will enable Germany and Europe as a whole to become more resilient.

3. Is there a case for using threat analyses and vulnerability indicators in Germany?

In order to efficiently increase the resilience of societies and their subsystems, it is first necessary to ascertain which subsystems are vulnerable or susceptible to which threats, as well as the reasons for and extent of their vulnerability. While this third lesson is largely based on Susan Cutter's work on social vulnerability, it also mirrors the first recommendation of the National Academies study insofar as it encompasses far more than indicators of social vulnerability. The Social Vulnerability Index developed by Cutter and her team is an exceptionally valuable tool that has yet to be adapted to the German context. However, in view of the significant benefits that this type of index could potentially

deliver, it would seem desirable to consider whether and how similar indicators might be developed for Germany. This could involve using the SoVI directly to measure the social aspects of vulnerability, given that the index has already been shown to work in different cultural contexts. However, it would also be desirable to systematically record other aspects of vulnerability at different levels and resolutions and present them in an appropriate format. The subsystem of critical infrastructure is one area where there is a particular need for this type of index. It is essential for the specific vulnerability of critical infrastructure to be systematically tracked and communicated to researchers and practitioners in an easily understood format so that appropriate measures to maintain its functionality in the event of a disaster can be researched, developed and implemented. The development of this type of index should therefore be studied over the next few years and, if appropriate, promoted and funded by the government. The same applies to other types of vulnerability such as geographical vulnerability. In keeping with the recommendations of the US National Academies, Germany could benefit significantly in this latter field from the establishment of a database that documents all types of adverse events on a statistically comparable basis, allowing threat analyses to be carried out for specific localities. Tools such as the SoVI, databases of past extreme events, threat analyses for specific geographical areas and indicators of critical infrastructure vulnerability are themselves essential components of a resilient society and can also help to ensure that other elements – such as structural measures to protect critical infrastructure – are calibrated precisely and continue to be correctly adjusted over the longer term.

4. Evaluating resilience: developing ways of measuring resilience

The fourth lesson relates to a significant and immediate challenge for the security research community: there are currently few if any appropriate methods for quantifying or measuring resilience. Practical ways of measuring the resilience of societies and their subsystems are needed so that their resilience can be compared, allowing them to be more easily optimised. As things currently stand, it is extremely difficult to systematically search for weaknesses, assess whether the financial benefits of investments outweigh their cost, or determine how individual measures influence a society's resilience. The research efforts called for under lesson three constitute a first important step towards developing a meaningful way of measuring resilience. However, they are not enough on their own, since they are confined to the description of threats and vulnerabilities. Any successful method of measuring resilience will need to incorporate the all hazards approach, work with systems of different types, sizes and purposes, and describe all the different dimensions of resilience. This results in a number of conceptual problems and methodological pitfalls. It is necessary to find answers to questions such as what the most important variables are, which indicators can best be used to measure them, how different dimensions should be integrated and weighted and whether indicators should be qualitative or quantitative and absolute or relative. It is also necessary to address problems such as the conflict between the static and dynamic interpretations of resilience or the fact that the existence of resilient subsystems does not necessarily guarantee that the system as a whole will be resilient and vice versa. Nevertheless, the methods for measuring resilience that we are calling for do not need to be perfect. The goal of making resilience quantifiable should not become an end in itself. What really matters are the significant benefits that a successful means of measuring resilience would bring to researchers, policymakers, industry and practitioners. The ability to make even just a reasonably accurate comparison of the resilience of different entities would be enough to enable an in-depth analysis of the particularly resilient subsystems so that lessons could be learned from them. It would also immediately draw attention to the need of the less resilient parts of society for different types of help. The German security research community should therefore take up the challenge of developing a practical method of

measuring resilience over the next few years. For this to be possible, it will require firm backing from policymakers. A partnership between researchers, government agencies and private critical infrastructure operators will allow targeted research to be conducted in this area, enabling problems such as the lack of access to the necessary data to be tackled and solved without, of course, contravening the relevant data protection legislation.

5. Resilience engineering: transforming the approach to engineering in the field of security research

Our society's critical infrastructure needs to be upgraded using innovative and advanced technologies in order to meet the needs of the 21st century. Consequently, the fifth lesson learned from our analysis of international perspectives on the concept of resilience is that we need to transform our approach to engineering in the field of security research in order to create "resilience engineering". While there are undoubtedly financial benefits to investing in critical infrastructure resilience, the human suffering that these investments prevent is an even more important factor. Resilience is thus more than just an expensive add-on and must form a fundamental part of future engineering strategies (see lesson seven). In our everyday lives, things actually work like they are supposed to most of the time. It is in fact rather unusual for something to go seriously wrong. Even complex systems function pretty smoothly under normal circumstances. It is this normal operation that form the basis of resilience engineering. An understanding of how complex systems work under normal circumstances is both necessary and sufficient to identify and minimise potential faults, problems and risks in such systems: "The goal of Resilience Engineering is to increase the number of things that go right rather than to reduce the number of things that go wrong."[223] Resilience engineering thus provides a means of managing the ever-greater complexity of modern systems, especially in terms of the wide spectrum of threats that they are exposed to.[224]

Resilience engineering means the systematic incorporation from an early stage of technological solutions to all kinds of security problems into every aspect of the planning and implementation of major social projects – from the individual level to the overall system level – particularly in the field of critical infrastructure. This approach to engineering makes it possible to assess the risks, identify and tackle threats from an early stage, minimise vulnerability, provide efficient support to crisis managers and emergency responders in the event of a disaster and prevent cascading effects from occurring. This new understanding of engineering as something that should ensure and augment society's resilience must inform the specific content of Germany's security research programme and in particular the German government's security-related strategies such as the National Plan for Critical Infrastructure Protection (KRITIS). In keeping with the requirements that PPD 21 places on the DHS in the United States, research into the resilient design and construction of critical infrastructure should also be prioritised as a key research imperative in Germany over the next few years.

6. Resilience modelling: modelling and simulating complex systems

Resilience engineering must be based on a detailed and comprehensive understanding of the relevant complex systems and how they work, particularly under extreme conditions. Customised technological solutions for increasing critical infrastructure resilience should be carefully analysed in terms of their influence and effects on the system as a whole. Researchers and practitioners can obviously not afford to wait until a serious adverse event occurs before they do this. Lesson six thus concerns the need for them to be able to develop system metrics and models capable of simulating all kinds of system behaviour. Security research should place far greater emphasis on research initiatives that enhance existing modelling techniques so that they are able to simulate and help investigate the impacts of adverse events, in particular

223 Hollnagel 2011, pp. 26–34.
224 Woods 2003, p. 5; Woods/Hollnagel 2006, p. 6.

cascading effects. These models must be capable of capturing the local interactions between a wide range of interconnected components which combine to create the global system behaviour. They should also be able to cater both for normal operating conditions and for a broad spectrum of exceptions caused by different types of adverse events. Another key factor that is also crucial to resilience engineering is the reliable identification of system-critical nodes and interfaces where damage could lead directly to cascading effects and total system failure. The technical safety and security of increasingly complex systems must be guaranteed for normal operation as well as for exceptional circumstances. Consequently, the ability to model the system's behaviour under normal operating conditions is just as important, especially since this provides a better understanding of how it is likely to behave in exceptional circumstances. In order to meet all of these requirements, future modelling techniques should stochastically simulate all the system's components in order to describe the behaviour of the entire system without resorting to predefined scenarios or system states. In view of the need to increase the resilience of our complex, interconnected critical infrastructure, it will be crucial to ensure the necessary investment in R&D.

7. Business case resilience: making the case for the value-added offered by resilience

Resilience costs money. Policymakers and business leaders must be willing and able to fund everything from the necessary investment in R&D to the additional cost of building resilient critical infrastructure and the introduction of the concept into school curricula. In a market economy where everything is geared towards optimising costs, there is a tendency to question the need for this type of additional expenditure where the value-added is not immediately apparent. Consequently, lesson number seven is that resilience must also offer economic value. It will be necessary to abandon short-term, short-sighted cost-benefit optimisation in favour of theoretical and practical approaches that are both strategic and sustainable. Investments in resilience, particularly critical infrastructure resilience, are in fact cost-effective over the longer term. The National Academies study cites a report by the Multi-Hazard Mitigation Council which found that for every dollar spent on pre-event mitigation related to earthquakes, wind and flooding, about four dollars were saved in post-event damages. Jon Coaffee discusses how resilience can indirectly create value for cities by attracting businesses and investment, as well as how insurance factors can add to the business case for resilience. If insurance premiums are based on the measures that have been put in place to boost resilience before an adverse event occurs, this could create a win-win situation for the insurance industry and policyholders. It is thus certainly possible to create an overall business case for resilience, but it is up to policymakers to raise awareness on this issue. In order to do so, they will need sound scientific arguments to back up their case. Future research into ways of increasing society's resilience should therefore include the economic aspects right from the outset.

8. Resilience responsibilisation[225] : information, raising awareness and promoting flexibility

The eighth learning can be summarised under the heading of responsibilisation. Strategies should be developed that help the public to become more self-reliant. In order to create a resilient society, its individual members also need to become more resilient. The State can support them through education, empowerment and encouragement. As far as the implementation of any initiatives is concerned, it will be key to engage in a dialogue as equal partners with the relevant sectors of the public. Both practitioners such as Rosanna Briggs and most of the researchers whose work was described in Chapter 3.2 repeatedly stressed the need to raise public awareness of the potential hazards. This public information aspect is key to ensuring resilient behaviour before, during and after a disaster. One means of achieving the necessary

[225] The term "responsibilisation" was coined by Jon Coaffee (see 3.2.4). In this "lessons learned" section, it has been consciously expanded to serve as a heading that encapsulates all the social aspects of resilience.

public awareness of risks and hazards is to incorporate the relevant content into the education of children and young people in our schools. However, further research is needed to establish how this could be rolled out successfully on a widespread basis. Responsibilisation also involves preparing for disasters by carrying out regular emergency and disaster exercises. The procedures that they rehearse and the routine behaviours that they establish can help to save lives in the event of an emergency. At present, there are still not enough of these large-scale, standardised exercises in Germany. Regular rehearsal of what to do in the event of a disaster also gives people the belief that they are well equipped and prepared to cope with any type of disaster. And the mere fact of believing means that they are to some extent better able to do so. Public responsibilisation also includes talking about the things that worked well during a disaster. This increases society's resilience by strengthening its belief in its own abilities. Finally, resilience also requires flexibility. Cities should still be able to (re)act resiliently even in the event of an unforeseen major disaster. It will be necessary to research, develop and implement flexible response strategies that help to activate the potential of the community and the responsible authorities without – as far as possible – being tied to specific types of disaster.

9. Resilience as a key component of sustainable development

Jon Coaffee is one of the authors who discusses the connection between resilience and sustainability. Sustainability can only be achieved if it incorporates resilience, meaning that resilience is a key component of sustainable development. This is the ninth and final lesson learned from our study of the international perspectives on resilience. However, why should sustainable development – i.e. socially just, economically viable and environmentally sustainable solutions – be resilient?[226] Over the past 25 years, sustainability, sustainable development and their underlying principles have risen to become the most important political motif on the international stage. The fact that resilience is an indispensable characteristic of sustainable systems is a direct product of the importance of these terms. A society can be described as resilient if it has the ability to defend itself against actual or potential adverse events, prepare and plan for them, cope with and recover from them and continuously improve its ability to adapt to them. These qualities are essential to a society's long-term stability, i.e. its capacity to persist even in the face of major challenges, including an inherent ability to learn from past events that is also a prerequisite for sustainability. This is key to development which meets the needs of current generations without compromising the ability of future generations to meet their own needs.[227] The defining characteristic of fully resilient systems is above all their ability to keep functioning, adapt, endure and learn in the face of fundamental change processes and simultaneous major adverse events: "Perhaps the essence of sustainability is resilience, the ability to resist disorder."[228] It is thus not surprising that resilience should be included under the heading of "Disaster Risk Reduction" in in the final declaration ("The Future We Want") of the United Nations Conference on Sustainable Development held in Rio de Janeiro in June 2012 (Rio+20). Together with decent jobs, a sustainable energy supply, food security and sustainable agriculture, sustainable urban development, access to clean drinking water and sustainable use of our oceans, resilient societies are one of the seven key components of sustainable development that must be continuously implemented and improved in order to ensure the sustainability of dynamic, evolving systems.[229] It will be necessary to implement all seven of these key components with equal care and attention if global development is to be truly sustainable. The final declaration calls for "disaster

226 Cf. the three pillars of sustainability model used e.g. by the European Commission (see Ec.europa.eu 2013) and the Council for Sustainable Development established by the German government in 2001 (see Nachhaltigkeitsrat.de 2013).
227 Definition of sustainability taken from the Brundtland Report by the World Commission on Environment and Development (A/42/427).
228 Fiksel 2003, p. 5332.
229 Un.org 2013, Uncsd.org 2013.

risk reduction and the building of resilience to disasters to be addressed with a renewed sense of urgency in the context of sustainable development."[230] All the relevant actors, including governments, international organisations, the private sector and civil society, should endeavour to improve the protection afforded to people, infrastructure and other valuable commodities against the impacts of disasters, as well as to reduce the risk of such disasters occurring in the first place.[231] As such, general resilience to all types of threats is an essential requirement for sustainable development and forms one of its key components.

Table 5 summarises the nine lessons that Germany can learn from the international perspectives on the concept of resilience. These nine lessons – ranging from the holistic understanding of resilience to resilience engineering and modelling and resilience as a key component of sustainable development – provide a series of concrete and extremely valuable ideas for informing future research, discussion and work on resilience in Germany. When the international experts came to Berlin in mid-May of 2013 for the "International Perspectives on Resilience" workshop, they could scarcely have imagined that just a few weeks later their expertise and advice would be more urgently needed than ever when Central Europe was hit by some of the worst floods in its history. A better and deeper understanding of the concept of resilience allows us to analyse this disaster with greater clarity. It enables us to recognise the success stories, such as the tireless and heroic efforts of the numerous volunteers and the exemplary display of social cohesion. But it also allows us to see how the problems and failings – e.g. with regard to innovative structural flood defence concepts and the retention of adequate flood plain capacity – fit into the wider context. Even these brief reflections are enough to demonstrate just how valuable the recommendations derived directly from the lessons learned can be in assisting policymakers to significantly reduce the loss of life and financial, social and environmental impacts not only of natural disasters like the June 2013 floods but also of terrorist attacks, industrial accidents and other extreme events. The recommendations thus constitute the first step in the marathon endeavour of creating tomorrow's resilient society.

230 A/RES/66/288, p. 36.
231 A/RES/66/288, p. 36f.

Table 5: Lessons learned from the international perspectives on resilience

LESSON LEARNED	CONTENT
1. The resilience equation: resilience as a holistic concept	The key feature of resilient societies is that they are able to keep all the different types of damage caused by adverse events to an absolute minimum. To this end, the holistic approach employs a combination of technological, social, economic and other solutions. Countries such as the US, the UK and Switzerland are already implementing this approach and Germany can benefit from their experience.
2. A national resilience strategy: establishing resilience as an organising principle	A national resilience strategy should be formulated, including detailed plans for research and development. Resilience can act as the underlying principle of all future research initiatives in the field of security research.
3. Is there a case for using threat analyses and vulnerability indicators in Germany?	In order to increase resilience, it is necessary to have a clear understanding of which systems are vulnerable and at risk and how and why this is the case. There is thus a need for indices capable of describing these factors. Serious consideration should be given to the development of such indices over the next few years.
4. Evaluating resilience: developing ways of measuring resilience	Over the next few years, the German security research community should take up the challenge of developing a practical method for measuring resilience. To do this, it will require firm backing and adequate funding.
5. Resilience engineering: transforming the approach to engineering in the field of security research	We need to transform our approach to engineering in the field of security research in order to create "resilience engineering". Resilience engineering means the systematic incorporation from an early stage of technological solutions to all kinds of security problems into every aspect of the planning and implementation of social projects – from the individual level to the overall system level. Resilience engineering should be prioritised as a key future research imperative.
6. Resilience modelling: modelling and simulating complex systems	System metrics and models should be developed that are capable of simulating all kinds of system behaviour. Reliable identification of system-critical nodes and interfaces will be key. This will require innovative research initiatives in the field of security research.
7. Business case resilience: making the case for the value-added offered by resilience	While resilience costs money in the short term, investing in it pays off in the longer term. It is up to policy-makers to raise awareness on this issue, using sound scientific arguments to back up their case. Resilience research should therefore include the economic aspects right from the outset.
8. Resilience responsibilisation: information, raising awareness and promoting flexibility	Strategies should be developed that help the public to become more self-reliant and flexible in the face of adverse events. The State can provide support by supplying information, raising awareness of the potential hazards, organising more emergency exercises, promoting flexibility and much more besides.
9. Resilience as a key component of sustainable development	Only resilient societies can learn from the past and ensure their long-term survival in the face of increasingly frequent adverse events – a quality that is also essential for sustainability. Resilience is thus a key component of sustainable development.

4 RESILIENT BUSINESSES

LUCAS DAUS, BURKHARD KESTING, TIMO KUKUK

4.1 GOALS AND PLACE WITHIN THE "RESILIEN-TECH" PROJECT

Chapter 4 on "Resilient Businesses" looks at the establishment and improvement of resilience in private-sector companies and public institutions in Germany.

In order to help develop the content for this chapter, we organised an expert workshop called "Resilience in Businesses". This provided an opportunity for representatives of the business and research communities to discuss their ideas on business resilience with university lecturers and emergency planners.

In the business world, the concept of resilience is strongly associated with the establishment of a business continuity management system (a definition of this term is provided in Chapter 4.2). In order to get the participants thinking about the topic of BCM and the structural components that a better practice-based BCM system should contain, the workshop featured two presentations:

1. "Implementation approach following ISO 22301:2012 and BSI 100-4"

2. "An approach for improving the resilience of an ICT provider"

This was followed by a World Café session (see 4.4 for a description of this format) where the following questions were discussed:

- How might a civil defence and emergency planning regulation for businesses look?
- What are the differences with regard to resilience between public-sector "businesses" such as the fire service or the German Federal Agency for Technical Relief (THW) and private-sector companies?

The remainder of this chapter is structured as follows: section 4.2 formulates a definition of business resilience based on the results of the workshop. Section 4.3 summarises the two presentations that were given on the implementation approach based on ISO 22301 and BSI 100-4 and a strategy for improving the resilience of an ICT provider. It furthermore describes the current state of affairs regarding the implementation of BCM in practice. Section 4.4 features a detailed overview of the workshop's outcomes. These provide the basis for section 4.5, which sets out the motivations for businesses to improve their resilience. The final section 4.6 contains a conclusion.

4.2 RESILIENCE – A DEFINITION FOR THE BUSINESS CONTEXT

4.2.1 RESILIENCE

based on the international standard ISO 22301[232] and the BSI Standard 100-4[233], business resilience can be defined as follows:

Resilience is the ability of a business to prevent or mitigate hazards that pose a threat to its survival by being well prepared (prevention) and taking the appropriate measures should an event occur (response). Resilience may thus be defined as "a business's ability to withstand adverse events and ensure its survival".

Preventive measures are measures that are defined and implemented before an adverse event occurs and help to reduce the risk of its occurrence. Similarly, reactive measures are defined prior to the occurrence of an adverse event, but are not implemented until after the event has occurred. They are geared towards managing its direct impact and may, for example, include emergency plans for specific emergency scenarios.

[232] ISO 22301: Societal security – Business continuity management systems – Requirements, International Organization for Standardization.
[233] BSI Standard 100-4 – Business Continuity Management, Federal Office for Information Security.

A hazard is described as posing a "threat to business survival" if its occurrence would put the business's continued existence at risk. In order to quantify this threat, thresholds are defined for various aspects relating to the business's financial and legal status and its reputation. If these thresholds are crossed, measures must be taken to preserve the business's high level of resilience. In practice, particularly in the realm of service management, these thresholds are often stipulated in the service level agreements (SLAs) between customers and service providers. SLAs also set out the relevant penalties or fines for failing to comply with the specified thresholds.

4.2.2 BUSINESS CONTINUITY MANAGEMENT (BCM) – A STRUCTURED APPROACH TO DELIVERING RESILIENCE

The implementation of a BCM system in a business involves creating organisational structures and implementing measures aimed at establishing a high degree of resilience. Traditionally, BCM systems comprise the following structural components:

- BCM Policy and Management System
- Awareness & Training
- Business Impact Analysis
- Risk Management
- Strategy & Recovery
- Process Development
- Exercise & Test

These structural components are described in detail in Chapter 4.3.

In order to create an efficient BCM system, it is important to focus on the company's critical business processes. These must therefore be distinguished from all the non-critical processes within the company. The BCM risk management process (see 4.2.2.1) then identifies both the risks that pose a threat to the survival of the business and the corresponding strategies for critical business processes. However, the emergency and crisis plan must also contain a cost-benefit analysis of the strategies for dealing with the critical risks identified during this process. The cost-benefit analysis helps to decide whether these risks should be addressed directly via preventive measures or whether it is necessary to formulate an emergency plan or address the relevant risks through a crisis management process. The outcome of the cost-benefit analysis provides a basis for developing and implementing the relevant BCM processes. The final component of an efficient BCM system involves exercises and testing. The effectiveness of the measures, processes and emergency plans that have been put in place is measured in practice so that the areas worth improving or updating can be identified.

In order for a business to create an organisational structure that assigns clear responsibilities for different types of risk, it is necessary to distinguish between BCM risk management and business and IT risk management (see 4.2.2.2).

4.2.2.1 BCM risk management

Since the concept of resilience is closely tied to risks that pose a threat to business survival, this section takes a closer look at BCM risk management. The different stages of the BCM risk management process are predominantly based on traditional business and IT risk management methods (see Chapter 4.2.2 for the difference between these two terms). The ISO 27005 standard[234] constitutes one example of a better practice method for IT risk management. The BCM risk management process derived from this approach incorporates the following stages:

[234] ISO 27005: Information technology - Security techniques - Information Security Risk Management, International Organization for Standardization, 2011.

Risk identification

Risks arise from the combination of a hazard to and a weakness in the business. Hazards may be natural or man-made, accidentally or deliberately caused and the result of factors inside or outside the organisation. A hazard can only harm a business if a business shows corresponding weaknesses. Weaknesses exist where security measures are either inadequate or completely lacking. As the number of weaknesses grows, the extent to which the organisation is protected against existing hazards diminishes and the likelihood of a risk event occurring increases. In a BCM system, the risk identification process focuses on risks that could pose a threat to business survival.

Risk assessment

Following the identification of business survival threatening risks and the protective measures that are currently in place, a risk assessment is carried out based on this information. All hazards are evaluated based on a combination of their probability of occurrence and the harm they would cause if they occurred.

Risk management

The options for managing risks after they have been identified and assessed include risk reduction, risk acceptance, risk prevention, and risk transfer. Sometimes several of these options will need to be combined in order to manage a particular risk. For example, there may be cases where the best approach involves combining risk reduction measures with a risk transfer strategy for displacing the potential harm that may result from any residual risk onto a third party.

The goal of *risk reduction* is to reduce risks that pose a threat to the survival of the business by implementing adequate countermeasures. The results of the risk identification and assessment process provide the basis for determining which risk reduction measures need to be taken. One example of a risk reduction measure would be the formulation of an emergency plan, particularly in the case of risks that pose a threat to the survival of the business.

Risk acceptance can also constitute a risk management measure, since in some cases it may be necessary to accept certain risks. For example, the relevant risk reduction measures may not be cost-effective or the potential benefits may mean that the risk is worth taking.

If an identified risk cannot be accepted and the cost of implementing other risk management measures outweighs the benefits, *risk prevention* measures may be used in order to try and prevent the risk from occurring in the first place. This involves eliminating the risky process or measure. For instance, the solution to an environmental risk may involve a change of location to a place where this risk is well controlled or non-existent.

Risk transfer involves shifting the impact of the harm caused by a risk event to a third party. This may take the form of insurance or some other type of agreement between the party affected by the risk and the party who agrees to assume the risk on their behalf (e.g. an outsourcing agreement). It is important to bear in mind that although risk transfer arrangements do enable the responsibility for managing certain risks to be transferred, they do not normally allow transfer of the liability for any damage.

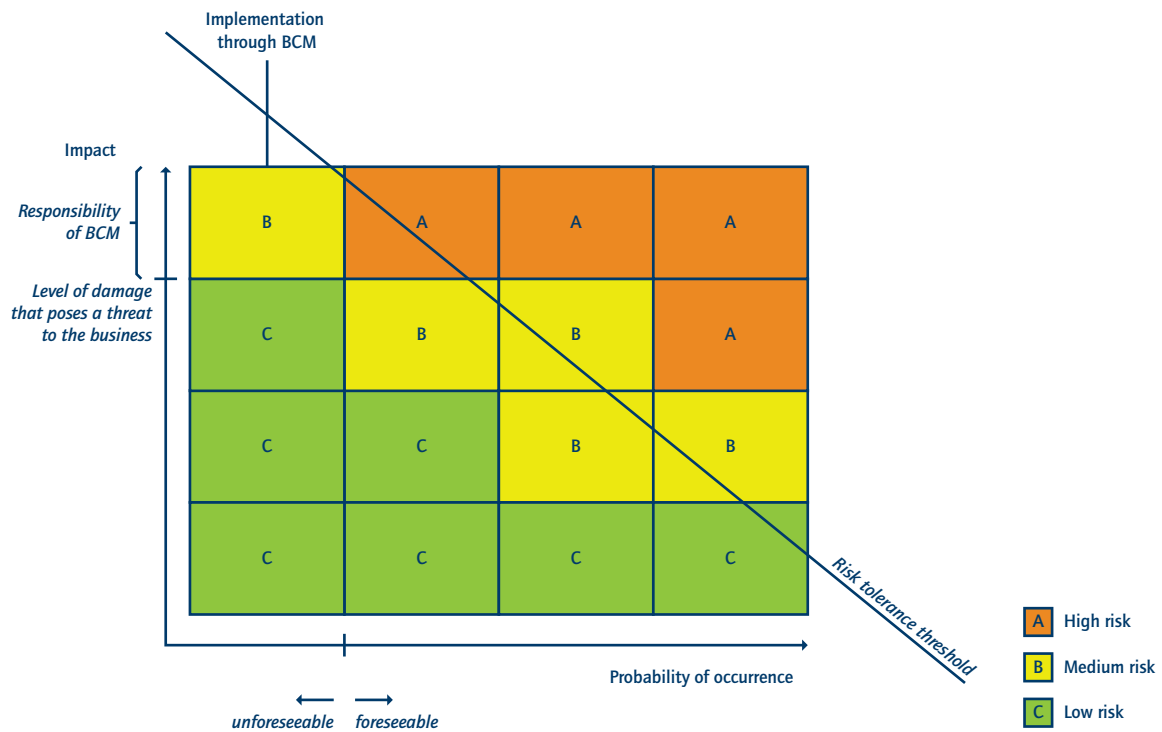
4.2.2.2 Distinguishing between BCM risk management and business and IT risk management

Although BCM risk management is closely related to business and IT risk management, its focus is different. While business and IT risk management has a broader remit that includes all types of risks, BCM risk management only addresses risks that could result in an emergency or crisis and pose a threat to the survival of the business. If a business is to achieve a high degree of resilience, close cooperation and coordination between these two areas is essential in order to ensure transparency with regard to all the identified risks.

This is important, as the risks dealt with by business and IT risk management may be relevant to BCM and vice versa. It is thus key to ensure a shared understanding of the relevant tasks (via an interface definition) and responsibilities and to provide a clear definition of what constitutes an incident, an emergency, and a crisis. In practice, incidents are usually dealt with by business and IT risk management, whereas emergencies and crises are the preserve of BCM risk management.

BCM risk management is responsible for all risks that pose a threat to the survival of the business, irrespective of how likely they are to occur. Implementation of measures for managing high-probability[235] risks that could pose a threat to the survival of the business is usually delegated to the business and IT risk management function. BCM measures are thus focused on managing critical risks with a low probability of occurrence. In addition to natural disasters and pandemics, these may also include cyber-attacks which are posing an increasingly serious threat to companies' survival. Risk matrices (see Fig. 13) are used to provide a transparent overview of all the risks that a business is exposed to. A risk matrix classifies risks based on their probability and impact.

Figure 13: Risk matrix



Source: KPMG AG WPG.

[235] High-probability risks should be managed by standard operating procedures.

4.3 PUTTING BUSINESS RESILIENCE INTO PRACTICE

4.3.1 IMPLEMENTATION APPROACH BASED ON ISO 22301:2012 AND BSI 100-4

There are various standards that businesses can use as a guide for implementing business continuity management systems (BCMS). Two of the most important standards in this area are the International Organization for Standardization's ISO Standard 22301:2012 and the BSI 100-4 Business Continuity Management Standard of Germany's Federal Office for Information Security.

This section uses the ISO 22301 standard and the accompanying guidance document ISO 22313[236] to illustrate the requirements that a BCMS is expected to meet. It will also compare these requirements with those of the BSI 100-4 standard.

4.3.1.1 BCMS requirements as defined by ISO 22301:2012

The international standard ISO 22301:2012 divides the implementation of a business continuity management system (BCMS) into seven key areas. It distinguishes between the two overarching themes of

- BCM Policy and Management System and
- Awareness & Training

and five further areas that build on each other:

1. Business Impact Analysis,
2. Risk Management,
3. Strategy & Recovery,
4. Process Development and
5. Exercise & Test

(see Fig. 14).

BCM Policy and Management System

This area provides the basis for a functioning BCMS. The BCM policy adopted by senior management sets out the framework for the company's specific BCMS and allocates the resources for all BCMS-related activities. It also defines the BCM roles and responsibilities for both normal business operation and crisis situations. Finally, it establishes processes and procedures for continuously improving the management system.

Awareness & Training

This area involves the development of a targeted training strategy, together with concrete measures to train employees and prepare them for their respective roles in the various BCMS plans. It also includes raising awareness of the need for business resilience.

Business Impact Analysis

The business impact analysis (BIA) uses company-specific criticality parameters to determine which business processes are critical. Subsequently, the resources or supporting assetsrequired by these critical business processes are identified.[237]

Furthermore, the BIA assesses the potential impacts of critical business process failures on the business (impact analysis). The impacts are assessed in terms of their duration so that recovery parameters can be determined (e.g. the maximum tolerable period of disruption (MTPD) or recovery time objective (RTO)) and recovery measures for crisis situations can be prioritised. In order to enable recovery, the resources and supporting assets (IT systems, data, human resources, materials, buildings, etc.) that are absolutely indispensable for both normal and emergency business operations are then selected from among the previously identified supporting assets.

Risk Management

The risk management involves analysing the threats and weaknesses of the resources and supporting assets that

[236] ISO 22313: Societal security - Business continuity management systems - Guidance, International Organization for Standardization, 2012.
[237] Barry A. Cardoza, 2006.

are needed for the critical business processes to operate correctly (see 4.2.1). The identified risks are then rated and prioritised. Measures are subsequently established to ensure that these resources are available to the critical business processes and will function correctly. The outcome of the risk management is a detailed plan for dealing with the identified risks (risk treatment plan) and an established process for the structured analysis, evaluation, and treatment of risks.

Strategy & Recovery

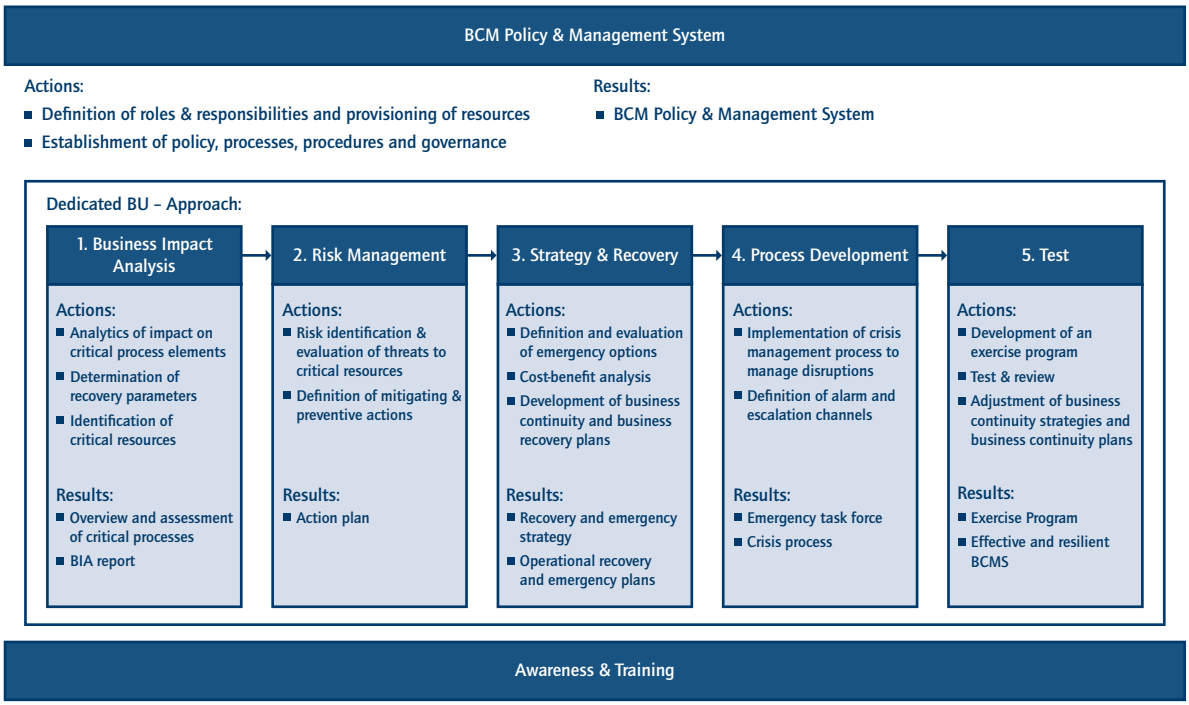
Based on the results of the business impact analysis and risk management, the options and strategies for recovering critical business processes in different emergency scenarios are evaluated and subjected to a cost-benefit analysis. The outcome is a recovery strategy encapsulated in an emergency strategy document[238].

This emergency strategy forms the basis of the individual operational recovery plans (emergency plans) that contain step-by-step instructions for restoring critical business processes to normal operation.

Process Development

The process development area involves the development and implementation of crisis management processes, as well as the procedures for crisis alarm and escalation, convening the crisis management team, in-house and external

Figure 14: Business continuity management system (BCMS) implementation approach based on ISO 22301:2012



Source: KPMG AG WPG.

238 Also referred to as a crisis strategy or recovery strategy.

crisis communication, crisis monitoring, de-escalation up to the point where the situation has returned to normal and follow-up measures once the business is operating normally again.

Exercise & Test

Emergency and evacuation exercises are carried out as part of a comprehensive testing programme. The results are reviewed and used to improve and adjust the recovery plans. The testing programme also incorporates test cycles to ensure continuous improvement of both the recovery plans and the BCMS as a whole.

4.3.1.2 Differences between ISO 22301:2012 and BSI 100-4

While ISO 22301:2012 provides generic guidelines for implementing a business continuity management system, the BSI 100-4 standard contains far more detailed instructions written in the style of an implementation guide.

The key aspects of implementing a business continuity management system are identical in both standards. BSI 100-4 also begins by stipulating the establishment of a framework that defines the relevant roles and responsibilities (initial set-up of emergency management structures). These functions then carry out the business impact analysis and risk management processes, identify the necessary measures and produce the relevant emergency plans (design phase, implementation of emergency contingency strategy and emergency management measures). The standard also requires tests and exercises to be carried out (exercise and testing phase) in order to ensure the quality of the emergency management processes and identify any necessary improvements.

The BSI's detailed hazard and measures catalogues are of particular note. They describe specific threats to businesses and concrete measures that can be taken to counter them.

4.3.2 A STRATEGY FOR IMPROVING THE RESILIENCE OF AN ICT PROVIDER

The business continuity management system of the ICT provider in this example defines resilience as "securing financial survival when the business is confronted with a crisis" or "keeping the business running in the event of a crisis or disaster".

The company draws a clear distinction between business continuity management and ICT service continuity management (ICTSCM) on the one hand and standard operating procedures on the other. The goals of the former are to provide preventive protection against hazards and to establish emergency operation within the maximum tolerable period of disruption for business-critical ICT services. Consequently, BCM/ICTSCM measures are not implemented across the board for all applications, since in this context increasing the applications' availability is not the goal.

The BCM system of the ICT provider in this example has to comply with requirements derived from a combination of statutory obligations, service level agreements with external customers, and operational level agreements with internal customers. These requirements are addressed through a company-wide process model. The first step in this process model involves analysing continuity planning requirements. Business impact analyses and risk management processes are then used to identify the relevant risks, enabling the subsequent development of BCM/ICTSCM strategies.

These strategies are then implemented at a technical and organisational level in the continuity implementation stage of the process model. This is where crisis management procedures are determined, roles and responsibilities defined, training measures planned, and test scenarios for the measures derived from the strategy devised.

The continuity survey stage involves the development and implementation of continuity tests aimed at identifying weaknesses. The test results provide the basis for further improvements to the BCM and ICTSCM.

The disaster management stage involves response measures geared towards ensuring effective management in the event of an actual disaster. After a disaster has occurred, the disaster management documentation is reviewed in order to identify additional measures to improve the BCM/ITSCM system.

The lessons learned from implementing this process model are collected as a matter of course and used to make improvements to the ICT provider's BCM/ICTSCM processes, ensuring a continuous improvement process.

4.3.3 RESILIENCE IN INDUSTRY

On 11 June 2013, KPMG ran a workshop for the BCM user group of Versicherungsforen Leipzig, entitled "Yes, we want a BCM! What are the requirements of the ISO 22301 standard and what does management commitment mean in practice?". The workshop's participants were given the following challenge:

"Consider and discuss how senior management's obligations and commitments should be framed and implemented for each of the individual BCMtopics"

In order to address this challenge, the participants discussed five subject areas based on the content of the ISO 22301 standard. This allowed them to identify what decision-makers need to do in each subject area in order to implement and maintain resilience through a business continuity management system. The five subject areas were as follows:

1. Project Management/Training & Awareness
2. BCM Policy & Management System
3. Business Impact Analysis & Risk Management
4. Strategy & Recovery/Crisis Process
5. Emergency Exercises & Testing

The approaches, ideas and factors that were identified for the different subject areas where collated and the participants, who came from eleven different insurance companies, then had the opportunity to assess the extent to which they are currently implemented in their own company.

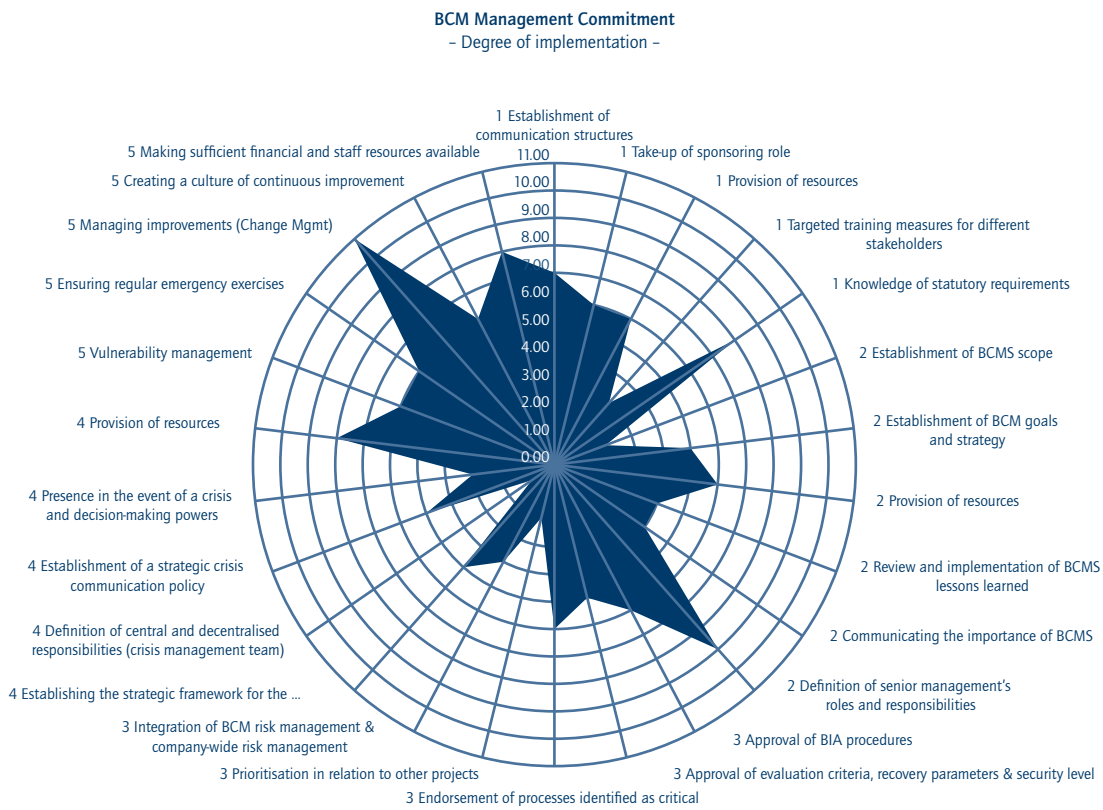
Figure 15 summarises the key factors and the extent to which they are currently implemented.

It is clear that the decisions and measures of senior management required to establish resilience in businesses currently only exist to a limited extent. In addition to the appointment of people to BCM roles, most progress has been achieved in the subject area of emergency exercises & testing. Unlike the other subject areas, this area is at least partly regulated (e.g. in Article 4.4 of the Health and Safety at Work Act, ArbStättVo).

4.4 WORKSHOP OUTCOMES

As part of the "Resilien-Tech" project, we ran a workshop that brought together representatives of government, public institutions, the research community and the financial services and telecommunications industries in order to discuss the differences between the public and private sectors in terms of their perception of resilience and the extent to which it is currently being implemented. We also set out to determine whether the participants felt that a civil defence and emergency planning regulation would be desirable and, if so, what its content might look like.

Figure 15: BCM Management Commitment



Source: KPMG AG WPG.

The workshop employed the World Café discussion format. The idea of World Cafés is to get different participants talking to each other in a way that facilitates an open discussion of pre-defined themes. Small groups of three to five people each sit at their own table. The discussion is enriched by repeatedly asking the participants to switch tables so that all of the specific aspects are discussed by different groups of people. The results are presented by the participants at the end of the session.

The workshop posed two key questions that were discussed by the participants together with the various aspects specific to each of them.

4.4.1 QUESTION 1: HOW MIGHT A CIVIL DEFENCE AND EMERGENCY PLANNING REGULATION FOR BUSINESSES LOOK?

The aim of addressing this question was to discuss the extent to which the private sector considers regulation to be important. In addition, consideration was given to how regulation can contribute to increasing the resilience of businesses.

Aspect 1: What regulations are needed to ensure that the interactions between businesses and public institutions function correctly in the event of an emergency? Would it also make sense to regulate emergency exercises?

The participants identified two different motivations for creating resilience in businesses:

a) financial motivation
b) regulatory motivation

The participants indicated that a financial motivation for resilience exists if creating resilience increases shareholder value. The regulatory motivation for resilience, on the other hand, is a product of statutory or other external obligations on the business.

The discussion groups started outby tackling the question of when a regulation for improving the interactions between businesses and public institutions is deemed desirable. The consensus was that regulatory intervention is only necessary if a lack of regulation would have a negative impact on public welfare or other aspects of society. These are the only circumstances under which the State should introduce regulations for private enterprises. In this context, "public welfare" was equated with the term "system-relevant".

The participants also pointed out that legislation and regulations governing emergencies do in fact already exist. However, it was stressed that these laws and regulations only apply to the defence of the realm (emergency laws). Since most of the threats to public safety and security in the last 20 years have involved natural disasters such as flooding, periods of extremely cold weather or heavy snowfalls, it was felt that further regulation is required to complement the existing legislation.

The growing trend towards privatisation of the public sector was seen as a challenge for efforts to increase resilience. Many former public services are now being farmed out to the private sector in the shape of public-private partnerships (PPPs). A number of notable examples are found in the field of road and bridge construction in particular. The participants believed that this approach could well be extended to include privatisation of the emergency services. In particular, private companies could be used to provide the emergency vehicle fleet. In such a case, the State would need to introduce stronger regulation to ensure that this new interface did not have a detrimental effect on resilience.

The participants also discussed the German government's critical infrastructure protection initiative. It was felt that businesses covered by the KRITIS[239] strategy should be subject to regulation requiring them to become more resilient. However, there was some disagreement as to whether enough companies are currently classified as falling under the KRITIS strategy. In summary, the participants believed that while private-sector companies with a role in managing and overcoming national emergencies should be subject to a regulatory framework requiring them to become resilient, there is also a need to optimise the interface between these companies and the nation's civil defence institutions.

239 Federal Ministry of the Interior (2009): National Strategy for Critical Infrastructure Protection (KRITIS) (http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf, accessed 23.09.2013): Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

Aspect 2: The Federal Financial Supervisory Authority regulates resilience in the financial services industry. Would a similar type of regulation work in other industries and what are the advantages for public institutions?

All the participants agreed that the Federal Financial Supervisory Authority (BaFin) plays an important role in the financial services industry. The organisation is perceived as having a positive influence on the industry's behaviour.

The discussion then moved on to the question of whether the regulatory requirements imposed by the BaFin do indeed help to increase the resilience of banks and insurance companies. Again, most people felt that they do. Further discussion led to the conclusion that regulation by a BaFin-like institution could have a similarly positive impact on the resilience of companies outside the financial services industry. However, it proved impossible to reach a consensus on which criteria (e.g. size) should be used for selecting the companies that would have to comply with the regulations introduced by this new institution.

The workshop also looked at an example of resilience taken from the United States. The US has passed legislation introducing compulsory insurance in order to prevent a recurrence of past situations where the State ended up having to foot the damages bill because people and organisations affected by a disaster were uninsured. The regulations concern both insurers, who are required to provide the relevant policies, as well as companies and natural persons, who are required to take out this type of insurance. Rather than being introduced nationwide, these compulsory insurance regulations only apply to US states that are regularly affected by tornadoes.

The participants also suggested the introduction of transitional regulations to increase the resilience of the relevant businesses. This could be implemented in the form of a "top runner programme" where companies able to demonstrate an increase in their resilience would receive preferential market treatment for the duration of the transition period. Moreover, any businesses that failed to follow suit beyond a certain deadline could be penalised with higher insurance premiums, additional levies, etc.

The overall feeling was that regulation of resilience is at present neither necessary nor good for business.

Aspect 3: Might it be feasible to introduce compulsory reporting of BCM incidents for businesses? And if so, who should they be reported to?

The workshop participants felt that it would only be worth trying to bring in compulsory reporting of BCM incidents as part of industry-specific early warning systems. The suggestion was made that these early warning systems could be organised by the relevant industry associations. Airlines were mentioned as one example, but the insurance industry also has strong industry associations that consult with their members on a regular basis. However, the participants also felt that Germany currently lacks the culture of dialogue needed to successfully establish an early warning system.

The first issue to be discussed was which incidents should be subject to compulsory reporting. This could be determined using both quantitative and qualitative criteria. Incidents could be classified based on the seriousness of their impact. However, most participants did not find a detailed classification of reportable incidents to be necessary.

The participants also called for better prevention. One particular approach discussed as a possible means of promoting measures to increase resilience involved amending the laws governing publicly traded companies (Art. 91 of the German Stock Corporation Act (AktG) for joint stock companies and Art. 43 of the German Limited Liability Companies Act (GmbHG) for PLCs).

In particular, there was much discussion of how to distinguish BCM incidents from incidents such as pandemics, for which compulsory reporting and early warning systems already exist.

The participants also addressed the structure of BCM incident reporting chains. Should businesses report BCM incidents to the local, regional or national authorities and what would need to be done to ensure that reports were passed on to the appropriate other levels? The key question in this context was which incidents are deemed to be of national importance.

The participants concluded that compulsory reporting as part of an early warning system must offer benefits to the companies that report incidents. This would be true of e.g. a sectoral approach with industry-specific reporting criteria. In order to achieve meaningful benefits, it would be necessary to review the reported and published information after the incident was reported, once again highlighting the importance of targeted and carefully chosen reporting criteria.

4.4.2 QUESTION 2: WHAT ARE THE DIFFERENCES WITH REGARD TO RESILIENCE BETWEEN PUBLIC-SECTOR "BUSINESSES" SUCH AS THE FIRE SERVICE OR THE GERMAN FEDERAL AGENCY FOR TECHNICAL RELIEF (THW) AND PRIVATE-SECTOR COMPANIES?

The second question addressed during the World Café was aimed at analysing the differences (and similarities) between the private and public sectors with regard to resilience.

Aspect 1: Is there any difference between private companies and public institutions as far as making improvements to resilience is concerned?

The discussion of the differences and similarities between the private and public sectors in terms of making improvements to resilience was informed by representatives of both sides. It became clear that private companies have a shorter-term perspective than the State when it comes to planning ahead.

The participants agreed that governments' tendency to take unpopular decisions at certain points in the lifetime of a parliament has a significant influence in the public sector. This can have a negative impact on the implementation of plans to increase resilience, since their benefits usually only become apparent after a very lengthy period of time. The key factors that influence whether or not a private company decides to improve its resilience include the company's legal form, the industry it operates in and who it is owned by. There was a consensus that publicly traded companies that are not run by their owners generally tend to have shorter-term policies than e.g. family businesses that have been run by their owners for many generations.

The participants suggested that "more State" would be one way of addressing the conflicts of interest that can sometimes occur. It was proposed that legislation could be passed to prevent companies from failing to comply with (as-yet undefined) resilience requirements. However, most people favoured an incentive system that would reward companies for increasing their resilience. All the participants agreed that a "culture of resilience" does not currently exist. It was suggested that policymakers should establish incentives geared towards developing a culture of resilience in Germany.

The discussion concluded that the State should be responsible for tackling the current conflict of interests between private companies and public institutions with regard to the establishment of resilience. In addition to its role in protecting national interests, the challenge for the State is to address the extremely wide-ranging concerns of private companies

and, ideally, develop appropriate incentive systems for reconciling public and private sector interests insofar as this is possible.

Aspect 2: Are there any differences between public institutions and private companies in terms of the frequency of exercises, the way they are carried out, and the way their results are analysed?

The workshop commenced by discussing the goal and purpose of emergency exercises. The participants felt that private companies tend to focus their emergency exercises on the failure of components that have been identified as being system-critical. There is thus a tendency only to consider emergency scenarios that the company believes to have a realistic chance of occurring. Fire drills were one example mentioned in this context.

This attitude can be attributed to management's reluctance to invest resources in scenarios that it believes to be unrealistic, on the grounds that such investments are not cost-effective. Employees are also less likely to want to take part in exercises for emergency scenarios that they subjectively perceive as unrealistic. Rather than feeling supported by these exercises, they will tend to see them as an imposition. Efforts to increase business resilience should therefore aim to improve the perceived value of emergency exercises to employees and encourage the organisation to buy into the importance of exercises for ensuring the company's survival.

The cost of carrying out emergency exercises varies owing to the different activities undertaken by companies in different industries. The cost of exercises to companies in non-manufacturing industries, for example consultancy firms, will be lower than for manufacturing companies in e.g. the chemical industry. These differences explain the significant variability in the extent and frequency of exercises in different private-sector companies.

The participants confirmed that the success of emergency exercises is highly dependent on the involvement and attitude of management. In other words, one of the key drivers of success is how employees perceive "management commitment".

It was also pointed out that in addition to emergency exercises it can be helpful to carry out simulations and simulation games. One participant described a workshop for CEOs of German businesses where they were given an operational role in a fictitious company and then asked to tackle the typical problems that their employees would be faced with in the event of an emergency. This exercise drew the CEOs' attention to the fact that their strategic overview of their business might not suffice in an emergency situation. The cost of this workshop was much lower than what an organisation would spend on individual emergency exercises. It thus proved to be an efficient exercise, since the small changes that it brought about in the CEOs' attitudes had a major impact within their businesses.

The representatives of public institutions said that emergency exercises are regarded as a worthwhile activity in the public sector. This contrasts with the situation in private companies, where there is a conflict between the cost of exercises and the perceived likelihood of an emergency event occurring, meaning that they are not seen as a priority and are often regarded with scepticism. No definitive answer was found to the question of how to develop a financially compelling preventive approach that would save companies from having to learn the hard way.

Aspect 3: Are businesses in Germany resilient?

The final question addressed by the workshop was aimed at establishing how resilient businesses in Germany are and comparing this against the resilience of businesses in other countries.

The decision to implement a BCMS in order to increase a company's resilience is taken by the board of directors. However, the board's focus is primarily on strategic issues and it lacks the understanding of operational issues needed to assess which measures are required to improve the resilience of the business. The participants felt that the relevant company structures were therefore less likely to approve measures aimed at increasing resilience.

The example of the US was used to compare the situation in Germany with what is happening elsewhere in the world. The participants felt that companies in the United States have a greater awareness of resilience. They put this down to the higher number of natural disasters that businesses in the US are bound to encounter. Moreover, the regulations governing the personal liability of company directors mean that there is more awareness than in Germany of events that could potentially harm the business.

The participants added that the extent to which a CEO or board member is motivated to increase resilience depends on the nature of their relationship with the company. They believed that managing partners have a much stronger financial interest in protecting their company, even if the cost of doing so may mean that they receive lower dividends. Managing directors who are simply employees of the company, on the other hand, have no personal interest in the success of the business beyond their own salary and bonuses. They thus tend to be motivated by more short-term considerations.

In order to provide an overall answer to this final question, it is thus necessary to take a range of different factors into account. While the relevant public institutions regard defined emergency scenarios as essential to their ability to carry out their core business, private-sector companies find it much harder to adopt this attitude. The focus of private companies is on their customers and on making a profit. This means that they are quick to regard any shortcomings in areas outside of their core business as critical cost drivers. Cost-effectiveness is thus a key factor in terms of how businesses approach resilience. Another factor becomes apparent when German businesses are compared with companies in other countries. The fact that disasters occur less frequently in Germany means that there is less awareness of them among German businesses. A further key driver appears to be the legal structure of the company and the resulting differences in the personal liability of its senior executives. Finally, it is crucial not to overlook the significant influence of cultural factors.

4.5 MOTIVATING BUSINESSES TO INCREASE THEIR RESILIENCE

An analysis of the workshop's outcomes revealed that businesses and/or their decision-makers currently recognise two motivations for increasing their resilience:

- financial motivation
- regulatory motivation

It should be noted that none of the participants in the workshop mentioned the threat of penalties as a reason for increasing resilience. However, during the discussions, various people cited negative consequences that had come about as a result of financial and regulatory penalties for failing to implement resilience.

4.5.1 THE FINANCIAL MOTIVATION

During the workshop, discussions with the representatives of the business community revealed that the reasons for companies taking measures to improve their resilience are often financial in nature. These can be divided into two categories: competitive advantage and internal process optimisation.

A high degree of resilience can provide a company with a significant competitive advantage as a result of the high market availability of its products and/or services. Suppliers can, for example, offer their customers attractive contracts containing service level agreements with fixed product or service availability thresholds. In situations where several companies in the same industry are affected by a critical hazard, highly resilient companies can gain a further competitive advantage from their ability to respond more rapidly and effectively to the hazard and recover their critical business processes within a short period of time.

In addition, a high level of resilience helps to optimise and strengthen a company's internal processes, making them less vulnerable to hazards that pose a threat to the business. The probability and impact of interruptions to business continuity are thus reduced. And even if business continuity is interrupted as a result of an adverse event, the company is in a position to recover its critical processes relatively rapidly and efficiently[240].

4.5.2 THE REGULATORY MOTIVATION

There are currently no specific statutory regulations that require the introduction of a business continuity management system. However, several pieces of legislation do stipulate generic requirements, for example the German Stock Corporation Act (AktG), Federal Data Protection Act (BDSG), German Civil Code (BGB), German Limited Liability Companies Act (GmbHG), Principles of Proper Accounting (GoB), Principles of Proper Computerised Accounting (GOBS) and Control and Transparency in Business Act (KonTraG). Point 7 of the annex to Article 9 of the BDSG requires "...that personal data are protected against accidental destruction or loss (availability control) ...". This can be interpreted as a BCM measure that improves both resilience and data protection.

The Control and Transparency in Business Act (KonTraG) calls for timely identification of risks that could pose a threat to the survival of the business. For this category of risk, the potential consequences of an interruption to business continuity should be analysed and safety and security strategies and emergency plans should be developed. This is largely in line with the requirements of a business continuity management system.

Commercial laws such as the German Commercial Code (HGB), GoB and GoBS stipulate that companies must provide the information requested by the tax authorities for the purpose of account and tax audits. Companies must therefore make the necessary provisions to ensure that this data is available at all times and is not irretrievably damaged as a result of an adverse event.

According to both the German Stock Corporation Act and the German Limited Liability Companies Act, businesses must carry out risk management and thus should address the risks of crises and emergencies. They are required to assign roles and responsibilities and implement risk monitoring procedures. Areas requiring improvement should be regularly tested for and communicated. As far as BCM is concerned, areas for improvement can also be identified by regular testing of the emergency plans.

For companies wishing to raise equity through a share issue, the Stock Corporation Act sets out certain requirements that can be met by an effective BCM system. Article 91.2 of the Act places a legal obligation on the board of management and supervisory board of joint-stock companies to take suitable measures, in particular the establishment of a monitoring system, to ensure that developments threatening the survival of the company are detected early on. The exact nature of these measures is left to the discretion of the company in question.

Companies in certain industries must meet special requirements concerning the continuity of the products or services they supply. Telecoms companies, for example,

[240] The measures' efficiency is ensured by carrying out risk and cost-benefit analyses before the BCM measures are introduced.

are subject to a universal service obligation. Implementation of standards such as ISO/IEC 22301 and BSI 100-4 supports compliance with these statutory obligations. It ensures that a company can continue to operate in the event of a disturbance and protects business-critical supporting assets against loss and failure. Such standards are nevertheless not legally binding.

4.6 CONCLUSION

The discussions with the participants in the workshop resulted in a series of recommendations and potential next steps for improving the resilience of businesses in Germany.

It became apparent during the course of the workshop that private-sector companies and public institutions in Germany differ significantly in their attitudes towards maintaining and improving resilience. While public authorities and institutions are required to attain a statutory level of resilience so that they are able to meet their obligations to society, there is currently no direct requirement for private companies to increase their resilience or maintain it at an acceptable level.

Various different sources require businesses to address operational risks. The German Stock Corporation Act, German Commercial Code and other laws all refer to early risk detection and management as one of the responsibilities of the organs of publicly traded companies. However, a closer look at the operational risks detailed in corporate risk reports reveals a complete absence of any reference to damage caused by meteorological events, disasters and emergencies. In practice, companies generally focus only on operational risks with a high probability of occurrence, since they tend to believe that investing in measures for extremely low-probability risks is not cost-effective. Since the risk categories reported by companies fail to include disasters and emergencies, it is necessary to assess whether risks that pose a threat to the survival of the business could be defined centrally and compulsorily assigned to specific risk categories.

The perception often exists that establishing or maintaining resilience is at odds with the company's core business. After all, the chief purpose of a business is to provide services, manufacture products and make a profit. Companies do believe that ensuring the company's survival in terms of its efficiency and profitability is one of the direct goals of their business, and this is undoubtedly also something that contributes to resilience. However, this is just one of the exogenous factors that companies need to be resilient to and other factors such as natural disasters and damage caused by meteorological events tend to be overlooked. It is quite simply not enough to focus exclusively on resilience to risks of a financial nature.

It is thus necessary to create incentive systems for promoting resilience in private companies so that they can attain a level of resilience comparable to that found in the public sector.

The lessons learned can be summarised as follows:

Table 6: Lessons learned from the workshop "Resilient Businesses"

LESSON LEARNED	CONTENT
1. Regulate the interface between the State and the private sector	The interface between private-sector companies with a role in managing and overcoming national emergencies and the nation's civil defence institutions should be regulated.
2. Compulsory insurance	Where companies fail to implement adequate resilience measures, they should be required to take out compulsory insurance. Insurance could also be used as an optional measure for increasing resilience. Measures should furthermore be taken to ensure that insurance companies provide the relevant policies.
3. Monitoring and providing incentives for resilience	A government resilience monitoring system run by a supervisory authority similar to the Federal Financial Supervisory Authority should be introduced. The system would provide appropriate rewards to businesses that are able to demonstrate an increase in their resilience. Businesses that failed to take measures to improve their resilience would be penalised with higher insurance premiums, additional levies, etc.
4. Early warning system with compulsory reporting	It is necessary to define the parameters for the introduction of a national early warning system, together with industry-specific compulsory reporting arrangements (i.e. the criteria for reporting events would vary from industry to industry). The system would need to offer resilience benefits to the companies that report incidents.
5. Incentive systems	In addition to its role in protecting national interests, the State must address the extremely wide-ranging concerns of private companies and develop appropriate incentive systems for reconciling public and private sector interests. A national incentive system would provide a framework for developing a culture of resilience and would encourage companies to increase their resilience by getting them to perceive it as one of their business's corporate values.
6. Regulate to ensure that emergency and crisis exercises are carried out	Regulations should be introduced to ensure that emergency and crisis exercises are carried out in order to increase business' acceptance of the need for resilience despite conflicting financial goals. The regulations should be industry-specific and should take differences in the size of companies into account.
7. Cyber risks	Since cyber risks are increasingly capable of posing a threat to companies' survival, existing cybersecurity initiatives such as those launched by the Federal Office for Information Security (BSI) – for example the Alliance for Cybersecurity – should be combined with new measures.

5 THE CASE FOR RESILIENCE AS THE KEY TO ENERGY SECURITY

FRIEDBERT PFLÜGER

On July 17, 1913, almost exactly 100 years ago, the First Lord of the Admiralty, Winston Churchill, took the floor of the British House of Commons. British warships, he proclaimed, would henceforth be powered by oil instead of coal, in order to become faster and more cost-efficient than the German fleet. This, however, also meant that the Royal Navy had to substitute domestic coal with Persian oil. Countering claims by his critics in the opposition that this would pose a threat to supply, he insisted that London should never become dependent on a single country, route, energy source or (oil) field: "Safety and certainty in oil lie in variety, and variety alone."[241] Churchill had thereby outlined the central theme for all future debates on energy security: the diversification of energy supplies.

60 years later, in October 1973, OPEC's oil embargo shocked the West. Neglecting Churchill's warning, the industrialised world had, for some time already, fallen into dependence on oil-producing countries, particularly from the Middle East. Now oil prices quadrupled, the economy slowed down and overnight it became clear that the world's power balance had shifted: the producers in the global "South" had become a political power. For the first time, the "North" appeared vulnerable to the "oil weapon".

In the wake of the Oil Crisis, energy security became the core concern for industrialised Western nations. At the 1974 Washington Energy Conference, they agreed on a concerted reaction in the event of future disruptions of energy supplies. This is how, among other things, the so-called strategic oil reserves came about, as well as the International Energy Agency (IEA), which was set up as an institutional "counterweight to the OPEC empire"[242]. The IEA, based in Paris, lived up to its founders' expectations. Today, its analyses and forecasts of developments in energy policy provide a common basis for science, business and government alike. It also formulated the now widely accepted definition of energy security as "an uninterrupted availability of energy sources at an affordable price."[243]

The importance of energy has only continued to increase in a globalised and digitalised world. Today, hardly anything is conceivable anymore without energy, be it drinking water, television, computers or phones. In the absence of the global network of transportation, cooling systems and stores, our supply chains providing people with food and essential goods would fail. The uninterrupted supply of affordable energy has thus become all the more important. The advent of renewable forms of energy in the last decade – which can currently cover about two percent of global energy demand (excluding hydropower)[244] – has not diminished the dominance of fossil fuels. Even by 2035, around 80 percent of energy demand will be met by oil, natural gas and coal (in almost equal shares)[245]

Energy security in the international context will therefore continue to depend on uninterrupted supplies of fossil fuels for the foreseeable future. Supply security at an affordable price is an extremely complex and fragile matter, and hence continuously at risk. In this context, we can distinguish seven central risk factors:

Seven risk factors for energy security:

1. Wars, crises and conflict in energy-producing countries
can lead to disruptions of the production and supply of energy that affect the global economy. The Iranian Revolution of 1979, the First Gulf War of 1990/91 and the complete halt of Libyan oil production as a consequence of the

241 Churchill 1913.
242 Yergin 2012.
243 http://www.iea.org/topics/energysecurity/ [accessed: 22. 01. 2014].
244 IEA 2013.
245 IEA 2012.

war in 2011, for example, all had drastic effects on supply chains, energy prices and, as a consequence, the economies of importing countries. Similarly, the 2002 general strike in Hugo Chavez' Venezuela and the Iraq War of 2003 also had serious repercussions and contributed – alongside other factors that will be discussed later – to a continued surge in the price of oil which eventually passed 140 US dollars per barrel in July 2008, contributing significantly to the global economic crisis that followed.

2. Political extortion as a consequence of a one-sided dependence on a single energy producer

is another risk factor for an uninterrupted supply of energy at an affordable price. The dominance of Russian gas supplies to parts of Europe, in particular the Central and Eastern European countries, meant that gas prices were no longer only determined by supply and demand mechanisms but were also decided politically. The disruptions of Russian gas supplies to the Ukraine in 2005/06 and 2009 caused a supply crisis in several Central European countries, even though its actual impact was secondary to the fear surrounding Russia's clout. The two gas crises, which Moscow should not be blamed for unilaterally, sparked an intensification of the European debate on energy security and gave new impetus to plans for more diversification of the gas sector through alternative supplies from the Caspian region via the "Southern Corridor" (Nabucco Pipeline, Trans Adriatic Pipeline TAP). In addition, they led to the inception of a genuine European energy policy and the appointment of a dedicated EU Commissioner for energy (Günther Oettinger).

3. An impending re-nationalisation – and even energy imperialism –

now pose real threats to a global supply system based primarily on the interplay of supply and demand. More than 80 percent of conventional reserves of oil and natural gas are produced by state- or semi-state-owned energy companies, i.e. they are directly or indirectly dependent on the political leaders of their respective country who are well aware of the political relevance of the resources that they control. Increasing scarcity of natural resources against the backdrop of a dramatic growth in the world's population and its thirst for energy – global demand will increase by one third by 2035[246] – will make it all the more tempting for countries to use their riches for nationalist or even imperialist ends. China's determination to secure access to sources of energy and raw materials across the entire globe ranks as one of the most significant geopolitical phenomena of the early twenty-first century.

4. Terrorist attacks against energy infrastructure,

i.e. on the routes of oil and LNG tankers as well as on pipelines and oilrigs, can also pose a threat to affordable supply security. In 2006, terrorists in the Niger Delta (in Nigeria) caused a dramatic reduction in oil production. The Arish-Ashkelon pipeline between Egypt and Israel was attacked 13 times by terrorists in the year following the fall of President Mubarak, with dramatic consequences for Israel's energy security – 40 percent of Israel's gas supplies depend on Egypt[247]. As recently as January 2013, Islamist terrorists attacked BP's oil production in the Algerian desert and kidnapped employees of the company. From the Strait of Malacca to the Strait of Hormuz and the Bab-el-Mandeb between Yemen and Somalia, wherever there are straits, terrorists and pirates lurk, often working closely together.

5. Cyber terrorism against critical energy infrastructure

represents a growing and often underestimated danger to energy security. Frank Umbach recently pointed out that although the US military has been forced to make all kinds of cuts to its budget, the Pentagon's Cyber Command has bucked this trend by increasing its personnel from 900 to 4,900. President Barack Obama recently warned that enemies of the United States could attempt to sabotage its energy infrastructure, particularly its power grids. The head of the US national intelligence service, James Clapper,

246 IEA 2012.

247 http://energy.gov.il/English/Subjects/Natural%20Gas/Pages/GxmsMniNGEconomy.aspx [accessed: 22. 01. 2014].

added that such attacks constituted "the most immediate threat".[248] What if a cyber attack succeeded in disabling the cooling systems of nuclear power plants? In 2012, Austrian author Marc Elsberg wrote a political thriller about the dangers of cyber terrorism for Europe's electricity supply, which he recently presented at the Forum FAZ/Munich Security Conference.

6. Natural disasters
are a real threat to supply security, as hurricanes Katrina and Rita demonstrated in 2005. These storms destroyed about 170 offshore oil rigs in the Gulf of Mexico.[249] Almost a third of American oil production and its refining capacity was lost – with farreaching and longlasting consequences for supplies across the entire country. The impact of the earthquake and ensuing tsunami that hit Japan on 11 March 2011 was even worse. It led to the death of thousands of people and a "beyond design-basis accident" at the Fukushima Daiichi nuclear power plant, with dramatic consequences for Japan's society and economy. Beyond disasters of such magnitude, reinsurance companies report that the number of devastating floods and storms is on the rise – not least as a consequence of climate change. And natural disasters like these are usually accompanied by short- or long-term disruptions of energy supplies. These threats will increase as climate change gathers pace. Monster storm Sandy forced the evacuation of 375,000 people and left 8 million people without electricity for several days in October 2012, but it was little more than a taste of things to come.[250] Only a few years ago, it was inconceivable that storms of this magnitude could appear so far north. Climate change also brings dangers for people and energy supplies in other parts of the world. What, for example, will it mean for Russia's pipeline network if the permafrost regions of Siberia keep getting warmer? What will the consequences be for supplies to Chinese cities if Himalayan glaciers continue to melt and the big hydropower plants can no longer produce enough electricity?

7. Technical failure, often related to human error,
is and continues to be a threat to energy security. Technology will never be perfect; a residual risk always remains. The tragic Chernobyl disaster in 1986 is a prime example, but even comparatively minor accidents like the 1989 Exxon Valdez oil spill in Alaska can, besides damage to humans and ecosystems, also affect regional energy supplies. Greater threats to energy security are posed, for example, by the hitherto unresolved issue of the final storage of spent nuclear fuel rods, as well as the theoretical possibility that chemicals used in "fracking" – the technology involved in the production of fossil energy in shale formations – could come into contact with groundwater. Even the hypothetical scenario of accidents like these, caused by the interaction of humans and technology, can lead to a reduction in public acceptance of such forms of energy production.

So how should we deal with these threats? The key is to build resilient energy supply systems.

In 2013, the European Centre for Energy and Resource Security (EUCERS), together with the National Academy of Science and Engineering (acatech) and the Konrad Adenauer Foundation (KAS) hosted a series of five round table discussions on the development of resilient energy systems within an international context. Each event began with two or three keynote speeches of ten to 15 minutes' duration. The remainder of the session was given over to an open discussion between the 30 or so participants from the research community, industry, government and the media. The goal was to engage in a thought-provoking and constructive debate in order to inform policymakers, researchers, practitioners and the public about the latest trends and perspectives in this field.

248 Mazzetti/Sanger 2013.
249 Kennett 2006.
250 see Saul 2012; Johnsson/Polson 2012.

The presentations and discussions at the five expert round table events placed particular emphasis on the importance of building resilient energy systems. Both researchers and practitioners made important contributions to the current debate and concrete proposals about how to take it forward (see appendix).

Seven measures to build resilient energy systems

A resilient energy system is defined by its ability to withstand interruptions or to prevent failure through protective measures. Churchill's century-old demand for variety, i.e. diversification, takes centre stage in this endeavour.

1. Diversification and energy independence

Churchill defined the most important task over 100 years ago: diversification. Only a diverse range of energy sources, producing countries and supply routes can bring security. The desire to overcome dependence in the wake of the OPEC oil embargo led to Richard Nixon's "Project Independence" of November 1973, in which he demanded American energy independence from foreign countries. This goal, which has been pursued by practically every US president since Nixon, might finally be realised half a century later: by the mid-2020s, the United States could become independent of oil and gas imports as a result of the shale revolution!

2. Decentralisation

Another option for protecting complex energy systems, especially in terms of preventing major disruptions or limiting their impact, lies in the development of complementary, decentralised supply systems. Renewable forms of energy are particularly well suited to this purpose, for example wind, PV, solar thermal, biomass, geothermal and hydropower. Many households and small and medium-sized businesses are now trying to become largely independent of the main grid through such decentralised energy sources. As renewable forms of energy are subject to high output fluctuations, they currently still rely on conventional energy sources for back-up – at least as long as storage technologies remain inadequate.

3. The highest safety, efficiency and environmental standards

Safety and environmental standards may be expensive. But in the end, they serve everybody because of their pre-eminent importance for public acceptance of the relevant energy source. Although hurricanes Rita and Katrina cost many lives and caused widespread destruction, particularly in New Orleans, it was due to the fact that the highest standards were in place that no oil was spilled into the Gulf of Mexico despite many drilling rigs being destroyed. BP, on the other hand, incurred significant financial costs and damage to its image in 2010 as a result of insufficient safety and environmental standards in the context of the sinking of its Deepwater Horizon offshore drilling rig. The auto and petroleum industries both owe their continued acceptance in Europe to the dramatic progress that they have achieved in efficiency and environmental standards.

4. Dialogue between producers and consumers of energy

Maintaining an intensive and trust-based dialogue between importers and exporters of energy is of central importance when it comes to the prevention of disruption to the global energy system. It is particularly important to understand the interests of the other side, because the meaning of energy security is very different for producing countries and for consumers. To the former, energy security does not mean supply security, but "security of demand". The big petroleum exporters such as Russia, Saudi Arabia, Libya, Angola and Venezuela depend on steady sales of their resources at what they regard as an acceptable price. Just as higher oil or gas prices can be harmful to Western economies, low energy prices reduce the revenue earned by producing countries. This can easily have a knock-on effect on their political stability. The IEA, and indeed all bilateral and multilateral encounters – from state visits to academic

conferences – play an important role in maintaining a dialogue. Likewise, the work of political foundations and chambers of commerce – and especially the cooperation between managers, engineers and personnel in joint projects – helps to build mutual understanding of interests and cultural differences and create transparency by facilitating the comparison of data and analyses. This in turn helps to build trust. At present, one particularly important task in this regard is the integration of China and India into the various forums of the international energy dialogue.

5. Integrating young people: jobs

The rapid population growth in many exporting nations, especially in the Middle East, Africa and Latin America, means that even if their economies grow, these countries are rarely able to create enough jobs for the younger generation. Around half the population in Algeria, Libya and Saudi Arabia and over 60 percent[251] of Iraqis are under the age of 25. However, oil and gas production is capital-intensive rather than labour-intensive, meaning that it creates very few direct jobs. The millions of young people affected by unemployment and poverty provide fertile ground for political radicalisation, allowing Islamist extremists to sow the seeds of their violent ideologies. Therefore, it is in Western countries' own interest to do everything they can to help petroleum states diversify their economies and provide job-training opportunities for their young people. The work of development agencies such as Germany's GIZ and the political foundations is particularly important in terms of helping to improve the prospects of as many young people as possible in the petroleum states.

6. Preventive measures by the police and military

It was US President Jimmy Carter who formulated the 1979 American foreign policy doctrine according to which any attempt by a foreign power at gaining control over the Persian Gulf would be regarded as "an assault on the vital interests of the United States of America" that would be countered by any means necessary, including military action.[252] Ever since, the United States has considered it a top priority to secure the energy lifelines, i.e. the uninterrupted flow of Middle Eastern oil and gas. There may undoubtedly be good reasons to be critical of specific political and military measures undertaken by Washington in this context. Nonetheless, it is a fact that Europeans have benefitted at least as much as the United States from American commitment to securing the energy routes. Free movement by tankers through straits, protection against pirates and terrorists, the gathering of intelligence on terrorist groups and the fight against them domestically – all these tasks call for continued protective action by the police and the military. Europe will in all probability have to increase its contribution in this domain, given that the United States' readiness to carry out military action overseas will probably decline as a result of the shale revolution in North America.

7. Disaster control

Finally, the design of resilient energy supply systems should incorporate adequate emergency measures that can be rapidly deployed in the event of a catastrophic supply crisis following a terrorist or cyber attack on the energy infrastructure, as well as in the case of an accident or natural disaster. In countless calamities ranging from Chernobyl and Fukushima or storms such as Katrina and Sandy to Deepwater Horizon, it transpired that very few emergency plans were in place e.g. for evacuations, medical care, emergency shelters, etc. In particular, there were no clear guidelines allocating responsibilities. But our ability to quickly restore supply security depends on how swiftly we are able to respond in the event of an emergency.

Former State Secretary Prof. Dr. Friedbert Pflüger is the director of the European Centre for Energy and Resource Security (EUCERS) at King's College London and a Senior

251 CIA 2013.
252 Carter 1980.

Non-resident Fellow at the Atlantic Council. At acatech, he is responsible for energy issues within the Resilien-Tech project group; he also chairs the Natural Resources working group at the Atlantik-Brücke. Prof. Pflüger is owner and CEO of two management consultancy firms.

Appendix

The first of the five round table discussions (held in March 2013) addressed the subject of "Europe's Vulnerability to Energy Crises". The keynotes were given by Dr. Frank Umbach (EUCERS) and Dr. Thomas Rid, Department of War Studies, King's College London, who recently published a book entitled "Cyber War Will Not Take Place".

BThe title of the second event was "Building Resilient Energy Infrastructure Beyond Europe's Borders". The keynotes were given by acatech member and Director of the Fraunhofer Institute for High-Speed Dynamics, Prof. Dr. Klaus Thoma, and Dr. Yolanda Garcia-Mezquita, DG Energy, European Commission.

Under the title of "The Danger of Blackouts – Electricity Security as the Achilles Heel of Resilient Energy Infrastructure?", the third round table featured keynotes by Jörg Asma, former KPMG Partner and former member of acatech's Resilien-Tech Working Group and Sarah Mandar, Tyndall Energy Programme, University of Manchester.

The fourth event was entitled "Challenges and Prospects for an Integrated Energy Infrastructure in Europe". The keynote addresses were given by Dr. Anita Orban, Ambassador-at-Large for Energy Security, Hungary, Thomas J. Dimitroff, Partner, Infrastructure Development Partnership LLP, and Tora Leifland Homström, Government Affairs Advisor, Trans Adriatic Pipeline (TAP). In the run-up to the southern corridor decision, the participants discussed the political significance of the European energy infrastructure.

The final round table in the series was held at the end of October 2013. Jennifer Giroux of the Center for Security Studies (CSS), ETH Zürich, Dr. Frank Umbach (EUCERS) and Prof. Dr. Alexander Fekete (Cologne University of Applied Sciences) spoke on the subject of "Terror Attacks on Energy Infrastructure – A Growing Threat?".

6 SUMMARY

BENJAMIN SCHARTE, DANIEL HILLER, TOBIAS LEISMANN, KLAUS THOMA

Fukushima, 9/11, hurricanes Katrina and Sandy – all have become bywords for disaster. No longer are they just a town in Japan, a date on the calendar or a couple of girl's names. Instead, they have come to symbolise the dangers of modern technology, the destructive rage of ideologies with no respect for human life and the untameable power of nature. They have also become synonymous with societies that failed to prepare properly – if they prepared at all –, societies whose defence mechanisms failed, whose emergency precautions were inadequate and whose basic ability to keep functioning was fully or partially impaired if not completely destroyed. In a nutshell, they are all classic examples of a serious lack of resilience.

What can our societies do to prevent serious adverse events like these from having such a devastating impact? How can they avert loss of life, minimise the financial losses suffered by private and public property owners and keep their basic functions up and running? Resilience can provide an answer to these questions. The key feature of resilient societies is that they are able to keep the damage caused by adverse events to an absolute minimum. This is the one principle shared by everyone who comes into contact with the complex concept of resilience, be it in their capacity as academics, practitioners, policymakers or indeed anything else. On the other hand, the best ways of delivering these goals, which measures can and should be taken, what the pitfalls and problems are and exactly what the concept does and does not include are all far more controversial questions that are the subject of complex debates in various different academic disciplines all over the world. This is at least partly due to the long history of the term "resilience". Over the course of the past 60 years, the term has been adopted by a variety of completely different scientific disciplines, beginning with developmental psychology and going on to include ecology, the social sciences and engineering. Chapter 1 provides a brief overview of the term's origins. Contemporary researchers tend to focus on different specific aspects of the concept, depending on which of these traditions they belong to.

For the "Resilien-Tech" project, we consciously chose to focus on resilience in the context of applied security research. The project's goal was to achieve a better understanding of the concept of resilience as applied in the field of security research, so that concrete recommendations could be formulated for decision-makers in government, business and society as a whole. The recommendations contain proposals for how a resilience by design approach can be integrated into future research strategies so that critical infrastructure resilience can be increased and resilience can become a fundamental principle of technological and societal security solutions. Although the project did not focus on the legal and psychological aspects of the concept, these aspects are of course extremely important for the implementation of appropriate measures to increase the resilience of technological and social systems and should therefore be systematically taken into account. The focus of the "Resilien-Tech" project, however, was on the actors addressed by the field of applied security research and the question of how the public, the people affected by disasters, emergency responders, end users, policymakers and the research and academic communities can contribute to increasing society's resilience, as well as the concrete solutions that they require at their respective levels in order to do so.

The project began by developing a working definition of resilience based on a thorough review of the literature. According to this definition, resilience can be understood as the "the ability to repel, prepare for, take into account, absorb, recover from and adapt ever more successfully to actual or potential adverse events. Those events are either catastrophes or processes of change with catastrophic outcome which can have human, technical or natural causes." Adverse events include a wide range of phenomena, from terrorist attacks and waves of organised crime to natural disasters and large-scale industrial accidents. They also

include gradual, long-term change processes that can have a devastating impact on society once they cross a certain undetermined threshold. Examples of such processes are climate change, the population decline in Germany or – conversely – the growth of the global population.

The working definition and review of the literature provided a platform for organising and running three expert workshops. The outputs of the workshops were consolidated into a number of "lessons learned" that form the basis of the study's recommendations. The first workshop sought to explore national perspectives on the concept of resilience and clarify where the German security research community currently stands with regard to this interesting concept. It is clear from the content of Chapter 2 that the national perspective on resilience is still relatively strongly focused on theoretical social science discourse. At the same time, however, there is also a trend towards using resilience to try and bridge the gap between the apparently contradictory social and technological approaches to addressing security problems.

The second workshop broadened the perspective by taking a look at research initiatives and practical examples from around the world from which the debate in Germany stands to benefit enormously. It became apparent that the international debate is some way ahead of the debate in Germany and that the concept of resilience has already been incorporated into government research strategies and emergency plans in other parts of the world (see Chapter 3). In particular, there is a pronounced focus on the adoption of a holistic approach to making societies more resilient. Moreover, methodologies such as resilience engineering and resilience responsibilisation are the subject of intensive research and development, offering the prospect of enabling social subsystems – from critical infrastructure to local communities – to increase their specific resilience. In this context, resilience engineering refers to a new understanding of the role of engineering in security research. It involves making greater use of innovative technological solutions to security problems in the planning, implementation and operation of critical infrastructure. Meanwhile, the "Resilien-Tech" project uses "resilience responsibilisation" as an umbrella term for strategies geared towards helping the public to take more responsibility when adverse events occur. This involves e.g. the relevant government agencies and the public engaging in a dialogue as equal partners.

Finally, the third workshop sought to identify and assess the specific challenges, problems and opportunities associated with resilience in a business context. For example, the abovementioned dialogue and efforts to raise awareness of the relevant threats would appear to constitute valuable measures that the State should consider implementing for businesses, particularly small and medium-sized enterprises (see Chapter 4). Many businesses are currently not even aware of the problem. Moreover, the majority of businesses are unlikely to invest in measures to increase resilience unless they are given good reason to do so. Indeed, it appears that they are most likely to take action if they have been forced to "learn the hard way". In other words, it is only after an adverse event has caused them serious damage that businesses take appropriate contingency measures to prevent a recurrence. Other promising short- to medium-term strategies for increasing the resilience of businesses include a carrot-and-stick approach based on financial incentives and penalties. In keeping with the conclusions of Chapter 3, a review of international trends in this area revealed that Germany is still some way behind other countries in the field of Business Continuity Management (BCM). In the US, for example, company law in particular contains extensive BCM regulations that place various risk prevention and management requirements on enterprises. German companies can expect to see an increase in this type of regulation over the next few years.

The findings described in the "lessons learned" have been consolidated into ten wide-ranging recommendations that

very consciously address completely different aspects of the complex concept of resilience. Some are also aimed at different target groups and they operate on various different abstraction levels. The aim is to ensure that resilience really is implemented as a holistic concept so that it can provide the field of applied security research with enough value-added to justify the substantial amount of work invested in its study. Taken together, the recommendations can be seen as an agenda for creating the resilient society of the future. They set out the first few steps that need to be taken, whilst also raising several questions that will have to be answered before the goal of a more resilient society can be delivered.

RECOMMENDATION 1

Resilience should be employed as a holistic strategy for minimising the harmful impacts of adverse events on our society. *This will facilitate a sustainable improvement in the ability of complex systems to keep functioning, adapt, endure and learn in the face of external or internal shocks. In order for this to be possible, it will be necessary to research, develop and implement appropriate and coordinated technological, social and economic measures and to ensure that they are combined in an integrated manner.*

What does this mean?

Since resilience is in itself a rather vague concept, the adoption of a holistic approach is the key long-term benefit that the use of this term can bring to German society. Why is this the case? Because of its origins and the way it has been used in the past, there is a danger that the word "resilience" could degenerate into just another buzzword that is devoid of any real meaning and is intentionally used in completely different ways by different actors to suit their own particular ends. This danger can be averted through a consistent and clear understanding of the core features at the heart of resilience. In essence, resilient societies must be able to keep the human, economic and environmental damage caused by adverse events to an absolute minimum. They do this by making use of every realistically conceivable solution, irrespective of whether it involves technology, social tools – such as education or engaging as equal partners in a dialogue with the public – or economic incentives. One of the features that marks out a resilient society is the adoption of a holistic approach and the targeted, combined deployment of these different types of solution before, during and after an emergency. Resilient societies are distinguished by their ability to respond dynamically to the constant changes in their environment and adapt to unforeseen adverse events. Rather than being a static condition, resilience is in fact a property of dynamic and adaptable systems that are able to learn from past events. This understanding of resilience is already being employed in countries such as the US, the UK and Switzerland both as a basis for their research programmes and in concrete government policies. Serious consideration should be given to adopting a similar approach in Germany.

RECOMMENDATION 2

Metrics and indicators should be developed for evaluating vulnerability and resilience. *It is essential to develop well-designed and practical tools for producing quantitative comparisons of the vulnerability and resilience of societies and their subsystems. These tools will improve our ability to systematically identify weaknesses, establish the effectiveness of investments and determine how specific measures impact on resilience. The German research community should therefore take up the challenge of developing a practical method for measuring resilience.*

What does this mean?

Vulnerabilities can be identified, categorised, measured, described and compared. The vulnerability to specific threats of certain geographical, technological or other

entities is already assessed both in Germany and in other countries such as the US. The challenge is to consolidate these efforts and systematically extend them across different disciplines to cover all the systems that could potentially be affected and all the different types of threats. The need for further research is evident in view of the complex phenomena involved. The challenge of developing a suitable method for measuring resilience is even more difficult and a fully satisfactory solution has yet to be found. Researchers are confronted with numerous conceptual problems and methodological pitfalls, for example questions about the most important variables, about which indicators can best be used to measure them, whether it is possible to compare the resilience of different systems, which dimensions should be included and how should they be weighted, and whether the indicators should be qualitative or quantitative and absolute or relative. And, given its dynamic nature, how can resilience be meaningfully evaluated by making an assessment or taking a measurement at a single point in time? Despite all these unanswered questions, however, measuring resilience remains a worthwhile endeavour. Moreover, the measurement of resilience does not need to produce perfect results. The ability to make only a reasonably accurate comparison of the resilience of different entities would be enough to identify particularly resilient systems that can be used as models and particularly unresilient systems that are in need of help. The German security research community – with firm backing from policymakers – should therefore take up this challenge in partnership with all the relevant actors such as the operators of critical infrastructure.

RECOMMENDATION 3

Methods should be developed for modelling and simulating complex socio-technical systems that are critical to our society. *Security research should place greater emphasis on research initiatives that develop existing modelling approaches and help to simulate the impacts of adverse events, particularly in terms of cascading effects. It will be especially important to guarantee reliable identification of system-critical nodes and interfaces that could trigger cascade effects if damaged, as well as to predict the system's potential for self-organisation.*

What does this mean?

In order to make targeted improvements to the resilience of complex systems, the relevant actors require a detailed and accurate understanding of the systems' behaviour and how they work, particularly under extreme conditions. Since they can obviously not afford to simply wait and see what happens when an external or internal shock occurs, they need the ability to simulate extreme events as realistically as possible before they occur, both during the system planning stage and during normal operation when the system is working as intended. This allows them to identify weaknesses, plan counter-measures, correct faults and do everything in their power to prepare the system as fully as possible for the occurrence of adverse events. This is exactly what the ability to simulate and model complex systems enables them to do. A wide variety of modelling techniques already exist today. However, as the complexity of systems continues to increase and the interdependencies between previously discrete subsystems multiply, even more comprehensive, ultra-advanced methods are required in order to reliably model how systems will behave when unforeseen events occur. More research is therefore needed into methods that go beyond merely computing the outcomes of predetermined scenarios. Future modelling techniques should be capable of modelling the entire system without relying on pre-established scenarios. The aim is to produce multimodal simulations that use an integrated approach to model technological and social systems and the complex interactions between them. This will require investment in R&D, including efforts to standardise different modelling approaches and make them compatible with each other.

RECOMMENDATION 4

Resilience engineering should be established as an independent discipline. Research, development and implementation of resilient critical infrastructure design and construction should be promoted. *Innovative technology should be employed to ensure that infrastructure is capable of meeting the needs of the 21st century. Resilience engineering involves the development of customised technological and interdisciplinary methods and solutions for building resilience into systems that are critical to our society.*

What does this mean?

The sustained and reliable functioning of critical infrastructure in our modern society is, as the name suggests, critical to its survival. Society as we know it simply could not exist without energy, water, food, transport, communication, etc. Resilience engineering is the best way of guaranteeing and indeed increasing the ability of critical infrastructure to keep functioning, adapt, endure and learn in the face of different types of adverse events. The term "resilience engineering" refers to interdisciplinary engineering R&D into procedures and methods for increasing the ability of systems that play a key role in our society to endure, adapt and self-organise. It involves the consistent incorporation from an early stage of technological solutions to all kinds of security problems into every aspect of the planning and implementation of major social projects – from the individual level to the overall system level. Its goal is to maintain the critical sub-functions of these systems in a controlled manner, even when damage to the system forces them to operate outside their normal parameters, thus allowing catastrophic total system failure to be averted. It requires customised technological solutions for increasing the resilience of individual infrastructures. At the same time, the effectiveness of these solutions and their impact on the system as a whole must be optimised and they should be complemented by smart solutions from other fields such as economics, ecology and the social sciences. Examples might include technologies such as self-healing, adaptive materials or smart, adaptable buildings that use energy self-sufficient automated sensor networks. Resilience engineering also prevents the development of incompatible isolated solutions. This is where the holistic aspect of resilience comes in, since future technologies will need to be compatible both with each other and with any other potential external solutions. This new understanding of the role of engineering in terms of ensuring and increasing the resilience of society and in particular its critical infrastructure should play a greater part in Germany's national security research programme and in particular the German government's security-related strategies such as the National Plan for Critical Infrastructure Protection (KRITIS).

RECOMMENDATION 5

Strategies should be developed and implemented for sustainably strengthening people's self-reliance in the face of adverse events. *In order to ensure that they are actively involved in shaping resilient societies, the public should be engaged in a dialogue as equal partners and provided with wide-ranging opportunities to participate at a variety of different, decentralised levels. Government can encourage people to take precautions against risks and promote their acceptance, for example through school curriculum content, by supporting volunteering with the fire service, Red Cross, humanitarian aid organisations such as Germany's THW and other emergency services, or through other concrete measures.*

What does this mean?

The first step is to create a responsible awareness among the public of the dangers that exist. People need to recognise the threat of adverse events before they can make the mental and practical preparations that will allow them to withstand any shocks with as little damage as possible. Regular emergency and disaster exercises are one example of the measures needed to create this awareness and enable efficient emergency planning and

preparedness. The procedures that they rehearse and the routine behaviours that they establish can help to save lives in the event of an emergency. Regular rehearsal of what to do in the event of a disaster also gives people the belief that they are well equipped and prepared to cope with any type of disaster. And the mere fact of believing means that they are to some extent better able to do so. Many people in Germany already volunteer with the fire service or other emergency services. It is important to sustain their involvement, attract still more recruits and use these people as a resource for raising awareness about disasters among the general public. Another avenue that will need to be explored more thoroughly going forward is the incorporation of the relevant learning content into school curricula and continuing professional development provision. This focus on educating and training people in order to increase their resilience is an extremely important part of creating a more resilient society. In this context, it is essential to prevent information overload from causing people to become blasé about the dangers, as well as to ensure that they do not descend into a state of permanent panic because of the enormity of the threats involved. By combining different methods for enhancing people's self-reliance it should, in the longer term, be possible not only to increase individual empowerment but also to strengthen social capital and social cohesion within local communities. In the event of a disaster, these factors could ultimately have a major say in how well different geographical locations manage to cope with the relevant impacts. Research initiatives and practical strategies aimed at strengthening the public's self-reliance should therefore be promoted at different levels.

RECOMMENDATION 6

The case should be made for the long-term value-added that resilience can bring to our society. *We need to adopt a wider perspective, abandoning short-termist and short-sighted cost-benefit optimisation in favour of strategic, long-term thinking and actions. Future research initiatives should therefore incorporate the economic aspects right from the outset, demonstrating why it is worth investing in resilience and making the business case for why resilience should not simply be regarded as a cost.*

What does this mean?

In market economies, investment decisions are fundamentally based on cost-benefit analyses of varying degrees of sophistication. Government investment decisions are to some extent exempt from this principle, since in many cases they are not expected to generate direct monetary benefits. Nevertheless, within the constraints of the pre-defined requirements that it is subject to, even the State tries to get the best possible return from its limited resources. In other words, it attempts to ensure that its resources are used as efficiently and effectively as possible. In this context, the method used to assess whether the resources have been employed efficiently and effectively is absolutely key. Measures geared towards increasing society's resilience cost money, be it necessary investment in R&D, the additional cost of building resilient critical infrastructure or the introduction of the concept into school curricula. Nevertheless, resilience is more than just a "costly add-on" or unnecessary luxury – it is in fact a key requirement of sustainable investments. In view of the ever greater challenges confronting our societies, systems which collapse at the first tiny sign of trouble because they were designed according to radical cost-cutting principles hardly constitute a sustainable long-term model. In a sustainability-based approach, the extra initial outlay required to create resilience soon pays for itself, not only in terms of the human suffering that it prevents in the event of a disaster but also financially. According to a report by the Multi-Hazard Mitigation Council, for every dollar spent on pre-event mitigation related to earthquakes, wind and flooding, about four dollars were saved in post-event damages (see 3.2.2). This does, of course, require a detailed knowledge of the exact pay-back of specific investments

in different locations. Future research initiatives geared towards increasing resilience should thus build in the economic aspects right from the outset.

RECOMMENDATION 7

Incentives should be created for businesses to increase their resilience. *Consideration should be given to the introduction of a standardised resilience monitoring system that would be supported and, if necessary, coordinated by the State. The system would provide appropriate incentives to socially critical businesses that were able to demonstrate an increase in their resilience. It would also seek to influence the behaviour of those socially critical businesses that failed to take measures to improve their resilience by penalising them with higher insurance premiums, additional levies, etc.*

What does this mean?

In essence, the purpose of a company is to maximise the profits obtained from its business. In order to do this, it needs the business to run as smoothly and with as little disruption as possible. The majority of companies therefore make some kind of provision for risks, at least implicitly. In other words, they take contingency measures to protect them against certain adverse events. The key drivers are the extent of the losses that they are likely to suffer and the probability of the event actually occurring. However, the business world is no different to anywhere else insofar as resilience still concerns unforeseen events that are highly unlikely to occur. Even though natural disasters, for example, can cause huge losses, only a handful of businesses are prepared for this type of threat. The impression is that any investments will not be cost-effective because of the low probability of such events. Consequently, it will be necessary to find ways of helping businesses to increase their resilience with regard to low-probability adverse events that can nonetheless have a serious impact. One promising idea is the introduction of compulsory insurance against adverse events, although it will be necessary to give insurers incentives to provide this type of policy. Another option would be to introduce government monitoring of the measures taken by companies to increase their resilience. This would require regulation of what businesses are expected to do in order to become more resilient, for example carrying out emergency and disaster exercises or the introduction of certain redundancies and buffers into their business processes. The State would then reward compliance with these regulations or penalise companies that failed to observe them. More work is required to establish how this system could be effectively implemented without jeopardising companies' competitiveness.

RECOMMENDATION 8

An early warning system should be established, featuring compulsory reporting of adverse events. *While the probability of major adverse events may be low, they do nonetheless occur from time to time. A national early warning system should therefore be established, together with industry-specific compulsory reporting arrangements (i.e. the criteria for reporting events would vary from industry to industry). Businesses would thus be under an obligation to report security-critical events.*

What does this mean?

Most companies do not anticipate sudden major shocks in their day-to-day business and many are therefore unaware of the relevant threats. The roll-out of compulsory reporting for certain types of incident would help to raise awareness on this issue. It would act as an early warning system and contribute significantly to better prevention. It is likely that companies will be concerned that compulsory reporting could lead to them being publicly named and shamed, causing damage to their business. These concerns should be taken seriously and should

be addressed through the design of the compulsory reporting system. Furthermore, thorough research should be carried out before the regulations are introduced in order to establish which events should be subject to compulsory reporting in different industries, exactly what information needs to be provided and who it should be reported to. The system should only apply to companies if a partial or total collapse of their business could have a serious negative impact on the local, regional or national economy. Compulsory reporting could also prove to be especially valuable for combatting the growing threat of cybercrime, since it would alert people to probable or imminent attacks and enable targeted counter-measures to be taken. Once again, it would be necessary to design the system in such a way as to prevent any risk of the companies involved suffering damage to their reputation or any other disadvantage.

RECOMMENDATION 9

A national resilience strategy should be developed. *In the broader context of sustainable development, it will be necessary to develop an overarching vision of resilient societies. The holistic concept of resilience is not something that can simply be ordained by law. A national resilience strategy, on the other hand, can provide a consistent and comprehensive basis for addressing the numerous challenges associated with an increasingly complex, high-tech world, serving as a platform for the subsequent development of targeted solutions for specific problems.*

What does this mean?

It will only be possible to maximise the benefits that the holistic concept of resilience can provide to society if policymakers buy into the concept, recognising it as necessary and giving it their full support. The first step towards this goal is the formulation of a national resilience strategy. By developing such a strategy, government and the responsible authorities would be sending out a signal that they recognise that increasing the resilience of society and its relevant subsystems is absolutely key to enabling them to continue functioning successfully. The strategy would also provide a framework for developing specific plans to implement measures geared towards increasing resilience, for example in the critical infrastructure sector. It would also involve continuous monitoring of individual government departments – including e.g. the emergency planning authorities that report to them – in order to assess whether they have adequately adopted resilience as an organising principle in their work and whether they cooperate sufficiently with other responsible agencies on implementation actions. Resilience could constitute the underlying principle of all future research initiatives, particularly in the field of applied, solution-oriented security research. This would allow innovative ideas and approaches to be identified more rapidly and effectively, gaps in the research to be filled and the potential value-added that individual solutions contribute to the overall resilience of society to be reliably evaluated. Recommendations 2 to 8 can thus be understood as the topics and fields where further R&D will enable Germany and Europe as a whole to become more resilient.

RECOMMENDATION 10

Resilience should be established as a key component of sustainable development. *Sustainability means finding a way of living together that meets the needs of the people alive today without jeopardising future generations' ability to in turn meet their own needs. For this to be possible, societies must be capable of surviving major challenges. The fundamental characteristics of resilient systems are the ability to keep functioning, adapt, endure and learn. These are all key to a society's ability to survive. The concept of resilience thus bridges the gap between security and sustainability research.*

What does this mean?

Over the past two decades, sustainability has become one of the most important policy areas throughout the world. This is particularly true in Germany, where the "Energiewende" (energy transition concept) is already attempting to put one of the core principles of sustainable development into practice. Of course, sustainability means much more than simply switching a society's energy supply from fossil fuels to renewables. The United Nations, for example, has identified seven key components of sustainable development which provide a basis for the content of the concept's three key dimensions. Development is sustainable if it meets the environmental, economic and social needs both of the people alive today and of future generations. This model is known as the "three pillars of sustainability". The seven key components underpinning this model of sustainable development are decent jobs, a sustainable energy supply, food security and sustainable agriculture, sustainable urban development, access to clean drinking water, sustainable use of our oceans and resilient societies. Each of these key components must be broken down still further to allow concrete recommendations for increasing the sustainability of our societies to be formulated. Nonetheless, it is clear that it will be necessary to implement all seven of these key components with equal care if global development is to be truly sustainable. In this context, resilience involves maintaining the ability to keep functioning, adapt, endure and learn in the face of underlying change processes and concurrent major adverse events. This ability is critical to sustainability, i.e. human society's capacity to survive in the future. In other words, resilience must form an integral part of any successful model of sustainability. Both security and sustainability researchers should therefore incorporate resilience into their work and carry out the corresponding research projects.

Taken together, these ten recommendations constitute a blueprint for how to build a more resilient society. Furthermore, they provide a valuable toolkit for decision-makers. As mentioned above, they cover an extremely wide range of completely different aspects of the complex concept of resilience. Without unnecessarily narrowing the perspective and undermining the usefulness of the concept, many of the recommendations do nonetheless focus on ways of increasing critical infrastructure resilience, in keeping with the goals of this project. In this context, it is important to understand complex and interdependent critical infrastructures as socio-technical systems. For both critical infrastructure and for society as a whole, it will be necessary to integrate a resilience by design approach into future research strategies so that resilience can become a fundamental principle of all technological and societal security solutions. This will be key to ensuring that there is no repeat of 9/11 or Fukushima. It will be key to limiting the human and material cost of future Katrinas, Sandys and Haiyans, even though the storms themselves will be no less powerful. And it will be key to ensuring that Germany can respond resiliently should it ever be affected by such a serious adverse event.

7 LITERATURE

Abramson, M.: *For Lower Ninth Residents, New Orleans Saints' Super Bowl Victory Serves as a Symbol of Resiliency*, 2010. URL: http://www.nydailynews.com/sports/football/ninth-residents-new-orleans-saints-super-bowl-victory-serves-symbol-resiliency-article-1.196260 [Accessed: 06. 08. 2013].

Adger, N.: "Social and Ecological Resilience. Are They Related?". In: *Progress in Human Geography*, 24: 2000, pp. 347 – 364.

Al-Khudhairy, D./Axhausen, K./Bishop, S./Herrmann, H./Hu. B./Kröger, W./Lewis,T./MacIntosh, J./Nowak, A./Pickl, S./Stauffacher, D./Tan, E.: "Towards Integrative Risk Management and More Resilient Societies". In: *The European Physical Journal Special Topics*, 214: 1, 2012, pp. 571 – 595.

Badische Zeitung: *Insgesamt 8 Tote bei Hochwasser – Weiter Gefahr von Deichbrüchen*, 2013. URL: http://www.badische-zeitung.de/nachrichten/panorama/insgesamt-8-tote-bei-hochwasser-weiter-gefahr-von-deichbruechen--72691971.html [Accessed: 01. 08. 2013].

Bara, C./Brönnimann, G.: *CRN Report. Risk Analysis. Resilience – Trends in Policy and Research* (Focal Report 6, Crisis and Risk Network), Zürich: Center for Security Studies (CSS), ETH Zürich 2011.

Bauman, Z.: *Liquid Modernity*, Cambridge: Polity Press/Blackwell Publishing 2000.

Beck, U./Bonß, W.: *Die Modernisierung der Moderne*, Frankfurt a. M.: Suhrkamp 2001.

Beck, U.: *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*, Frankfurt a. M.: Suhrkamp 2007.

Beckmann, K.: „Jetzt auch noch resilient?". In: Beckmann, K. (Hrsg.): *Anforderungen an die Krisenfestigkeit der Städte,* Deutsches Institut für Urbanistik, Difu Sonderveröffentlichung 2012, pp. 7 – 13.

Bloomberg: *Coke Gets Hacked And Doesn't Tell Anyone*, 2012. URL: http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html [Accessed: 22. 08. 2013].

Bonß, W.: „Für eine neue Kultur der Unsicherheit". In: Steinmüller, K./Gerhold, L./Beck, M.-L. (Hrsg.): *Sicherheit 2025. Forschungsforum Öffentliche Sicherheit*, Schriftenreihe Nr. 10, 2012). URL: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_10.pdf [Accessed: 02. 10. 2013].

Brand, F.: *Ecological Resilience and its Relevance within a Theory of Sustainable Development*. Leipzig: UFZ Centre for Environmental Research 2005.

Bürkner, H.-J.: *Vulnerabilität und Resilienz: Forschungsstand und sozialwissenschaftliche Untersuchungsperspektiven*, 2010. URL: http://www.irs-net.de/download/wp_vr.pdf [Accessed: 02. 10. 2013].

Cabinet Office: *A Summary of the 2012 Sector Resilience Plans*, 2012. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62312/Summary-2012-Sector-Resilience-Plans.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Civil Contingencies Act 2004: A Short Guide (Revised)*, URL: http://www.essex.gov.uk/Your-Council/Local-Government-Essex/Documents/15mayshortguide.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Community Emergency Plan Toolkit*, 2011. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60925/Community-Emergency-Plan-Toolkit.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to Improving the Resilience of Critical Infrastructure and Essential Services*, 2011b. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *National Risk Register of Civil Emergencies*, 2013. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Preparing for Emergencies: Guide for Communities*, 2011c. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60923/PFE-Guide-for-Communities_0.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Sector Resilience Plan for Critical Infrastructure 2010*, 2010. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62310/sector-resilience-plan.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *Strategic National Framework on Community Resilience*, 2011d. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60922/Strategic-National-Framework-on-Community-Resilience_0.pdf [Accessed: 30. 07. 2013].

Cabinet Office: *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*, 2011e. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Accessed: 30. 07. 2013].

Cardoza, B.A.: *Building a Business Impact Analysis (BIA) Process: A Hands-on Blueprint*, CRC Press 2006.

Carter, J.: *The State of the Union Address Delivered Before a Joint Session of the Congress*, 1980. URL: http://www.presidency.ucsb.edu/ws/?pid=33079#axzz2hK5mhUm7 [Accessed: 18. 10. 2013].

Centre for the Protection of National Infrastructure (CPNI): *Centre for the Protection of National Infrastructure*, 2013. URL: http://www.cpni.gov.uk/ [Accessed: 07. 08. 2013].

Churchill, W.: *Shipbuilding, Repairs, Maintenance, etc. – Personnel (Vote 8, Section 1)*, 1913. URL: http://hansard.millbanksystems.com/commons/1913/jul/17/shipbuilding-repairs-maintenance-etc#S5CV0055P0_19130717_HOC_426 [Accessed: 22. 01. 2014].

CIA: *The World Factbook*, 2013. URL: https://www.cia.gov/library/publications/the-world-factbook/ [Accessed: 15. 12. 2013].

Coaffee, J./Murakami Wood, D./Rogers, P.: *The Everyday Resilience of the City. How Cities Respond to Terrorism and Disaster* (New Security Challenges, Hrsg.: Croft, S.), Basingstoke: Palgrave Macmillan 2008.

Coaffee, J./Wood, D./Rogers, P.: *The Everyday Resilience of the City. How Cities Respond to Terrorism and Disaster, New Security Challenges*, Hrsg.: Croft, S., Basingstoke: Palgrave Macmillan 2009.

Coaffee, J.: "Rescaling and Responsibilising the Politics of Urban Resilience: From National Security to Local Place-Making". In: *Politics*, 33: 4, 2013b, pp. 240–252. URL: http://onlinelibrary.wiley.com/doi/10.1111/1467-9256.12011/abstract [Accessed: 22. 10. 2013].

Coaffee, J.: *Making the Business Case for Urban Resilience*, 2013. URL: http://urbanresilience.net/2013/07/01/making-the-business-case-for-urban-resilience/ [Accessed: 19.07.2013].

Cranfield University: *Resilience*, 2013. URL: http://www.cranfield.ac.uk/cds/cisr/resilience.html [Accessed: 10.01.2013].

Cutter, S./Barnes, L./Berry, M./Burton, C./Evans, E./Tate, E./ Webb, J.: "A Place-Based Model for Understanding Community Resilience to Natural Disasters". In: *Global Environmental Change*, 18: 2008, pp. 598 – 606.

Cutter, S./Boruff, B./Shirley W.: "Social Vulnerability to Environmental Hazards". In: *Social Science Quarterly*, 84: 2, 2003, pp. 242 – 261.

DUDEN: *Resilienz*, 2013. URL: http://www.duden.de/rechtschreibung/Resilienz [Accessed: 15.01.2013].

Dunn Cavelty, M.: *Das Resilienz-Paradox: Zwischen Ohnmacht und Allmacht*, 2013. URL: http://www.sicherheitspolitik-blog.de/2013/04/24/das-resilienz-paradox-zwischen-ohnmacht-und-allmacht/ [Accessed: 02.10.2013].

Edwards, C.: *Resilient Nation*, London: Demos 2009.

Essex Resilience Forum (ERF): *Essex Resilience Forum*, 2013. URL: http://microsites.essex.gov.uk/essex_resilience/ [Accessed: 07.08.2013].

ETH Risk Center: *About Us*, 2013. URL: http://www.riskcenter.ethz.ch/about/index [Accessed: 22.07.2013].

ETH Risk Center: *Kröger, Wolfgang, Prof. Dr.*, 2013b. URL: http://www.riskcenter.ethz.ch/people/wkroeger [Accessed: 22.07.2013].

European Union: *Sustainable Development*, 2013. URL: http://ec.europa.eu/environment/eussd/ [Accessed: 02.08.2013].

Federal Ministry of the Interior (BMI): *National Plan for Critical Infrastructure Protection (KRITIS Strategy)*, 2013. URL: http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf [Accessed: 02.10.2013]

Federal Office for Information Security: *BSI Standard 100-4 – Business Continuity Management*, 2008.

Federation of American Scientists (FAS): *Presidential Policy Directives (PPDs). Barack Obama Administration*, 2013. URL: http://www.fas.org/irp/offdocs/ppd/index.html [Accessed: 31.07.2013].

Felgentreff, C./Kuhlicke, C./Westholt, F.: „Naturereignisse und Sozialkatastrophen". In: F*orschungsforum Öffentliche Sicherheit*, Schriftenreihe Sicherheit Nr. 8, 2012.

Fiksel, J.: "Designing Resilient, Sustainable Systems". In: *Environmental Science & Technology*, 37: 23, 2003, pp. 5330 – 5339.

Filkins, D.: *Kabul Attack Shows Resilience of Afghan Militants*, 2010. URL: http://www.nytimes.com/2010/01/19/world/asia/19afghan.html?pagewanted=all&_r=1& [Accessed: 06.08.2013].

Floeting, H.: „Von harten Zielen und weichen Maßnahmen – Sind „resiliente" Städte „sichere" Städte?". In: Beckmann, K. (Hrsg.): *Anforderungen an die Krisenfestigkeit der Städte*, Deutsches Institut für Urbanistik, Difu Sonderveröffentlichung 2012, pp. 14 – 22.

Flynn, S.: "A National Security Perspective on Resilience". In: *Resilience: Interdisciplinary Perspectives on Science and Humanitarianism*, 2: 2011, pp. i-ii.

Frankfurter Allgemeine Zeitung: *Schadensbilanz des Hochwassers. Rekordverdächtige Flut*, 2013. URL: http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/schadensbilanz-des-hochwassers-rekordverdaechtige-flut-12276172.html [Accessed: 01. 08. 2013].

Gebhardt, H./Glaser, R./Radtke, U./Reuber, P. (Hrsg.): *Geographie. Physische Geographie und Humangeographie*, Heidelberg: Spektrum Akademischer Verlag 2011.

Gov.uk: *Policy. Improving the UK's Ability to Absorb, Respond to, and Recover from Emergencies*, 2013. URL: https://www.gov.uk/government/policies/improving-the-uks-ability-to-absorb-respond-to-and-recover-from-emergencies [Accessed: 07. 08. 2013].

Günther, E.: *Klimawandel und Resilience Management.* Wiesbaden: Gabler Edition Wissenschaft 2009.

Gürtler, L./Studer, U./Scholz, G.: *Tiefensystemik. Band 1. Lebenspraxis und Theorie. Wege aus Süchtigkeit finden.* Münster: Monsenstein und Vannerdat, 2010.

Guyton, P.: *Passau. Eine Geisterstadt voller Wasser*, 2013. URL: http://www.zeit.de/gesellschaft/zeitgeschehen/2013-06/hochwasser-passau-jahrhundertflut [Accessed: 01. 08. 2013].

Haut Comité Français pour la Défense Civile (HCFDC): *Pavillon Orange pour la Sauvegarde des Populations*, 2013. URL: http://www.pavillon-orange.org/index.php [Accessed: 29. 07. 2013].

Haut Comité Français pour la Défense Civile (HCFDC): *Presentation of the French High Committee for Civil Defense*, 2013b. URL: http://translate.google.fr/translate?hl=fr&sl=fr&tl=en&u=http%3A%2F%2Fwww.hcfdc.org%2Fasso%2F [Accessed: 26. 07. 2013].

Hazards and Vulnerability Research Institute (HVRI): *Changes and Improvements in the SoVI® Formulation for 2006-10*, 2013. URL: http://webra.cas.sc.edu/hvri/products/sovi_details_2006.aspx [Accessed: 17. 07. 2013].

Hazards and Vulnerability Research Institute (HVRI): *Social Vulnerability Index for the United States – 2006 – 2010*, 2013b. URL: http://webra.cas.sc.edu/hvri/products/sovi.aspx [Accessed: 17. 07. 2013].

Hazards and Vulnerability Research Institute (HVRI): *Social Vulnerability Index for the United States. Components*, 2013c, URL: http://webra.cas.sc.edu/hvri/docs/sovi0610_factorsb.pdf [Accessed: 07. 08. 2013].

HBGary: *Cybersecurity Directly Affects Investor Attitudes, New HBGary Survey Finds Survey Reveals Investors Demand More Transparency About Corporate Cyberattacks.* URL: http://www.hbgary.com/article/cybersecurity_directly_affects_investor_attitudes_new_hbgary_survey_finds_survey_reveals [Accessed: 22. 08. 2013].

HM Government: *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [Accessed: 30. 07. 2013].

HM Government: *CONTEST. The United Kingdom's Strategy for Countering Terrorism*, 2011. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf [Accessed: 19. 07. 2013].

HM Government: *How Prepared Are You? Business Continuity Management Toolkit*, URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/137994/Business_Continuity_Managment_Toolkit.pdf [Accessed: 30. 07. 2013].

Holling, C.: "Resilience and Stability of Ecological Systems". In: *Annual Review of Ecology and Systematics*, 4: 1973, pp. 1 – 23.

Holling, C.: "Engineering Resilience vs. Ecological Resilience". In: Schulze, P. (Hrsg.): *Engineering Within Ecological Constraints*, Washington, D.C.: National Academy Press 1996, pp. 31 – 44.

Holling, C.: *From Complex Regions to Complex Worlds*, 2004. URL: http://www.ecologyandsociety.org/vol9/iss1/art11 [Accessed: 06. 10. 2013].

Hollnagel, E.: Prologue: "The Scope of Resilience Engineering". In: Hollnagel, E./Pariès, J./Woods, D./Wreathall, J. (Hrsg.): *Resilience Engineering in Practice. A Guidebook*, Farnham, Surrey: Ashgate 2011, pp. 29 – 39.

Ibert, O.: *Vulnerabilität und Resilienz – die Notwendigkeit einer Beobachterperspektive zweiter Ordnung*, 2013. URL: http://www.sicherheitspolitik-blog.de/2013/05/02/resilienz-ibert/ [Accessed: 06. 10. 2013].

IBM: *IBM Intelligent Operations Center*, 2013. URL: http://www-03.ibm.com/software/products/us/en/intelligent-operations-center/ [Accessed: 19. 07. 2013].

International Organization for Standardization: *ISO 22301: Societal security — Business continuity management systems — Requirements*, 2012.

International Organization for Standardization: *Information technology - Security techniques - Information security risk management*, 2011.

International Organization for Standardization: *ISO 22313: Societal security - Business continuity management systems – Guidance*, 2012.

International Energy Agency (IEA): *Medium-Term Renewable Energy Market Report Executive Summary*, 2013. URL: http://www.iea.org/Textbase/npsum/MTrenew2013SUM.pdf [Accessed: 22. 01. 2014].

International Energy Agency (IEA): *Topic: Energy Security*. URL: http://www.iea.org/topics/energysecurity/ [Accessed: 22. 01. 2014].

International Energy Agency (IEA): *World Energy Outlook*, 2012.URL:http://www.iea.org/publications/freepublications/publication/german.pdf [Accessed: 22. 01. 2014].

Israel Ministry of National Infrastructures, Energy and Water Resources: *The Natural Gas Sector in Israel*. URL: http://energy.gov.il/English/Subjects/Natural%20Gas/Pages/GxmsMniNGEconomy.aspx [Accessed: 22. 01. 2014].

Johnsson, J./Polson, J.: *Sandy Cuts Power to More Than 8 Million in U.S. Northeast*, 2012. URL: http://www.bloomberg.com/news/2012-10-30/hurricane-blackouts-cut-power-to-about-8-million-customers.html [Accessed: 13. 12. 2013].

Kaschner, H.: Neues Risiko Terrorismus. Entgrenzung, Umgangsmöglichkeiten, Alternativen. Wiesbaden: VS-Verlag für Sozialwissenschaften, 2008.

Kaufmann, S./Blum, S.: "Governing (In)Security: The Rise of Resilience". In: Gander, H.-H./Perron, W./Poscher, R./Riescher, G./Würtenberger, T. (Hrsg.): *Resilienz in der offenen Gesellschaft. Symposium des Centre for Security and Society (Sicherheit und Gesellschaft. Freiburger Studien des Centre for Security and Society)*, Baden-Baden: Nomos 2012, pp. 235 – 257.

Kaufmann, S.: „Resilienz als ‚Boundary Object'". In: Daase, C./Offermann, P./Rauer, V. (Hrsg.): *Sicherheitskultur – Soziale und politische Praktiken der Gefahrenabwehr*, Frankfurt a. M.: campus Verlag 2012, pp. 109 – 131.

Kaufmann, S.: *Resilienz – ja, bitte! Nur wie?*, 2013. URL: http://www.sicherheitspolitik-blog.de/2013/04/29/resilienz-kaufmann/ [Accessed: 06. 10. 2013].

Kennett, J.: *Katrina, Rita Cost to Oil Industry Rises to Record $17 Billion*, 2006. URL: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aZjgqvrTSgrs&refer=exclusive [Accessed: 18. 12. 2013].

Kolliarakis, G.: *Das Konzept der Resilienz in der Sicherheitsforschung*, 2013. URL: http://www.sicherheitspolitik-blog.de/fokus/konzept-der-resilienz/ [Accessed: 06. 10. 2013].

Kreissl, R.: *Paradoxien der Sicherheitspolitik*, 2007. URL: http://www.irks.at/assets/irks/Publikationen/Working%20Paper/IRKS_WP01_Kreissl.pdf [Accessed: 06. 10. 2013].

Kröger, W.: "An Overview of Swiss Research on Vulnerability of Critical Infrastructure". In: Thoma, K. (Hrsg.): *European perspectives on security research*, Heidelberg: Springer Verlag 2011, pp. 67 – 79.

Lorenz, D.: "The Diversity of Resilience: Contributions from a Social Science Perspective". In: *Natural Hazards* 67: 7, 2013, pp. 7 – 24.

Luthar, S./Cicchetti, D./Becker, B.: "The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work". In: *Child Development*, 71: 3, 2000, pp. 543 – 562.

Mathews, S.: *From Agit Prop to Free Space: The Architecture of Cedric Price*, London: Black Dog Publishing 2007.

Mayer, J.: *Resilienz und Bevölkerungsschutz – eine Frage des Selbstschutzes?!*, 2013. URL: http://www.sicherheitspolitik-blog.de/2013/05/15/resilienz-mayer/ [Accessed: 06. 10. 2013].

Mazzetti, M./Sanger, D.: *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, 2013. URL: http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?hp&_r=0 [Accessed: 14. 12. 2013].

Meuser, M./Nagel, U.: „Experteninterviews – vielfach erprobt, wenig bedacht: Ein Beitrag zur qualitativen Methodendiskussion". In: Bogner, A./ Littig, B./Menz, W. (Hrsg.): *Das Experteninterview. Theorie, Methode, Anwendung*, Opladen: Leske/Budrich 2002, pp. 71 – 94.

Muir, H./Cowan, R.: *Four Bombs in 50 Minutes – Britain Suffers its Worst-Ever Terror Attack*, 2005. URL: http://www.guardian.co.uk/uk/2005/jul/08/terrorism.july74 [Accessed: 12. 03. 2013].

Nachhaltigkeitsrat: *Was ist Nachhaltigkeit?*, 2013. URL: http://www.nachhaltigkeitsrat.de/nachhaltigkeit/ [Accessed: 02. 08. 2013].

Parliament of the United Kingdom: *Civil Contingencies Act 2004*, 2004. URL: http://www.legislation.gov.uk/ukpga/2004/36/pdfs/ukpga_20040036_en.pdf [Accessed: 30. 07. 2013].

Perrow, C.: *Normal Accidents. Living With High Risk Technologies* (Revised edition), Princeton, NJ: Princeton University Press, 1999.

Perrow, C.: "Organizing to Reduce the Vulnerabilities of Complexity". In: *Journal of Contingencies and Crisis Management*, 7: 3, 1999b, p. 155.

Peter, A./Wernz, J.: „Operationelle Risiken". In: *RisikoManager*, 23: 2012, pp. 11 – 18.

Pimm, S.: *The Balance of Nature? Ecological Issues in the Conservation of Species and Communities*, Chicago: University of Chicago Press 1991.

Plodinec, M.: *Definitions of Resilience: An Analysis*, Community and Regional Resilience Institute 2009.

Prior, T./Roth, F.: "Disaster, Resilience and Security in Global Cities". In: *Journal of Strategic Security*, 6: 2, 2013, pp. 59 – 69.

Rijpma, J.: "Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory". In: *Journal of Contingencies and Crisis Management*, 5: 1, 1997, pp. 15 – 23.

Sacks, A.: *9-11 Dogs Dodge Ailments. Most Don't Suffer from WTC Dust*, 2006. URL: http://www.nydailynews.com/archives/news/9-11-dogs-dodge-ailments-don-suffer-wtc-dust-article-1.642258 [Accessed: 15. 07. 2013].

Saul, M.: *Parts of New York City Evacuated for Hurricane Sandy*, 2012. URL: http://online.wsj.com/article/SB10001424052970203880704578084701930663668.html# [Accessed: 15. 10. 2013].

Slovic, P. (Hrsg.): *The Perception of Risk*, Virginia: Earthscan 2000.

Smith, G.: *"Mold Awareness Workshops" Offer Sandy-Affected Residents Tips and Tools to Combat Dangerous Spores*, 2013. URL: http://www.nydailynews.com/new-york/mold-awareness-workshops-sandy-victims-stay-safe-article-1.1259827 [Accessed: 06. 08. 2013].

Springer Gabler Verlag (Hrsg.): *Gabler Wirtschaftslexikon, Stichwort: Lagebericht*. URL: http://wirtschaftslexikon.gabler.de/Archiv/58187/lagebericht-v9.html [Accessed: 22. 08. 2013]

Stangl, R./Stollenwerk, J.: *Studie S6. Terminologie von Katastrophenmanagementkreisläufen/-Phasen* (KIRAS-Projekt SFI@SFU), Wien: Sigmund Freud Privat Universität 2011.

Stock, J./Watson, M.: *Introduction to Econometrics*, Harlow, Essex: Pearson Education Limited 2012.

Stoddard, E.: *Conceptual Models of Human Behaviour in Disasters*, El Paso: Texas Western Press 1968.

The London Resilience Team: *About Us*, 2013. URL: http://www.london.gov.uk/mayor-assembly/mayor/london-resilience/preparing-london/about-us [Accessed: 07. 08. 2013].

The London Resilience Team: *London Strategic Emergency Plan*, 2010. URL: http://www.london.gov.uk/sites/default/files/archives/london-prepared-Strategic-Emergency-Plan-v6.pdf [Accessed: 30. 07. 2013].

The National Academies: *Disaster Resilience. A National Imperative*, Washington, D.C.: 2012.

The National Academies: *Disaster Resilience. A National Imperative. Summary*, Washington, D.C.: The National Academies Press 2012b.

The United Nations Office for Disaster Risk Reduction (UNISDR): *Partner Profile. French High Committee for Civil Defence (HCFDC)*, 2013. URL: http://www.unisdr.org/campaign/resilientcities/partners/view/11057 [Accessed: 29. 07. 2013].

The White House: *Presidential Policy Directive/PPD-21, Subject: Critical Infrastructure Security and Resilience*, 2013. URL: https://www.fas.org/irp/offdocs/ppd/ppd-21.pdf [Accessed: 31.07.2013].

The White House: *Presidential Policy Directive/PPD-8, Subject: National Preparedness*, 2011. URL: http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf [Accessed: 31.07.2013].

Tierney, K./Bruneau, M.: "Conceptualizing and Measuring Resilience. A Key to Disaster Loss Reduction". In: *TR News* 250: May – June 2007, pp. 14 – 17.

U.S. Securities and Exchange Commission (SEC), Division of Corporation Finance: *CF Disclosure Guidance: Topic No. 2*, 2011. URL: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [Accessed: 22.08.2013].

Ungericht, B./Wiesner, M.: „Resilienz. Zur Widerstandskraft von Individuen und Organisationen". In: *Zeitschrift Führung und Organisation*, 3, 2011, pp. 188 – 194.

United Nations (UN): *Our Common Future, Chapter 2: Towards Sustainable Development*. In: A/42/427. Our Common Future: Report of the World Commission on Environment and Development, 1987. URL: http://www.un-documents.net/ocf-02.htm [Accessed: 02.08.2013].

United Nations (UN): *Resolution Adopted by the General Assembly. The Future We Want*. In: A/RES/66/288, 2012. URL: http://www.unece.org/fileadmin/DAM/env/documents/2012/A_RES_66_288_TheFutureWeWant_e.pdf [Accessed: 27.01.2014].

United Nations (UN): *What is Sustainability?*, 2013. URL: http://www.un.org/en/sustainablefuture/sustainability.shtml [Accessed: 02.08.2013].

United Nations Conference on Sustainable Development (UNCSD): *7 Critical Issues at Rio+20*, 2013. URL: http://www.uncsd2012.org/rio20/7issues.html [Accessed: 02.08.2013].

United Nations Secretary-General's High-level Panel on Global Sustainability: *Resilient People, Resilient Planet: A future worth choosing* (Report), New York 2012.

University of Leeds: *What Is Resilience?* 2013. URL: http://www.engineering.leeds.ac.uk/resilience/what-is-resilience.shtml [Accessed: 10.01.2013].

Viscusi, W./Aldy, J.: "The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World". In: *Journal of Risk and Uncertainty*, 27: 1, 2003, pp. 5 – 76.

Von Gleich, A./Gößling-Reisemann, S./Stührmann, S./Woizeschke, P./Lutz-Kunisch, B.: „Resilienz als Leitkonzept – Vulnerabilität als analytische Kategorie". In: Fichter, K./von Gleich, A./Pfriem, R./Siebenhüner, B. (Hrsg.): *Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien*, Bremen/Oldenburg: Projektkonsortium „nordwest2050" 2010, pp. 13 – 49.

Walker, J./Cooper, M.: "Genealogies of Resilience. From Systems Ecology to the Political Economy of Crisis Adaptation". In: *Security Dialogue*, 42: 2, 2011, pp. 143 – 160.

Westrum, R.: *All Coherence Gone: New Orleans as a Resilience Failure*, URL: http://www.resilience-engineering-association.org/download/resources/symposium/symposium-2006(2)/Westrum.pdf [Accessed: 12.03.2013].

Whitney, D.: *"Normal Accidents" by Charles Perrow – Reviewed by Daniel E. Whitney, Massachusetts Institute of Technology, Engineering Systems Division. Working Paper Series*, 2003. URL: http://esd.mit.edu/staging/wps/wplit-2003-01.pdf [Accessed: 27.01.2014].

Wildavsky, A.: „Die Suche nach einer fehlerlosen Risikominderungsstrategie". In: Krohn, W./Krücken, G. (Hrsg.): *Riskante Technologien. Reflexion und Regulation*, Frankfurt a. M.: Suhrkamp 1993, pp. 305 – 319.

Wildavsky, A.: *Searching for Safety* (Studies in Social Philosophy & Policy, Buch 10), Piscataway: Transaction Publishers 1988.

Woods, D.: *Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making. Testimony on The Future of NASA for Committee on Commerce Science and Transportation*, 2003. URL: http://history.nasa.gov/columbia/Troxell/Columbia%20Web%20Site/Documents/Congress/Senate/OCTOBE~1/Dr.%20Woods.pdf [Accessed: 27. 01. 2014].

Woods, D./Hollnagel, E.: "Prologue: Resilience Engineering Concepts". In: Hollnagel, E./Woods, D./Leveson N. (Hrsg.): *Resilience Engineering*. Hampshire: Ashgate Publishing Limited 2006, pp. 1 – 6.

Yergin, D.: *The Quest: Energy, Security, and the Remaking of the Modern World*, London: Allen Lane 2012.

Zolli, A.: *Learning to Bounce Back*, 2012. URL: http://www.nytimes.com/2012/11/03/opinion/forget-sustainability-its-about-resilience.html?pagewanted=all&_r=0 [Accessed: 06. 08. 2013].

ANNEX

LIST OF ILLUSTRATIONS

LIST OF TABLES

> PREVIOUSLY PUBLISHED TITLES IN THE acatech STUDY SERIES AND ITS PREDECESSOR ACATECH REPORTS AND RECOMMENDS:

Appelrath, H.-J./Kagermann, H./Krcmar, H. (Hrsg.): *Future Business Clouds. Ein Beitrag zum Zukunftsprojekt Internetbasierte Dienste für die Wirtschaft* (acatech STUDIE), München: Herbert Utz Verlag 2014.

Buchmann, J. (Hrsg.): *Internet Privacy. Options for adequate realisation* (acatech STUDY), Heidelberg u. a.: Springer Verlag 2013.

Albers, A./Denkena, B./Matthiesen, S. (Hrsg.): *Faszination Konstruktion. Berufsbild und Tätigkeitsfeld im Wandel* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

Buchmann, J. (Hrsg.): *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

Geisberger, E./Broy, M. (Hrsg.): *agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

Spath, D./Walter, A. (Hrsg.): *Mehr Innovationen für Deutschland. Wie Inkubatoren akademische Hightech-Ausgründungen besser fördern können* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

Hüttl, R. F./Bens, O. (Hrsg.): *Georessource Wasser – Herausforderung Globaler Wandel. Beiträge zu einer integrierten Wasserressourcenbewirtschaftung in Deutschland* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

Appelrath, H.-J./Kagermann, H./Mayer, C. (Hrsg.): *Future Energy Grid. Migrationspfade ins Internet der Energie* (acatech STUDIE), Heidelberg u. a.: Springer Verlag 2012.

acatech (Hrsg.): *Organische Elektronik in Deutschland.* (acatech BERICHTET UND EMPFIEHLT, Nr. 6), Heidelberg u. a.: Springer Verlag 2011.

acatech (Hrsg.): *Monitoring von Motivationskonzepten für den Techniknachwuchs* (acatech BERICHTET UND EMPFIEHLT, Nr. 5), Heidelberg u. a.: Springer Verlag 2011.

acatech (Hrsg.): *Wirtschaftliche Entwicklung von Ausgründungen aus außeruniversitären Forschungseinrichtungen* (acatech BERICHTET UND EMPFIEHLT, Nr. 4), Heidelberg u. a.: Springer Verlag 2010.

acatech (Hrsg.): *Empfehlungen zur Zukunft der Ingenieurpromotion. Wege zur weiteren Verbesserung und Stärkung der Promotion in den Ingenieurwissenschaften an Universitäten in Deutschland* (acatech BERICHTET UND EMPFIEHLT, Nr. 3), Stuttgart: Fraunhofer IRB Verlag 2008.

acatech (Hrsg.): *Bachelor- und Masterstudiengänge in den Ingenieurwissenschaften. Die neue Herausforderung für Technische Hochschulen und Universitäten* (acatech BERICHTET UND EMPFIEHLT, Nr. 2), Stuttgart: Fraunhofer IRB Verlag 2006.

acatech (Hrsg.): *Mobilität 2020. Perspektiven für den Verkehr von morgen* (acatech BERICHTET UND EMPFIEHLT, Nr. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

acatech represents Germany's technological sciences both at home and abroad. It is an autonomous, independent non-profit organisation. As a working academic institution, acatech provides advice to policymakers and the general public on strategic issues relating to the technological sciences and technology policy. Moreover, acatech resolves to facilitate knowledge transfer between science and industry and to encourage the next generation of engineers. The Academy counts a number of eminent scientists from universities, research institutes and business among its Members. acatech receives institutional funding from the national and state governments along with donations and third-party funding for specific projects. It organises symposiums, forums, panel discussions and workshops in order to foster discussion of technological advances in Germany and demonstrate the potential of innovative technologies for industry and society. acatech publishes studies, recommendations and statements aimed at the general public. The Academy is composed of three bodies: the Members, who make up the General Assembly, the Executive Board, which is appointed by the Academy's Members and Senate and which guides the Academy's work, and the Senate, which comprises well-known figures principally from the worlds of industry, science and politics who advise acatech on strategic issues and facilitate a dialogue with industry and other scientific organisations in Germany. acatech's head office is located in Munich and it has additional offices in the capital, Berlin, and in Brussels.

For more information, visit www.acatech.de