Building A RESILIENT SOCIETY

By Dr. KLAUS THOMA and BENJAMIN SCHARTE

Europe pursues a holistic and sustainable security approach

On July 22, 2011, a car bomb blasted Oslo's government quarter, killing eight people and injuring 10. Right-wing extremist Anders Behring Breivik's improvised explosive device filled the streets with glass and debris. The attack demonstrated that even in presumably secure countries, severely adverse events can happen. Thus, our societies need to ensure the security of their citizens. Civil security research is one way to do that.

Within the last few years a new term has gained prominence in security research: resilience. People, societies and infrastructure shall become resilient, rather than secure. But what does resilience mean? And is there a difference between security and resilience? This article makes a point that, yes, there are indeed differences.[1]

Mainly, resilience means systematically and holistically approaching security problems by linking necessary expertise from all fields of science and practice. The key word is holistic (Scharte et al. 2014b: 119). Conversely, security is often linked with robust and rather static solutions. Could this new approach be called "holistic security" and has much of this already been done? Of course, but the new term allows us to reset the political agenda and bring resilience, thus also security, into important discussions on topics like sustainability right from the start.

THIS ARTICLE ANSWERS FIVE QUESTIONS:

- Why do we need resilience?
- What is resilience?
- How is resilience implemented into civil security research programs?
- How can engineering science help make our societies more resilient?
- What challenges need to be addressed on the way toward more resilient societies?

WHY DO WE NEED RESILIENCE?

Terrorist attacks, natural disasters and accidents can cause serious and irreversible damage. Terrorist attacks can paralyze transport infrastructure, natural disasters can render living in whole regions impossible, and accidents in power plants can result in the collapse of our energy supply. This is why we need security. And the same holds true for resilience, because resilience is the wider picture when talking about security. Furthermore, owing to the increasing complexity of our modern world and never-ending change, adverse effects of hazards tend to multiply (Coaffee et al. 2009: 122-132). Our systems are extremely susceptible to cascading effects because they are closely linked and intertwined.

Norwegian soldiers provide first aid in the aftermath of a terrorist bombing that ripped through central Oslo in July 2011. The military has a role to play in building resilience in the face of such crises.

AFP/GETTY IMAGES

Growing complexity, dependency and interconnectedness are also the reasons why security alone is not sufficient anymore. Current risk analysis often concentrates on specific components of systems, as well as known and expected threats. Finding ways to safeguard these components against specific threats is normally understood as building security (cf. Linkov et al. 2014: 407). Resilience goes further, comprising the dynamism needed to adapt to changing conditions. In a world that is facing ever more potentially devastating threats, and at the same time growing intrinsically more vulnerable because of complexity and interconnectedness, security is no longer sufficient.

DEFINING RESILIENCE

In the past 60 years, the term and concept of resilience have been widely used in the sciences, including developmental psychology, ecology, social sciences and engineering (CSS Analysen 2009: 1, Flynn 2011: i, Kaufmann & Blum 2012: 237ff, Plodinec 2009: 1).

As a scientific concept, resilience was first used in developmental psychology. Its breakthrough came in the 1970s with the seminal work of Emmy Werner. In her famous longitudinal study, *The Children of Kauai,* she found that children who grow up in difficult conditions can develop positively (Luthar et al. 2000: 544, Ungericht/Wiesner 2011: 188f). Resilience in terms of developmental psychology refers to the ability of individuals to cope with adverse events.

The work of Canadian ecologist Crawford S. Holling marked a quantum leap in resilience research. His 1973 article, "Resilience and Stability of Ecological Systems," broadened the field of application to ecology and led to a paradigm shift. For the first time, resilience did not refer solely to individuals, but to entire ecosystems. This idea was crucial for the further development of the concept. According to Holling, the foremost threat to an ecosystem's ability to survive comes from abrupt, radical and irreversible changes triggered by unusual and unanticipated events (Holling 1973: 1f, 14ff, Walker/Cooper 2011: 145ff). In nonresilient systems conceived only with stability, the deterministic features that previously enabled an equilibrium to be maintained prevent the system from responding flexibly, causing it to collapse (Holling 1973: 18ff, Kaufmann/Blum 2012: 239).

In the 1980s, resilience was finally used in connection to disasters, especially by engineers referring to technical infrastructure. Resilience encompasses the ability to deal with disasters, preventing them from turning into uncontrollable catastrophes (Plodinec 2009: 1). At the same time, American political scientist Aaron Wildavsky "translated" resilience into the social sciences. He defined resilience as "the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back" (Wildavsky 1988: 77). Since then, a central aspect of his rationale on resilience has evolved. He understood anticipation and resilience to be opposites. Modern concepts define resilience as a comprehensive, holistic approach to problem solving, the aim of which is to increase the overall resistance and regenerative capacity of technical and social systems. This implies anticipation and prevention, as well as response and adaptation (CSS Analysen 2009: 1).

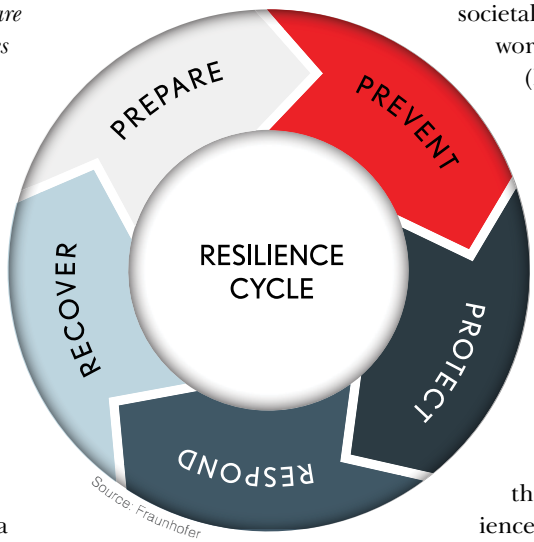
A recent definition emerged from the U.S. National Academies: "Resilience is the ability to prepare and plan for, absorb, recover from or more successfully adapt to actual or potential adverse events" (The National Academies 2012b: 2). Adverse events can be caused by nature or humans, by chance or with purpose. This understanding is called "all hazards approach" (The National Academies 2012: 14). To better understand the wide-ranging concept, Charlie Edwards' 2009 publication *Resilient Nation* borrows extensively from classical disaster management cycles (Edwards 2009: 20). Similarly, *Resilien-Tech* drew on both Edwards and disaster management cycles to develop a resilience cycle that provides an easily understood visual depiction of this complex concept.

The cycle is composed of five resilience phases: prepare, prevent, protect, respond and recover. The first phase, prepare, involves making thorough preparations for disasters, especially early warning systems. By reducing underlying risk factors, it is possible to prevent some adverse events from occurring, hence prevent. When an adverse event does occur, the next stage is to ensure that physical and virtual protection systems operate flawlessly to minimize the negative impacts — protect. It is necessary to provide rapid, well-organized and effective disaster relief. This requires the system to maintain its functionality as far as possible — respond. Once the adverse event is over,

it is important that the system recuperate and learn relevant lessons from what has happened to be better prepared for future hazards — recover.

Based on the resilience cycle, and drawing heavily on the work of the National Academies, here is a definition:

"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" (Scharte et al. 2014: 17).



Building resilience can be successful only if technological and societal approaches are linked and combined (Bara/Brönnimann 2011: 33, CSS Analysen 2009: 1). In this sense, resilience is a holistic way of thinking about security. Regardless of how this objective is achieved, resilient societies are characterized by the fact that the human, economic and environmental damages of adverse events are minimized. Resilient societies are distinguished by their ability to respond dynamically to constant changes in their environment and adapt to unforeseen events. Rather than a static condition, resilience is a property of dynamic, adaptable systems that are able to learn from past events.

RESILIENCE IN CIVIL SECURITY RESEARCH PROGRAMS

If we are talking about research funding, we cannot make a selective, clear-cut distinction between resilience and security. At the same time, societies would not have opportunities to become resilient if it were not for security research.[2] The development of sophisticated technologies, methods and tools for addressing imminent and specific security problems is a precondition for resilience.

Civil security research programs were established in Europe about eight years ago. The Seventh Framework Programme for Research and Technological Development (FP7) started in 2007 and for the first time, security became an independent research topic. In unison, the first German civil security research program was launched by the German Federal Ministry of Education and Research (BMBF) (Thoma et al. 2012: 322, 328). Both of these programs did not initially deal with resilience specifically but security. The European Commission implemented "Secure Societies" as one of seven societal challenges into the framework program Horizon 2020 (H2020), which started in 2014. The BMBF launched its second civil security research program in 2012. Besides classical security research, these programs specifically addressed resilience.

The European Commission tries to pursue several objectives with its societal challenge, Secure Societies. Two of these directly relate to resilience. Those are "Protecting and improving the resilience of critical infrastructures, supply chains and transport modes" and "Increasing Europe's resilience to crises and disasters" (2013/743/EU: 1029). Two more indirectly relate to resilience. When it comes to resilience in "Fighting crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs," thoughts need to be directed to new technologies and capabilities to "avoid an incident and to mitigate its potential consequences" (2013/743/EU: 1029). The European Commission also fosters "Enhancing standardization and interoperability of systems, including for emergency purposes." This objective contains the "integration and interoperability of systems and services, including aspects such as communication, distributed architectures and human factors," clear aspects of resilience (2013/743/EU: 1030).

In the Horizon 2020 Work Programme 2014-2015, a part titled "Secure societies – Protecting freedom and security of Europe and its citizens" has four primary goals. The first is enhancing the resilience of the society against human-induced as well as natural threats (European Commission 2014: 7ff). This specific call is divided into five

parts. Taken together, they represent a holistic understanding of resilience. All phases of the resilience cycle are addressed, including prevention and preparedness. Protection, response activities and recovering, including adaptation to changing environments, are indirectly mentioned in parts two, three and four (European Commission 2014: 9). Two examples very clearly demonstrate that the European Commission uses the concept of resilience supported in this article. Within the crisis management topic seven called "Crises and disaster resilience – operationalizing resilience concepts," resilience concepts shall be developed "for critical infrastructures … but also for the wider public to integrate and address human and social dynamics in crises and disaster situations" (European Commission 2014: 18). And the topic "Critical Infrastructure resilience indicator – analysis and development of methods for assessing resilience" states that proposals "shall demonstrate that a set of common and thoroughly validated indicators, including economic indicators, could be applied to critical infrastructures in order to assess its level of 'resilience' " (European Commission 2014: 29).

Within the BMBF's second civil security research program, resilience is defined as "a system's tolerance or capacity for resistance with respect to disruptive external influences" (BMBF 2012: 50). In principle, this definition could comprise all relevant aspects of resilience. Looking more closely, the BMBF shares exactly the same understanding of resilience as we do. The program focuses its "security research on the entire resilience cycle" (BMBF 2012: 7). Although resilience is no research topic on its own, it plays a vital role in societal aspects of security research, urban security, security of infrastructure and protection and rescue of people (BMBF 2012: 11, 14, 17).

In July 2014, the BMBF published a call on the topic of increasing resilience in crises and disasters ("Erhöhung der Resilienz im Krisen- und Katastrophenfall"). This call uses our definition of resilience, as well as the resilience cycle, and is aimed at funding research projects to improve society's capacity to prepare and prevent and/or respond and recover from adversities. Although it calls resilience a "key component of civil security" — which is not in line with a holistic understanding of resilience where security would rather be a key component of resilience — the call is about increasing resilience with the help of "holistic solutions." It strives to support projects by empowering people affected by a disaster. They are no longer just victims, but actors in preventing and responding to disasters. The focus of the call clearly lies on societal resilience and the resilience of rescue/disaster relief forces (BMBF 2014). In this regard it depicts just one very important part of the bigger resilience picture. In comparison to that, Horizon 2020 concentrates more on technologies for improving resilience. European and German civil security research programs show that resilience has found its way into security research. The next step needs to establish a new way of engineering thinking — resilience engineering.

THE NEED FOR RESILIENCE ENGINEERING

How can engineering science help us make societies more resilient? Engineers develop solutions: They observe problems and identify their causes. Then they create mechanisms either to eliminate the problems or counterbalance their negative effects with positive ones. The greater the task at hand, the more a society depends on the scientific expertise and the creative ingenuity of engineers. Thus, a resilient society requires a kind of resilience engineering.

Resilience engineering consequently provides ways to deal with the ever-growing complexity of modern systems, specifically with regard to many different types of hazards (Woods/Hollnagel 2006:6):

Resilience engineering means technological and interdisciplinary research and development on customized approaches and methods for improving functionality, resistance, adaptability and educability of systems with high societal value.

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 to the overall system level. Its goal is to maintain the critical subfunctions of systems in a controlled manner, even when severe damage forces them to operate outside normal parameters, thus allowing catastrophic total system failure to be averted. It requires customized technology 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 optimized, and they should be complemented by smart solutions from other fields such as economics, ecology and the social sciences.

An engineering approach to measure, evaluate and improve the resilience of cities is being

developed at Fraunhofer EMI. This approach uses resilience as a holistic concept. Additionally, it relies heavily on the results of the FP7 project, "Vulnerability Identification Tools for Resilience Enhancements of Urban Environments." Primarily, the approach tries to identify suitable technological indicators for measuring urban resilience with a special emphasis on the resilience cycle. These indicators are then formalized by a newly developed algorithm based on the overall concept of resilience. The objective is to use the indicators as well as the algorithm for the creation of a comprehensive software tool. This software shall be made available to urban planners, enabling them to implement resilience into their planning processes from the beginning. Since resilience cannot be understood purely technologically, the approach will include open interfaces that allow for the long-run implementation of findings from the social sciences.

A first step toward this more sophisticated resilience management tool is an already existing approach for the assessment of susceptibilities, vulnerabilities and averaged risk. The following example is applied to the scene of the Oslo bombings. First, averaged statistical-historical terror event data frequencies are interpreted as susceptibilities. Then, cumulated consequences attributed to a combination of sets of hazard loadings and affected objects are interpreted as averaged vulnerabilities (cf. Siebold et al. 2009, Fischer et al. 2014, Vogelbacher et al. 2014). The sums of the products of these averaged susceptibilities and vulnerabilities then determine the averaged risks. This allows urban planners to assess threat scenarios in detail using validated engineering-simulative methods (cf. Fischer/Häring 2009, Riedel et al. 2010). They then can select the most efficient countermeasures to mitigate the risks. This is of particular interest for increasing the resilience of urban areas.

This newly developed tool for risk assessment was applied in a kind of *à posteriori* investigation in Oslo. The buildings toward the middle of the government quarter were tremendously susceptible to terrorist threats and were the ones most severely damaged by the car bomb. An *à priori* risk analysis of this quarter would have uncovered that fact and probably helped save lives. This dramatically shows the importance of implementing security and resilience thinking into urban and other planning from the very beginning. Resilience engineering is a key component to the holistic concept of resilience.

MORE RESEARCH IS NEEDED

One very important challenge is to make sure that there is a persistent and well-supported effort to investigate technologies, methods and tools for resilience engineering. As shown, the European and German security research programs already take resilience into consideration. They have funded, and are currently funding, a wide array of projects which in some way or another focus on solutions for making our societies more resilient. Nevertheless, this is a huge technological, economical and societal task.

Research must continue. First, we need advanced methods for modeling and simulating complex socio-technical systems that are critical to society. This is a crucial part of what was defined above as resilience engineering. Such modeling and simulation tools will allow infrastructure operators, as well as urban and other planners, to identify weaknesses, plan countermeasures, correct faults and do everything in their power to prepare the system as fully as possible for adverse events. A wide variety of modeling techniques already exists today (cf. e.g. Renn 2008 and 2008b). However, as systems become increasingly more complex, the interdependencies among previously discrete subsystems multiply, and even more comprehensive, ultra-advanced methods are required to reliably model how systems will behave when unforeseen events occur (Al-Khudhairy et al. 2012: 574ff, Linkov et al. 2014). The aim is to produce multimodal simulations that use an integrated approach to model technological and social systems and the complex interactions among them.

Second, resilience has to pay off. Today, increasing security of relevant systems is often costly and to some, a dispensable add-on to their normal functioning. Thus, a case should be made for the long-term value that resilience can bring to society. We need to adopt a wider perspective, abandoning short-term and short-sighted cost/benefit optimization in favor of strategic, long-term thinking. Future research should therefore incorporate economics from the outset. In view of the greater challenges confronting us, systems that collapse at the first sign of trouble because they were designed according to radical cost-cutting principles hardly constitute a sustainable model. In a sustainability-based approach, the extra initial outlay required to create resilience soon pays for itself, not only in terms of reduced human suffering, but financially as well (The National Academies 2012: 13).

Third, 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 jeopardizing future generations' abilities to meet their own needs (A/42/427). The United Nations has identified seven key components of sustainable development. These are decent jobs, a sustainable energy supply, food security and sustainable agriculture, sustainable urban development, access to clean drinking water, sustainable use of oceans, and resilient societies (Un.org 2014,

Uncsd.org 2014). In this context, resilience involves maintaining the ability to function, adapt, endure and learn in the face of change and major adverse events. This ability is critical to sustainability, i.e., human society's capacity to survive the future. In other words, resilience must form an integral part of any successful model of sustainability.

In conclusion, resilience is different than security. To call it a holistic and sustainable security approach captures the most important of these differences. If we look at our ever more complex and interconnected world and at grand challenges like climate change, it becomes perfectly clear how desperately we need resilience. The concept itself is defined as the ability to repel, prepare for, take into account, absorb, recover from and adapt ever more successfully to actual or potential adverse events. Current civil security research includes many aspects of resilience research already. To address the manifold challenges we face today, we need the scientific expertise and creative ingenuity of engineers. Thus, we need to establish resilience engineering within civil security research. Resilience engineering means technological and interdisciplinary research and development on customized approaches and methods for improving functionality, resistance, adaptability and educability of systems with high societal value. Besides resilience engineering, security research must investigate the most advanced tools for modelling and simulation of complex systems, make a business case out of resilience and ensure that resilience is used as a key component of sustainable development. If we succeed in these tasks, our societies will be well prepared for tragedies like the Oslo bombings and look forward to a resilient and sustainable future. □

1. It is mainly based on the results of the project "Resilience by Design – a strategy for the technology issues of the future (Resilien-Tech)." The results of the project are published in Thoma 2014.
2. Thoma et al. 2014 gives a comprehensive overview about current security research.

Sources

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

Bara, C./Brönnimann, G. (2011): 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.

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

CSS-Analysen (2009): Resilienz: Konzept zur Krisen- und Katastrophenbewältigung. In: CSS Analysen zur Sicherheitspolitik, 60, Zürich: Center for Security Studies (CSS), ETH Zürich.

Edwards, C. (2009): Resilient Nation, London: Demos.

European Commission (2014): European Commission Decision C (2014)4995 of 22 July 2014: HORIZON 2020. WORK PROGRAMME 2014 – 2015. 14. Secure societies – Protecting freedom and security of Europe and its citizens. Revised.

European Council (2013): COUNCIL DECISION of 3 December 2013 establishing the specific programme implementing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC. Official Journal of the European Union, 2013/743/EU, cited as 2013/743/EU.

Federal Ministry of Education and Research (BMBF) (2012): Research for Civil Security 2012 - 2017. Framework programme of the Federal Government. Url: http://www.bmbf.de/pub/Rahmenprogramm_Sicherheitsforschung_2012_ENG.pdf [05.11.2014].

Federal Ministry of Education and Research (BMBF) (2014): Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien über die Förderung zum Themenfeld "Zivile Sicherheit – Erhöhung der Resilienz im Krisen- und Katastrophenfall" im Rahmen des Programms "Forschung für die zivile Sicherheit 2012 - 2017" der Bundesregierung. Url: http://www.bmbf.de/foerderungen/24109.php [05.11.2014].

Fischer, K./Häring, I. (2009): SDOF response model parameters from dynamic blast loading experiments. In: Engineering Structures, 31: 8, 1677-1686.

Fischer, K./Siebold, U./Vogelbacher, G. et al. (2014): Empirical analysis of security critical events in urban areas. In: Bautechnik 91:4, 262-273.

Flynn, S. (2011): A National Security Perpesctive on Resilience. In: Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, 2, i-ii.

Holling, C. (1973): Resilience and Stability of Ecological Systems. In: Annual Review of Ecology and Systematics, 4, 1-23.

Kaufmann, S./Blum, S. (2012): 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, Baden-Baden: Nomos, 235-257.

Linkov I./Kröger, W./Renn, O./Scharte, B et al. (2014): Risking Resilience: Changing the Resilience Paradigm, Commentary to Nature Climate Change, 4: 6, 407-409.

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

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

Renn, O. (2008): Concepts of Risk: An Interdisciplinary Review. Part 1: Disciplinary Risk Concepts. In: GAiA, 17:1, 50-66.

Renn, O. (2008b): Concepts of Risk: An Interdisciplinary Review. Part 2: Integrative Approaches. In: GAiA, 17:2, 196-204.

Riedel, W./Mayrhofer, C./Thoma, K./Stolz, A. (2010): Engineering and Numerical Tools for Explosion Protection of Reinforced Concrete. In; International Journal of Protective Structures, 1: 1, 85-101.

Scharte, B./Hiller, D./Leismann, T./Thoma, K. (2014): Einleitung. In: Thoma, K. (Hrsg.): Resilien Tech. Resilience by Design: Strategie für die technologischen Zukunftsthemen (acatech STUDIE). München: Herbert Utz Verlag, 9-18.

Scharte, B./Hiller, D./Leismann, T./Thoma, K. (2014): Fazit. In: Thoma, K. (Hrsg.): Resilien Tech. Resilience by Design: Strategie für die technologischen Zukunftsthemen (acatech STUDIE). München: Herbert Utz Verlag, 121-130.

Siebold, U./Ziehm, J./Häring, I. (2009): Terror Event Database and Analysis Software. In: Future Security, 4th Security Research Conference, Karlsruhe.

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

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

Thoma, K. (2014) (Hrsg.): Resilien Tech. Resilience by Design: Strategie für die technologischen Zukunftsthemen (acatech STUDIE). München: Herbert Utz Verlag.

Thoma, K./Leismann, T./Häring, I. (Hrsg.) (2014): 9th Future Security. Security Research Conference. Proceedings, Stuttgart: Fraunhofer Verlag.

Thoma, K./Drees B./Leismann, T. (2012): The Concept of Resilience in the Context of Technical Sciences. In: Gander, H.-H. Gander/Perron, W./Poscher, R./Riescher, G./Würtenberger, T. (Hrsg.): Resilienz in der offenen Gesellschaft. Symposium des Centre for Security and Society, Baden-Baden: Nomos, 321-340.

Ungericht, B./Wiesner, M. (2011): Resilienz: Zur Widerstandskraft von Individuen und Organisationen. In: Zeitschrift Führung und Organisation, 03, 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 [05.11. 2014], cited as A/42/427.

United Nations (UN): What is Sustainability?, 2013. URL: http://www.un.org/en/sustainablefuture/sustainability.shtml [Stand: 05.11.2014], cited as Un.org 2014.

United Nations Conference on Sustainable Development (UNCSD): 7 Critical Issues at Rio+20, 2013. URL: http://www.uncsd2012.org/7issues.html [05.11.2014], cited as Uncsd.org 2014.

Vogelbacher, G./Fischer, K./Häring, I./Riedel, W. (2014): Empirical susceptibility, vulnerability and risk analysis of urban areas to enhance security. In: Journal of Risk Analysis, submitted.

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

Wildavsky, A. (1988): Searching for Safety (Studies in social philosophy & policy, no. 10), Piscataway: Transaction Publishers 1988.

Woods, D./Hollnagel, E. (2006): Prologue: Resilience Engineering Concepts. In: Hollnagel, E./Woods, D./Leveson N. (Hrsg.): Resilience Engineering. Hampshire: Ashgate Publishing Limited, 1-6.