Working Paper

93 / March 2017

Österreichisches Institut
für Internationale Politik
Austrian Institute for
International Affairs

# The Difference Resilience Makes

# U.S. National Preparedness – From Civil Defence to Resilience

**Barbara Gruber**

**Working Paper 93 / March 2017**

This work was supported by ÖSTERREICHISCHE NATIONALBANK (OeNB Jubiläumsfond) Grant No. 16601 and is carried out in cooperation with the Donau University Krems

Keywords: Resilience, USA, civil defence, homeland security, difference

**Mag. Barbara Gruber** is researcher at the Austrian Institute for International Affairs (oiip) in Vienna. She is part of 'the governance of resilience' project, funded by the Anniversary Fund of the Austrian National Bank. Besides security and resilience, Barbara's research focus includes peace and conflict studies. She can look back to field research in Colombia and Sweden. Her main publications are 'Resilience and the Transformation of Sovereign Security' (Resilience, 2016) and 'Ser Eleno – Insurgent Identity Construction' (Small Wars & Insurgencies, 2015).

*Impressum:*

*Österreichisches Institut für Internationale Politik – oiip,*
*1090 Wien, Berggasse 7, www.oiip.ac.at, info@oiip.ac.at*

*Copyright © 2017*

## Executive Summary

Resilience is a new component of the security empire. But its conceptual relations to security and defence are still unclear. This paper argues that resilience is the replacement of former civil defence measures in the US. Hence, it traces the origins of resilience during the past 60 years of US policy history. National preparedness thereby serves as the key issue along which the conceptual changes are traced. The paper is guided by the research question *what is the difference resilience makes* and, therefore, establishes changes and continuities along the way.

In the first part, the reasons for the introduction of civil, or passive, defence as complementary to active defence are given. During this period, approximately 1950-1980, civil defence was based on retaliation and deterrence logics. During the 1970s, a major change took place when emergency management became part of security considerations and mitigation was introduced. Emergency management was nevertheless subsumed under a civil defence agenda. It was subsumed due to a 'dual-use' logic, stating that emergency preparation is fundamentally a local issue and independent of its source. Two characteristics of today's resilience policies are found in this regard: first, the 'dual-use' approach as precedent for todays' 'all-hazard' policies and second the perception that all emergencies are local phenomena.

The end of the Cold War led to a decisive change in the concept of security itself and rendered former civil defence conceptions obsolete. Thus, emergency management became independent, while civil defence considerations were poured into a new conception of 'homeland defence' directed at the new emerging threat of terrorism. After 9/11, homeland defence became 'Homeland Security', and incorporated the emergency management sector. The Department of Homeland Security was modelled after the Department of Defence and acted under the tight security conceptions 'prevent, protect, and respond'. These conceptions proved too tight for an agency responsible for 'all-hazards' as shown by Hurricane Katrina. After Hurricane Katrina, a new disaster circle was inaugurated which brought mitigation back and moreover introduced resilience as guiding organisational principle.

## Zusammenfassung

Resilienz ist mittlerweile eine etablierte Komponente der Sicherheitsarchitektur. Allerdings ist das konzeptionelle Verhältnis von Resilienz zu Verteidigung und Sicherheit immer noch unklar. In diesem Arbeitspapier wird diese Problemstellung aufgegriffen und argumentiert, dass Resilienz die Ablöse von früheren zivilen Verteidigungskonzepten ist. Aus diesem Grund stellt es an Hand eines historischen Abrisses die Ursprünge von Resilienz dar und verfolgt Veränderungen und Kontinuitäten. Der Fokus liegt dabei auf der Gestaltung von *National Preparedness* (Nationale Einsatzbereitschaft) in den USA. Die These ist geleitet von der Forschungsfrage was ist der Unterschied den Resilienz macht? Im ersten Teil werden die Gründe für die Entstehung von zivilen bzw. passiven Verteidigungskonzepten gegeben. Passive Verteidigung ist in den Jahren 1950 bis ca. 1980 als komplementär zur aktiven Verteidigung konzipiert. Während den 1970er Jahren findet eine massive Veränderung statt, da Katastrophenschutz nunmehr als Sicherheitsaufgabe des Staates wahrgenommen und in die Agenda der zivilen Verteidigung eingespeist wurde. Die Zusammengehörigkeit dieser Sektoren wurde damit argumentiert, dass jede Krise ein lokales Phänomen sei und beides Vorbereitung (dual-use approach) benötige. Diese Argumentation wurde im Zuge der Einführung von Resilienz-Politiken wieder aufgegriffen.

Das Ende des Kalten Krieges hat zu einer fundamentalen konzeptionellen Veränderung von Sicherheit geführt und hat zivile Verteidigung obsolet gemacht. Katastrophenschutz wurde unabhängig, während frühere zivile Verteidigungsaufgaben im neuen Konzept der ‚Homeland Security' eingefasst werden sollten. Dieses wurde benötigt, da Terrorismus als immer größere Bedrohung wahrgenommen wurde. Nach 9/11 wurde aus der Heimat Verteidigung das Ministerium für Heimatschutz, welches dem Verteidigungsministerium nachempfunden war und insofern mehr auf Sicherheitsaufgaben denn auf Katastrophenschutz konzentriert war. Das Scheitern dieses Ansatzes wurde durch den durchgängig fehlerhaften Umgang mit dem Orkan Katrina deutlich. Aus diesem Grund wurden alte Elemente des Katastrophenschutzes – Risikominderung (risk mitigation) und Resilienz – eingeführt.

# Table of Content

Introduction ..... 6
History of Civil Defence ..... 7
The Introduction of Disaster Management to the Concept of Civil Defence ..... 9
Precursors to all-hazards preparedness ..... 10
Homeland Defence ..... 12
Homeland Security ..... 15
A Culture of Resilience ..... 18
Preparedness as Engaging with Communities ..... 20
Preparedness as Critical Infrastructure Protection ..... 21
Conclusion ..... 25
Bibliography ..... 27

## Introduction

By now the concept of resilience is established as integral part of the security empire. In areas as diverse as climate security (Boas/Rothe 2016), peace- and statebuilding (OECD DAC, 2011) and National Security Strategies (WH 2010; 2015), resilience features prominently. In the US, no administration preceding Obama has used resilience so often in security strategies and policies alike (Selchow 2016). One question raised by scholars about this remarkable rise of resilience concerns the conceptual relation of resilience and security. Some authors argue that resilience is displacing security (Evans, Reid 2015), while others consider resilience not to be the replacement of security but rather of defence (Corry 2014). This paper follows up on the latter strand and claims that resilience is the replacement of a specific kind of defence, namely past conceptions of civil defence.

Civil defence was established as an answer to the Cold War threat perception. Hence it dealt with how to prepare the population of a country physically and mentally for a nuclear attack. In the US, the establishment of a 'permanent state of preparedness' can be traced through its policy history until its most recent incarnation – the 'National Preparedness Goals' of today. Although 'preparedness' as goal stayed the same during these times, different threat and risk perceptions required different approaches to preparedness. The most recent approach to national preparedness was the introduction of resilience. Hence this paper engages in the following questions: what triggered resilience-based approaches? What is the difference resilience makes?

I argue that resilience is the replacement of the 'low-risk – high-preparedness' approach introduced by the Bush administration after 9/11. The attacks on the World Trade Centre lead to the inauguration of Homeland Security, which serves as concept as well as institution. The Department of Homeland Security subsequently established the National Preparedness Goals as common vision for the security sector. But 'low-risk – high preparedness', based on a notion of overall protection, turned out to be neither possible nor feasible, as shown by the missing mitigation efforts before and during hurricane Katrina in 2005. The introduction of resilience as organisational principle subsequently displaced protection as the guiding principle. Resilience works differently as it re-introduces risk mitigation, manages to prioritise and focus, and establishes an integration among different sectors and stakeholders.

This paper starts with tracing the development of civil defence conceptions in the 1950s, when National Security was split into (active) defence and civil (passive) defence. During the 1970s, a crucial

shift becomes visible as emergency management became a security concern and was established as a yet another task of civil defence. Both parts will be guided by the research question 'what is the difference resilience makes'. In discussing this question, the paper compares those initial framings to today's concept of resilience. During the 1990s, the overall concept of 'National Security' changed. One consequence was the conceptual shift from civil defence to homeland defence. In the main part, this development and the change from homeland defence to homeland security as well as the reasons for the introduction of resilience will be elaborated. Finally the difference is illustrated through the topics of 'Critical Infrastructure Protection' and 'Engaging Communities'.

## History of Civil Defence

Collier and Lakoff (2008, p. 11) trace the origins of US civil defence back to the World War II conception of a total war. The introduction of total war led for example to strategic bombings, which did not target military sides, but aimed to destroy the civilian capacities. Civilian capacities were basically industries, which could prolong the war on all fronts (civil as well as military). Deriving from these changes in warfare 'National Security' emerged as an overall concept integrating military and non-military government agencies. The first institution concerned exclusively with civil defence was the Federal Civil Defence Administration inaugurated in 1950 (-1972), which was tasked to: "'strengthen our capacity to substantially withstand attack, our national resiliency, by insuring the continuity of civil government and the protection of civilian life' (Collier/Lakoff 2015, p. 29). The importance of civil defence, which is essentially a domestic security issue, was subsequently fuelled further by the emerging Cold War.

Two main debates arose concerning preparedness measures of civil defence, which are still prevalent today. The first dispute dealt with the question whether the Civil Defense Administration was tasked to invest in expensive stockings (food, medical supplies, engineering equipment) or if its main tasks consisted in providing for training, planning and guidance (Wayne 1986, p. 3). The second debate refers to the question if civil defence measures are the responsibility of the citizen, the local community and the State or if it's a federal responsibility (ibid., p. 4). A major undisputed task of civil defence at the federal level was how to deal with the public's reaction when faced by a nuclear attack. Therefore, Oakes (1994, p. 8) argues that civil defence was also a psychological strategy employed by the government towards the public to 'install popular tolerance' for the deterrence strategy: 'The cynical interpretation held that although the state could not protect the American people in a nucle-

ar attack and they could not be expected to protect themselves, they could at least be persuaded to believe that self-protection was possible'. A nuclear attack was presented like a 'manageable disaster' similar to a flood or a hurricane and was called back then 'civic preparedness' which was framed as 'civic virtue' of all Americans and necessary for maintaining American leadership (Oakes 1994, p. 8).

Major natural disasters at the end of the 1960s were a driver for a policy transformation. During the Nixon area (1969-1974), in 1971, it was argued that civil defence could be employed for peacetime (mostly natural) disaster preparedness. The argumentation back then resembles today's all-hazard argumentation: 'the development of local capabilities for effective action in emergencies is essential to civil preparedness, both in peacetime or in the event of attack' (Wayne 1986, p. 16). It was subsequently called 'dual-use local preparedness' and became part of the Defense Civil Preparedness Agency. The implementation of the strategy led to a disaster relief which was subsequently handled by more than 100 federal agencies, which rendered the enforcement completely ineffective (DHS 2006a, p. 14-16). During the mid-1970s, two strategical changes in the Cold War spurred changes in civil defence. One was the revelation that the Soviet Union had itself a strong civil defence system in place, and second that a 'limited nuclear war' could turn into a feasible option (Wayne 1984, p. 19). Therefore, the precedent of 'critical infrastructure protection' became inaugurated, as it was argued that the enemy would attack strategic sides of the country, instead of retaliation against massive population centres. Subsequently, civil defence in the form of stockings (like food, medical care, electric power and others) also increased (ibid.).

Despite the refocusing of civil defence for 'wartime' efforts during the mid-1970s, civil defence was nevertheless increasingly employed for 'peacetime' emergencies. The development of all-hazards planning was already in place. The narrative was more about 'national emergencies' focusing on 'a more general theory of organization to meet a national crisis regardless of its particular cause' (McReynolds quoted after Collier/Lakoff 2015, p. 37). As a result of these conceptual changes, the Federal Emergency Management Agency (FEMA) was inaugurated in 1979. It was composed from five other emergency related agencies: the Federal Insurance Administration, the National Fire Prevention and Control Administration, the National Weather Service Community Preparedness Program, the Federal Preparedness Agency of the General Services Administration and the Federal Disaster Assistance Administration, as well as the Civil Defence Agency (DHS 2006a, p. 18). Samuel Huntington chaired the interagency group which led to the approach taken by FEMA stressing five points: 'enhance deterrence and stability; reduce the possibility of Soviet crisis coercion; enhance survivability of the American people and its leadership in the event of nuclear war; include planning for popu-

lation relocation during time of international crisis; and be adaptable to help deal with natural disasters and other peacetime emergencies' (Wayne 1984, p. 21). But even the official history of the DHS minimises the impact of the reorganisation for civil defence: 'Despite the reorganisation and move toward greater mission clarity, civil defense planning on the ground did not change dramatically' (DHS 2006a, p. 19).

From roughly 1950 to 1970, national security consisted of passive (civil) and active defence. Passive defence was never independent from active defence, but was shaped by its active counterpart. For example, during the Cold War first a retaliation logic was in place which led to civil defence preparations like fallout shelters, than a deterrence logic replaced retaliation and led to an increase of stockings. Concerning the comparison to today's resilience conceptualisations the debates surrounding the responsibility trading between the individual, local, state and federal level are remarkably similar. In this regard the debates if the civil defence agency's major task is the provision of information and trainings, or has more expensive provisional tasks were also part of the discussion surrounding the installation of Homeland Security. The most substantial independent development of civil defence concepts was the introduction of disaster management. Therefore, the next section deals with this development.

## The Introduction of Disaster Management to the Concept of Civil Defence

During the 1970s, a shift in governance took place, not just at the conceptual level ('dual-use' approach), or institutionally (inauguration of FEMA) but also in how knowledge about potential catastrophes was generated. In former decades, especially natural disasters were perceived as a 'random act of God', and thus as individual and isolated events (Roberts 2012, p. 45). While the state was responsible for civil defence, as part of a war effort and 'natural' task of the state, natural disasters were not yet seen as a security task (ibid.). In the 1970s, however, this perception changed fundamentally. Crisis and risk management techniques were developed. Routine procedures, precaution measures and forecasting tools were introduced (Stampnitzky 2013, p. 85). Natural disaster *mitigation* efforts, essentially risk management, became a central aspect of the state's security provision for its citizens. 'Managing' indicates that disasters were no longer perceived to be a 'random act of a higher force' but a (disruptive) incident which can be controlled. This new perception led to the so called 'Stafford Act' of 1974 'which clarified the types of assistance that the federal government could provide in a disaster (Falkenrath 2001, p. 157). Furthermore, the costs of keeping a certain

status quo were higher, as the interconnection of services and the dependence on infrastructure increased. As the 1984 report 'America's Hidden Vulnerabilities: Crisis management in a Society of networks' argues: 'the nation had become economically, technologically and psychologically dependent on a number of "highly complex service networks" for "our daily wellbeing"' (Collier/Lakoff 2008a, p. 26).

Collier and Lakoff (2015, p. 41) call the new governance of risk 'reflexive risk', which is a forerunner of today's policies. They reconstruct the introduction of databased and statistical measurements in the area of flooding called 'catastrophe modelling for flood insurance' (ibid.). They point out that policy makers in the 1970s discovered through the model of 'reflexive risk' that earlier interventions through the construction of dams and levees encouraged people to settle in risky areas. Furthermore, disaster relief funds further discouraged them to stay out of harm's way (ibid.). A 'federal catastrophe insurance program' was launched, discouraging people to live in the most risky areas, assessed (although with difficulty as no data was available yet) through risk modelling. Risk modelling was then taken up as a central task of FEMA, and spreading to the private insurance sector in the 1990s, to be employed for other areas such as climate change and terrorism in the 2000s (ibid.).
The development from civil defence to a more complex set of risk management will be explored in the following through the institutional development of FEMA. One of the main differences from earlier preparedness approaches was the attempt to integrate industries on a broad basis into the national preparedness effort. Although the business sector was reluctant to spend money on nuclear preparedness plans, they were easier to convince when it concerned natural disaster preparedness. Thus, preparedness was introduced for example in the petroleum industry as a general feature, serving the protection from natural disasters as well as from 'doings of mankind' as this industry provided 75% of the country's energy (Collier/Lakoff 2008a, p. 18). Another central theme of civil defence, namely who is responsible in a case of disaster – the citizens, the local level, the state or the federal government – was at least partially resolved through the institutionalization of FEMA. The institutionalisation spread the perception that it was a public task and anchored at the federal level.

- **Precursors to all-hazards preparedness**

> 'The creation of FEMA centralized previously scattered disaster agencies in a single organization devoted to the new principle of "emergency management" rather than the old approach of "civil defense," a change as significant as the more recent use of the term "homeland security"' (Roberts 2012, pp. 46-47).

While the idea of one agency responsible for all-hazards was appealing to politicians, the relationship between civil defence planners and emergency managers was traditionally uneasy (Roberts 2012, p. 46). While strategies considering the preparation for isolated incidents to a full-fledged war were prepared, the divisions within former distinct spheres of disaster management were difficult to overcome (ibid.). But the divide between the civil defence sector and emergency management staff was even bigger. The separation between disasters management and security officers led to different stages of security clearances and reinforced a 'silo-thinking' within an organisation tasked to overcome this way of thinking. For example, FEMA developed a 'cutting-edge information technology system' but its security division did not allow it to be used for natural disasters (ibid., p. 49). In sum, FEMA suffered from not having a clearly stated mission, but shouldered the blame for unpreparedness when a disaster hit (Roberts 2012, pp. 46-48; Sylves/Cumming 2004, p. 9). During some major disasters at the end of the 1980s and beginning of the 1990s, FEMA performed poorly. This in turn affected the popularity of the federal government. Therefore, not just the end of the Cold War, but also previous experiences of unpreparedness led to a restructuring of national preparedness efforts during the 1990s.

With James Lee Witt an actual disaster manager became leader of FEMA for the first time. He defined the mission of the agency along a focus on natural disasters. He disbanded the security part of FEMA, thus counter-terrorism went back to be mainly a law enforcement task, to be delivered by the FBI. In contrast to Witt, all FEMA directors before him had fought hard for the counter-terrorism mandate, as counter-terrorism made FEMA more of a security agency (Roberts 2012, pp. 50-52). Furthermore, Witt eliminated all the purely political posts in the agency and delivered more money to the local and state level (ibid., p. 51). He streamlined the natural disaster division along the concept of mitigation by arguing that mitigation would save money in the long-term. Therefore, Witt relied on financial incentives to prevent building in floodplains, or to strengthen structures in earthquake zones (ibid., p. 50). But federal prestige projects, serving pork barrel politics, such as flood-control works carried out by the U.S Army Corps of Engineers, undermined such efforts (Birkland 2012, p. 110). Witt introduced the concept of all-hazards in a mature version, compromising 'early warning, the coordination of response by multiple agencies, public communication to assuage panic, and the efficient implementation of recovery processes' (Collier/Lakoff 2009, p. 258) and all phases (mitigation, preparation, response and recovery). Thereby, he changed the federal disaster management landscape.

The incorporation of 'natural' disasters into the federal responsibility of civil defence planning was a decisive shift. As shown, emergency management even gained the upper hand in civil defence con-

siderations. Both sectors seemed to completely drift apart in the 1990s, despite the 'dual-use' and later on 'all-hazard' approach which was propagated. Nevertheless, the techniques of 'risk governance' expressed in modelling, statistical analytics and forecasting were used in the military as well as natural disaster management, and changed the conceptual basis of 'how and whom to prepare' significantly. Mitigation became a major focus. Furthermore, the need for an increased communication between different agencies, departments and sectors, especially the wider public and the private sector, became inevitable. Both developments will find its repercussions in resilience policies. Meanwhile, major developments took place in the security realm as well throughout the 1990s, which will be traced in the next section when preparedness enters yet another stage.

## Homeland Defence

The first official 'National Security Strategy' was issued in 1987. Remarkably, security at this point still consisted of defence. It rather dealt with foreign policy than domestic issues. Accordingly, it centred on the Soviet Union as the main antagonist. Nevertheless, the world was described as changing and becoming ever more complex (WH 1987, p. 21). These features are usually attributed to the advent of 'resilience' into the security realm (cf. Chandler 2014, p. 47). Institutionally, the National Security Strategy concerned the Department of Defence and the Department of State.

The end of the Cold War changed the perception and conception of security substantially. Huysmans (2014, p. 1) strikingly called this process 'security unbound'. Security was lifted out of the narrow realm of defence and was broadened, or unbound, to encompass areas as diverse as environment policies or financial markets regulations (ibid.). This 'unboundedness' of security can be traced in the Security Strategies of the US after the end of the Cold War. Suddenly, new topics such as peace operations, the environment, energy security, counterterrorism and combatting narcotics featured prominently next to the former usual security issues such as 'maintaining a strong defense capability' (WH 1994, p. i). This change from defence to security happened because of the following reasoning: 'the line between our domestic and foreign policies has increasingly disappeared' (WH 1994, p. i). But it was not until 1998, when the 'National Security Strategy For A New Century' was drawn, that this new thinking slowly showed policy and subsequent institutional repercussions.

As security, and all it contained, changed substantially, the mode of preparedness changed as well. Hitherto, the passive or civil defence part rested on an active counterpart; this active counterpart went missing after the Cold War. Therefore, this new mode of civil defence – homeland defence –

became more independent. Yet, it rested on new enemy perceptions. Although there was no longer a single enemy entity (as the Soviet Union), terrorism nevertheless featured prominently in the new security environment. Under the heading of 'Enhancing Security at Home and Abroad', terrorism became the most dangerous 'Emerging Threat at Home' (WH 1998, p. 18). As solution to this emerging threat 'Critical Infrastructure Protection' (also including the predecessor for Cyber Security) and 'Managing the Consequences of WMD Incidents' were introduced. Both sectors lead to a considerable involvement of different existing agencies (e.g. FBI, FEMA, Department of Energy, Environmental Protection Agency, DoD) (ibid.). Those new policies were termed 'homeland defence', but the two 'natural' institutions for the job, DoD and FEMA, were not enthusiastic about the prospects.

The DoD was 'neither interested in the White House's new wars (peacekeeping, terrorism, organized crime and the like) nor the Joint Staff's futuristic technological blueprint. The military really wants to fight wars that are like those of the past, only with upgraded equipment on all sides' (Crenshaw 2001, p. 333). When the programme to act on these new policies in the form of a 'domestic preparedness program' was discussed, the DoD thus argued to shift the whole programme to FEMA (ibid.). Furthermore, they saw 'homeland defence' more as a law enforcement issue rather than a military one (ibid.). FEMA on the other hand did not want to take on the responsibility, as they reasonably suspected that this new responsibility would not be accompanied by more budget (ibid.). Despite such restraints, the 'domestic preparedness program' entered the Security Strategy in the following fashion:

## National Security Emergency Preparedness

> We will do all we can to deter and prevent destructive and threatening forces such as terrorism, WMD use, disruption of our critical infrastructures, natural disasters and regional or state-centered threats from endangering our citizens. But if an emergency occurs, we must also be prepared to respond effectively at home and abroad to protect lives and property, mobilize the personnel, resources and capabilities necessary to effectively handle the emergency, and ensure the survival of our institutions and national infrastructures. National security emergency preparedness is imperative, and comprehensive, all-hazard emergency planning by Federal departments, agencies and the military continues to be a crucial national security requirement' (WH 1998, p. 26).

Under the heading of 'Preparing Now for an Uncertain Future', the first milestones for a major transformation were laid. This concerned not just the above mentioned 'domestic preparedness', but of security as a whole (WH 1998, p. 23). Whereas before, during civil defence times, it was discussed

which level should carry the main responsibility for preparedness, now a full integration is proposed. Such integration referred not only to government levels (Federal, state and local), but aimed at an involvement of the private sector partners to 'protect against and respond to transnational threats at home'. This resulted also in privatisations within the military component: 'To support this transformation of our military forces, we will work cooperatively with the Congress to enact legislation to implement the Defense Reform Initiative, which will free up resources through a Revolution in Business Affairs. This revolution includes privatization, acquisition reform and elimination of excess infrastructure through two additional base realignment and closure (BRAC) rounds in 2001 and 2005' (ibid. 23).

Against this background, the 'Domestic Preparedness Program' to implement those policies was installed. Probably one of the most challenging tasks was to overcome the 'maze of domestic agencies' and the complexity of the interaction of technical and institutional factors, since both the private sector and NGOs were included in the effort (Falkenrath 2001, p. 175):

> 'The U.S. domestic preparedness program seeks to go beyond improving the physical security of particularly vulnerable or high-value targets, which has always been a part of the traditional counterterrorism formula. Instead it aims to reduce the vulnerability of American society to large, destructive acts of terrorism by improving operational response capabilities across the country, at all levels of government. This effort bears a superficial resemblance to the U.S civil defense program of the 1950 and 1960s, but its scale and complexity are unmatched' (Falkenrath 2001, pp. 147-48).

As stressed above, the distinction of domestic and foreign affairs collapsed, which triggered policy reforms, since institutional distinctions were no longer feasible. This became a 'policy truth' in many areas; in particular, anti-terrorism policies blurred this distinction completely. Deutch, Kanter and Scowcroft (2000, pp. 165-271) show this by invoking the responsibility of the State Department for international terrorism, while the FBI as part of the Department of Justice becoming responsible for domestic terrorism. FEMA in turn dealt with the management of the consequences of terrorism. Thus, the reorganisation of 'homeland defence' issues fundamentally rests on the 'new terrorism' thesis. Falkenrath (2001, p. 153) stresses that the 'domestic preparedness program' is basically an 'outgrowth and subset of U.S. counterterrorism policy' which became at the end of the 1990s based on the 'new terrorism' or back then 'super-terrorism' presumptions.

Four components characterise 'new terrorism': (a) new terrorists are no longer hierarchically organised, but in networked and fluid forms (e.g. swarms, as 'cyber terrorism' was also an emerging threat). (b) 'New terrorists' operate transnational; (c) ideology is replaced by religion; and (d) they may use Weapons of Mass Destruction (as legacy from the Cold War) (cf. Lesser, Hoffmann, Arquilla,

Ronfeldt, Zanini 1999). The nerve gas attack in the Tokyo subway in 1995 seemed to confirm this thesis (Falkenrath 2001, p. 161). This new approach resulted in a different conception of security: 'In addition to a greater emphasis on "economic security, "environmental security," and other issues that were of distinctly secondary importance during the Cold War, security perceptions are now increasingly driven by concerns about personal security and what may be termed "security of identity". … In many places around the world – including the United States – debates about security are to a great degree about personal security rather than the security of the state' (Lesser 1999, p. 97).

The 9/11 attacks became the next decisive event to shape the subsequent re-conceptualisation of security. The groundwork for a major re-structuring of domestic and foreign security was laid. The predominance of a security lens over a defence lens enabled security to move on, from being a state issue, over being a societal issue to finally become a personal issue. Especially the emphasis on the societal and personal dimension are the foundation for the introduction of resilience-based policies. Considering the societal component, the aforementioned 'Revolution in Business Affairs' allowed for a greater involvement of the private sector through a neoliberal agenda.

## Homeland Security

> 'Today's terrorists can strike at any place, at any time, and with virtually any weapon. Securing the American homeland is a challenge of monumental scale and complexity. But the U.S. government has no more important mission' (WH 2002a, p. 1).

9/11 finally triggered the installation of 'Homeland Security' and brought the scattered efforts to achieve national (security) preparedness together through the installation of the Department of Homeland Security. This department was tasked to reintegrate emergency management (mainly in form of incorporating FEMA), and to integrate law enforcement, military and the public and private sector. Henceforth, National Security consisted of Defence and Homeland Security:

> 'While we recognize that our best defense is a good offense, we are also strengthening America's homeland security to protect against and deter attack. This Administration has proposed the largest government reorganization since the Truman Administration created the National Security Council and the Department of Defense. Centred on a new Department of Homeland Security and including a new unified military command and a fundamental reordering of the FBI, our comprehensive plan to secure the homeland encompasses every level of government and the cooperation of the public and the private sector.' (WH 2002, p. 6).

> 'Definition: Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur' (WH 2002a, p. 2)

The institutional response also concerned the Department of Defence, the Intelligence sector and the FBI, all of which continued to be restructured according to the Clinton strategies (WH 2002, p. 30). Until 2006, transformations took place that facilitated information sharing between those entities. This was formerly prohibited due to privacy concerns (Department of Justice 2001). The Department of Homeland Security was tasked with 'the protection of the territory, critical infrastructures, and citizens of the United States by Federal, State, and local government entities from the threat or use of chemical, biological, radiological, nuclear, cyber, or conventional weapons by military or other means' (DHS 2006, p. 24). The DHS was modelled after the National Security System founded in 1947 (WH 2006a, p. 67). Therefore, it was organised along the (military) fashion of the Department of Defence, which led to some difficulties in the integration of the broad range of departments and stakeholders. FEMA in turn lost influence, staffing, budget and its main task preparation. Terrorism became the new priority in national preparedness, and disaster management got neglected (Moynihan 2009, p. 7).

In the aftermath of 9/11, 'threat-based planning' was adopted by the DoD, whereas Homeland Security took a 'capabilities-based approach'. The latter, according to then Secretary of Defense Rumsfeld, 'would focus more on how the United States would defeat an adversary's broad array of capabilities instead of identifying who the adversaries were and where they might threaten joint forces or United States' interest' (Caudle 2005, p. 5). Caudle describes that in that context that 'cascading policy goals' led to difficulties in the construction of a unified body. As a consequence, 'a single-source policy document for homeland security and national preparedness' should be implemented (ibid., p. 6). Subsequently the National Preparedness Goals were drafted. The directive that introduced the 'National Preparedness Goals' equated the state of preparedness with an all-time readiness (HSPD 2003, p. 1746). Accordingly, the Federal, State, and local level are required to have plans, procedures, policies, training and equipment in place to 'prevent, respond to and recover from major events' (ibid.). Strikingly mitigation, formerly a major guiding concept of FEMA, is missing in this new directive.

When Hurricane Katrina hit New Orleans, Homeland Security and its conceptions were tested for the first time. They failed spectacularly. The consequences of Katrina were spectacular itself, as they demonstrated what was a 'complex crisis': 'Katrina caused persistent flooding, a series of industrial

disasters, critical evacuation challenges, widespread lethal pollution, the destruction of 90% of the essential utility networks (energy, communications, water etc.), unprecedented public safety concerns, concern over the possible loss of the port area (which is essential to the continent's economy), even uncertainty as to whether portions of the city could be saved' (Lagadec quoted after Mynihan 2009, p. 1). In its aftermath, one of the most dramatic assertion was that there might have been enough organisations to help, but their lack of coordination rendered the response ineffective, until the Department of Defence took the lead and brought the military in (Roberts 2010, pp. 102-103). Basically all levels responsible for Homeland Security and Emergency Management were understaffed and too much focused on terrorism (ibid., pp. 8-9).

The failed response to Hurricane Katrina became the wake-up call that changed disaster preparedness and organisation once again. It also re-shifted attention back to natural disasters and led to a two-fold increase of FEMA personnel (cf. Kaufman et al. 2015, p. 152). It also led to a considerable change conceptually as protection became replaced by resilience:

> 'Protection is a physical thing – Critical Infrastructure Protection is basically gates, guns, guards, gadgets and gismos, it is a physical thing, it is node centric. But how many nodes do you have in the end?'
> We have not got quite out of the protection mode yet. But we will get there. Twenty years ago we created critical infrastructure protection - and then somebody said, well how much protection is necessary? Nobody had an answer to this question. Thus, it was a hard sell to businesses and communities, to invest in infrastructure protection, because you cannot give them an idea of what to do exactly and how much is enough. For example, everybody puts a lock on the door because that is the right thing to do, but when you talk about millions of dollars perhaps on achieving protection but you can't tell them how much is necessary – this is a hard sell! Therefore, assurance was introduced but this was too hard. The next concept was reliability. Reliability was replaced because a tree fell in Ohio and knocked out one third of the power on the East Coast United States. Then there was Katrina. Katrina was what let to resilience. The protection thing was not working - so there was policy recommendation made in 2006 and in 2013 it managed to make it three blocks down in Pennsylvania Avenue and they actually did it - they introduced resilience to the policy. Now we are finding out how to make resilience work and at the moment we are studying it some more' (Interview Gaynor, 1st September 2016 #00:13:06-1#)

Homeland Security is different from Civil Defence, as civil defence preparations are based on war scenario concepts like deterrence and retaliation. Homeland Security on the other hand deals with terrorism and hence requests to deal with more uncertainty regarding the scope, aim and impact of a possible attack. Security in this sense was based on prevention and protection, rather than more typical emergency management concepts such as preparation and mitigation. Katrina demonstrated

that the focus of Homeland Security was too narrow and not flexible. Hence, it provided the entry point for resilience.

## A Culture of Resilience

The National Security Strategy of 2010 (WH 2010, p. 5) recognises the failure of homeland security and the hence necessary reintegration with the realm of national security: 'Our intelligence and homeland security efforts must be integrated with our national security policies'. While security still was about 'prevent, protect and respond', never before the terms 'resilience' and 'resiliency' have been used so extensively. Selchow (2016, p. 10) assesses that the strategy even established 'resilience, this abstract quality, as nothing less than a natural and foundational aspect of (the culture) the United States'. Never before it was so clearly recognised that the 'lives of our citizens—their safety and prosperity—are more bound than ever to events beyond our borders' (WH 2010, p. 7). Force (or military power) alone was no longer seen as the most important features to mould the 'World We Seek'. Rather, it is the ability to act in a resilient manner which makes the difference in this new perception of the world: 'In the past, the United States has thrived when both our nation and our national security policy have adapted to shape change instead of being shaped by it' (WH 2010, p. 8). The perception of security and how to provide for security 'adapts to change' in the following fashion:

> 'Our national security begins at home. What takes place within our borders has always been the source of our strength, and this is even truer in an age of interconnection'. 'We are now moving beyond traditional distinctions between homeland and national security. National security draws on the strength and resilience of our citizens, communities, and economy' (ibid., p. 9, 10).

The security empire consist now of (active) defence which is still conceptually based on deterrence and the defeat of the enemies. The next section, 'Strengthen security and resilience at home', introduces resilience, because of the impossibility to protect against every threat (terrorism, natural disasters, cyberattacks, or pandemics):

> 'As we do everything within our power to prevent these dangers, we also recognize that we will not be able to deter or prevent every single threat. That is why we must also enhance our resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption' (WH 2010, p. 18).

The inauguration of a revised preparedness approach complements security and resilience. The preparedness goals introduce a new disaster circle consisting of five areas of preparedness (instead of the former three: prevention, protection and response) prevent, protect, mitigate, respond and recover (each area was poured into a policy framework). The major change in this regard is the reintroduction of mitigation. Notably, mitigation was the concept with which resilience came along:

> '[The] National Mitigation Framework Identifies capabilities necessary to reduce loss of life and property by lessening the impact of disasters. These capabilities include, but not limited to, community-wide risk reduction projects; improving resilience of critical infrastructure and key resources; risk reduction for specific vulnerabilities from natural disasters and acts of terrorism; and initiatives to reduce future risks after a disaster' (Brown 2011, p. 8).

Resilience in the context of the NSS is not a replacement of security, but rather an improved version of what was left of the civil defence/emergency management mix. The prevention and protection frameworks are led by the Interagency Policy Committees consisting of the 'Counterterrorism Security Group' and the 'Transborder Security Group'. Mitigation, Response and Recovery on the other hand are all led by the Interagency Group called 'Domestic Resilience Group' (Brown 2011, p. 12). In the mitigation area, Community Resilience and Critical Infrastructures are core issues. An annual report on the implementation of the 'National Preparedness Goal' was introduced and carried out in consultation with governmental and non-governmental stakeholders to keep them updated. Especially (public) infrastructure is still mentioned as being in a poor state.

In 2015, the former 'whole of government' approach becomes transferred into a 'whole of community approach'. Resilience becomes even more focused, namely for what is most essential during a crisis:

> 'The essential services that underpin American society must remain secure and functioning in the face of diverse threats and hazards. Therefore, we take a Whole of Community approach, bringing together all elements of our society—individuals, local communities, the private and non-profit sectors, faith-based organizations, and all levels of government—to make sure America is resilient in the face of adversity' (WH 2015, p. 8).

In contrast to cost-intensive and unspecific protection, resilience concentrates on the most essential functions, it prioritises and structures. What a resilience approach in the areas of mitigation, response and recovery does is based on emerging notions of reflective governance, or 'adaptive systems' (Comfort, p. 34). Information sharing between different organisations, especially between sectors tasked with security issues, and information flows from the security sector to the civil government became a major issue. Analysing past failures and learning from them, as well as trainings be-

came crucial, to ensure that plans remained operational. The next section elaborates these differences.

- **Preparedness as Engaging with Communities**

One instrument to enable participation which was also introduced under the Bush administration was the 'National Incident Management System' (NIMS). NIMS establishes a flexible and standardised system for government agencies and different level of government, as well as the private sector, non-governmental organisations and individual citizens alike to be included in the 'cycle of preparedness' (DHS 2007, p. 3)'. It is flexible as it can be applied to all manners of potentially disruptive incidents, and standardised so that different organisations are able to work together.

'Resiliency Advisors', a private company, works in partnership with local governments and develops plans and trainings to teach the application and integration of NIMS when a disasters hits. Their aim is to empower local community groups and leaders to act proactively (Interview Orloff, 15.8.2016). Their main task is to check out the local expertise (e.g. there is a local church, the church has expertise in feeding and therefore can also provide for a kitchen and volunteers), and to work with the already existing knowledge and apply it to emergency management. Furthermore, they train already existing groups (communities) in applying the NIMS, so that when catastrophes or crises hit, government agencies, responders and communities speak the same language, respond in the same network and use the same methodology (Interview Orloff, 15.8.2016).

Orloff stresses in this regard that it is less the crises or catastrophes that changed. It was rather the multiple ways to respond and the increased availability of communication that made crises more complex. Additionally, she perceives that state institutions such as FEMA are reacting to an overall shift to the community level: 'we are seeing definitely a shift in FEMAs understanding of the importance of engaging and empowering the local community. So I think we are seeing definitely a positive, more inclusive shift' (Orloff Interview, 15.8.2016).

Orloff emphasises the psychological dimension of resilience. Resilience is used to pro-actively react to a traumatic event, be it a terrorist attack such as 9/11 (the reason she started to engage with resilience) or a major natural disaster. This is particularly relevant regarding the community aspect:

> 'Resilience is not just about one individual, it is about a community of support that you have around you. and when you look at someone who is resilient, you look at someone who not only has developed certain positive coping skills, but you also look at someone who has surrounded themselves with a support network, that they are able to access when they are less resilient themselves (Orloff Interview, 15.8.2016).

- **Preparedness as Critical Infrastructure Protection**

The first comprehensive Critical Infrastructure Protection (CIP) legislation was issued in 1996 in the Clinton era, because computer and telecommunication technology became vulnerable to information breaches. Right from the start, the private sector was included in those efforts. Nowadays, the private sector owns about 80 – 85 % of the CIP in the US, therefore cooperation agreements between the state and the private sector are imperative. 'New terrorism' plays an important role in CIP, since nuclear utilities, chemical facilities and transportation are rendered as potential targets. Further, so-called electricity 'blackout', or an attack on water supplies or commercial facilities would have possibly an even greater impact on today's societies than a war. Yet, the following definition of CIP assessed a protection-based approach as impossible:

> 'They learn from experience and modify their tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. As security increases around more predictable targets, they shift their focus to less protected assets. Enhancing counter measures for any one terrorist tactic or target, therefore, makes it more likely that terrorists will favor another' (WH 2003, p. viii)

> 'The New Front Lines: Our technologically sophisticated society and institutions present a wide array of potential targets for terrorist exploitation. Our critical infrastructure industries change rapidly to reflect the demands of the markets they serve. Much of the expertise required for planning and taking action to protect critical infrastructures and key assets lies outside the federal government, including precise knowledge of what needs to be protected. In effect, the front lines of defense in this new type of battle have moved into our communities and the individual institutions that make up our critical infrastructure sectors' (WH 2003, p. 8).

As a result of the overarching protection focus of the Bush administration, there were attempts to protect virtually everything, and an ever growing range of infrastructure and key resources were stamped as 'critical'. Furthermore, total protection was not just impossible (there are 68.000 water systems, 300.000 oil and gas production facilities, 4.000 off-shore platforms, 278.000 miles of natural gas pipelines, 361 seaports, 104 nuclear power plants, 80.000 dams etc.), but not affordable (DHS 2005, p. 46).

As the first multi-sector CIKR policy points out, Homeland Security is different from National Security, as the government cannot be sole responsible anymore:

> 'Homeland security, particularly in the context of critical infrastructure and key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of federal, state, and local governments; the private sector; and concerned citizens across the country' (WH 2003, p. vii).

Therefore, the government established its role as the coordinator between different government agencies and the private sector, and it aimed at legislating coherent policies. The DHS was put in a dual role. For one, it was structured as security agency and characterised by inflexible internal structures, tasked to protect the homeland from terrorism. On the other hand, it should fulfil the function of a civil contingencies agency, which is a civil government agency tasked with cross-sector coordination 'serving as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector' (WH 2003, p. ix). From the outset, such a dual role carries an inherent contradiction. By incorporating other agencies like FEMA, which developed into a civil agency of professional emergency managers during the 1990s, the contradiction between security issues and emergency management became tenser.

Since the Obama administration, resilience got a boost. However, resilience can be traced back to the introduction of the new CIP legislation in 2003. There is a clear connection between the new era of preparedness and the 'security coming home' approach enacted after 9/11.

> The American public's resilience and support will be sustainable in the aftermath of future terrorist attacks only if expectations are clearly defined, attainable, and fulfilled' (WH 2003, p. 3).

> Our Nation's critical infrastructures are generally robust and resilient**.** These attributes result from decades of experience gained from responding to natural disasters, such as hurricanes and floods, and the deliberate acts of malicious individuals. The critical infrastructure sectors have learned from each disruption and applied those lessons to improve their protection, response, and recovery operations. Resilience is characteristic of most U.S. communities, and it is reflected in the ways they cope with natural disasters. (WH 2003, p. 9)

Resilience derives from the area of disaster management, and frames both the ability of self-organisation during disasters, and the psychological attitude towards their impact. In this logic, terrorism is just another disaster. Hence, the role of the government was described as the 'enabler'. Its task was to make an inventory, to establish incentives to encourage public-private partnerships tai-

lored to the specific needs of the private sector establish comprehensive policies and programs, take a role in development and transfer of technology, raise awareness e.g. through education, and establish stronger partnerships between local responders and service providers (p. 16). The DHS was tasked to be the coordinating agency, but also to assess threats and provide warnings. It was essentially modelled after the natural disaster responding agencies, along which 'every disruption or attack is a local problem' (ibid., p. 17, 19). The strategy of 2003 is a basic set of rules and state inventory and at times displaces the basics of civil rights (WH 2003, pp. 27-28). The strategy of 2006, in turn, provides an organisational framework and incorporated resilience as a mission goal:

> 'Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness**,** timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency' (DHS 2006, p. 9).

A long-term risk management approach was introduced (DHS 2006, p. 2). The NIPP of 2006 enforces a certain organisational structure in line with the National Preparedness Goals. Both the procedure and the goal are predecessors for the state and the local level to participate in the Federal grant program (ibid., p. 8). Again, the imminent threat of a terrorist attack is at the centre of CIP considerations. Resulting from this threat perception, the NIPP (DHS 2006, p. 10) stresses that the central tasks to counter this threat are: 'security-driven analyses, information sharing und unprecedented partnerships between the government and the private sector at all levels'. All three new approaches to security challenge the role of the central state as security provider and cause substantial organisational problems.

While the federal level cannot enforce regulations on the private sector, the state started to include the private sector in policy making from 2006. The Critical Infrastructure Partnership Advisory Council (CIPAC) was established as a Federal Advisory Committee. It ensures coordination between private and public entities, and engages in risk assessments, planning, the implementation of the National Infrastructure Protection Plan and operational activities (DHS 2009, p. 25). Other committees are appointed by DHS, such as the Homeland Security Advisory Council (HSAC), consisting of 'experts from state and local governments, public safety, security and first responder communities, academia and the private sector', the Private Sector Senior Advisory Committee, which is another subgroup of the HSAC, to provide 'expert advice from leaders in the private sector' (ibid.). Furthermore, there is the 'National Infrastructure Advisory Council', consisting of 30 members which are directly appointed

by the President, and the National Security Telecommunications Committee (NSTAC), also consisting of 30 members who advice the President directly (ibid.). As indicated by the name of the 2013 NIPP, 'Partnering for Critical Infrastructure Security and Resilience', the boards, platforms and advisory councils across the different levels became more integrated (DHS 2013).

The government on the other hand recognises that the private sector is constrained by 'risks-versus-consequences trade-offs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or within resource constraints' (DHS 2009, p. 24). Therefore, the government perceives its role mainly in providing knowledge of certain threat scenarios, and as an enabler. Enabling means reacting flexibly to the needs of certain branches, such as tailoring risk assessments more individually (Interview Brian Zawada, 25.8.2016). Furthermore, enabling includes the provision of platforms for exchanging experiences.

> 'Such additional actions reflect different levels of the public interest—some CIKR are critical to the national economy and to national well-being; some CIKR are critical to a State, locality, or region; some CIKR are critical only to the individual owner/operator or direct customer base. Actions to protect the public's interest that require investment beyond the level that those directly responsible for protection are willing and able to provide must be of sufficient priority to warrant the use of the limited resources that can be provided from public funding or may require regulatory action or appropriate incentives to encourage the private sector to undertake them.' (DHS 2009, p. 44)

The policy of 2013 stresses that owners and operators of CI usually include business continuity and emergency management plans. Further, resilience and redundancy shall be integrated into business processes of the private sector (DHS 2013, p. 46). Who is responsible for such investments appears not to be completely solved yet. At least, the importance of investments in infrastructure is stressed, albeit on a national (and not regional or individual) level: 'In this situation, public and private sector partners at all levels collaborate to address the security and resilience of national-level critical infrastructure, provide timely warnings, and promote an environment in which critical infrastructure owners and operators can carry out their specific responsibilities' (DHS 2013, p. 46).

Gradually, the risk environment moved from a narrow focus of terrorism to a much broader scale including extreme weather, pandemics, cyber threats, accidents and technical failures, as well as acts of terrorism (DHS 2013, p. 8). Along with the broadening of the threats, two additional policies were drafted comprehensibly to the update of 2013: the Climate Action Plan and the National Strategy for Information Sharing and Safeguarding' (DHS 2013, p. 9.). A tense web of private, public and private-

public councils on several state levels was woven around CI, as well as individual 'Information Sharing Organizations'.

## Conclusion

It was a specific conception of warfare that introduced security to a realm which formerly known as the sovereign issue of defence. When defence reacted on the requirements of a 'total war' concept by incorporating civil life into the military domain, the predecessor of National Security came along. As civil life became a target and a resource of warfare at the same time, passive/civil defence measures were introduced based on the concept of active defence. While active defence was based on deterrence, the resulting debates in the civil/passive defence department centred on sheltering or evacuation strategies. In this regard, the 'ideology of preparedness' came about as a special feature of US security.

A major shift took place when natural disasters were no longer perceived as a 'random act of God', but as a part of security, but also financial considerations. Disaster preparation became part of the civil defence effort. This rested on the assumption that effective action during times of emergencies is essentially a local task and depends on the local capabilities available, regardless of the specific source of the threat. The introduction of emergency management shifted threat-based assessments to risk-based ones, and implemented mitigation-based responses. This provided the foundation for resilience policies. The inauguration of FEMA institutionalised these new approaches and comprised security personnel and emergency management personnel in one agency. Yet, their relationship was uneasy, and different stages of security clearances led to divides and 'silo-thinking' within the agency. Later, the Department of Homeland Security, suffered from a similar problem.

When, during the 1990s, terrorism as new threat emerged, neither the Department of Defence nor FEMA felt responsible for domestic preparedness. Emergency preparedness was scattered and involved a whole range of independently acting governmental agencies. The plan to install a 'homeland defence' division was developed as a consequence of the shortcomings of such an approach. Homeland defence was designed to integrate the different state actors responsible for such a task, and, as a crucial task, also to integrate non-state actors. Homeland defence was an approach to reduce vulnerabilities and, as such, the first step in implementing the concept of a civil contingencies agency.

9/11 reinforced a protectionist stance. The result was the installation of the Department of Homeland Security. 22 government agencies were subsumed under this new department, which was modelled after the Department of Defence rather than a civil contingencies agency. This is a substantial difference. Whereas a security agency is naturally secretive and functions in a hierarchical fashion, a civil contingencies agency is more about coordinating, communicating to and integrating various sets of stakeholders. The focus after 9/11, however, was on terrorism, rather than other disasters. The conceptual basis 'prevent, protect, respond' let little room for risk-based approaches such as mitigation. When Hurricane Katrina hit, it was too late: the responses and respective outcomes showed what a complex crisis in an interconnected world looked like. Hence, Katrina triggered the introduction of resilience-based concepts.

Resilience essentially brought risk-based models back in. Mitigation and recovery became part of disaster management and the narrow focus on terrorism was broadened to include complex risks, such as pandemics, climate change and natural disasters. Yet, security was not replaced. Prevention and protection are still in the hands of the security division, while mitigation, response and recovery became the work of the 'Domestic Resilience Group'. Just during the mitigation phase, communities and the private sector are included in the preparation effort. Resilience is furthermore based on processes which were already used by the emergency management sector all along such as communication, information sharing and risk assessments.

Resilience, in contrast to protection, enables prioritisation and individualisation. Both is expressed in the critical infrastructure sector, were policies were drafted in accordance with the needs and possibilities of the private sector to ensure the public good in times of crisis. Furthermore, it is not a reactive concept, but a proactive one. Therefore, it also engages communities in order to enhance preparedness. As such it renders hitherto conception of a passive citizen-victim to an actively engaged citizen-survivor. A critical aspect in emergency management and security operations alike is communication before, during and after a crisis. Therefore, procedures of information sharing and a working communication system during crises (NIMS) were implemented to enable the inclusion of a broad range of actors. But the greatest advantage of resilience is that it enables conceptual learning, because it stresses adaption, and to actively shape adaption, as a fundamental feature. Therefore, it is quite possible that resilience – in different manifestations - has come to stay.

## Bibliography

Birkland, Thomas A. (2012). Federal Disaster Policy: Learning Priorities and Prospects for Resilience. Comfort, Luise, Boin, Arjen and Demchak, Chris (Ed.). Designing Resilience. Preparing for Extreme Events. Pittsburgh: University of Pittsburgh Press, pp. 106-129.

Boas, Ingrid and Delf Rothe (2016). From conflict to resilience? Explaining recent changes in climate security discourse and practice. Environmental Politics, 25:4, pp. 613-632.

Brown, Jared (2011). Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress. Congressional Research Service, CRS Report for Congress. https://fas.org/sgp/crs/homesec/R42073.pdf [access: 20/1/2017]

Caudle, Sharon (2005). Homeland Security Capabilities-Based Planning: Lessons from the Defense Community. Homeland Security Affairs, 1:2, pp. 1-21.

Chandler, David (2014). Beyond neoliberalism: resilience, the new art of governing complexity. Resilience: International Policies, Practices and Discourses, 2:1, pp. 47-63.

Collier, Stephen and Andrew Lakoff (2008). Distributed preparedness: the spatial logic of domestic security in the United Sates. Environment and Planning D: Society and Space, 26, pp. 7-28.

Collier, Stephen and Andrew Lakoff (2008a). The Vulnerability of Vital Systems: How "Critical Infrastructure" became a Security Problem. Dunn, Myriam and Kristian Soby Kristensen (Ed.), The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation. New York: Routledge.

Collier, Stephen and Andrew Lakoff (2015). Vital System Security: Reflexive Biopolitics and the Government of Emergency. Theory, Culture & Society, 32:2, pp. 19-51.

Corry, Olav (2014). From Defense to Resilience: Environmental Security beyond Neo-liberalism. International Political Sociology, 8:3, pp. 256-274,

Comfort, Louise (2005). Risk, Security, and Disaster Management. Annual Review Political Science 8, pp. 335-56.

Deutch, John, Arnold Kanter and Brent Scowcroft (2000). Strengthening the National Security Interagency Process. Carter, Ashton and John White (Ed.) Keeping the Edge. Cambridge: The MIT Press, pp. 265-285.

Crenshaw, Martha (2001). Counterterrorism policy and the political process. Studies in Conflict and Terrorism 24, pp. 329-337.

Department of Justice (2001). Patriot Act.
https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

DHS (2005). Homeland Security Budget in Brief, Fiscal Year 2005.

DHS (2006). National Infrastructure Protection Plan. Washington D.C.: Department of Homeland Security.

DHS (2006b). Civil Defense and Homeland Security: A short History of National Preparedness Efforts. Homeland Security National Preparedness Task Force. Washington D.C.: Department of Homeland Security.

DHS (2006c). Homeland Security Advisory Council. Report of the Critical Infrastructure Task Force. Washington D.C.: Department of Homeland Security.

DHS (2007). National Preparedness Guidelines. Washington D.C.: Department of Homeland Security.

DHS (2009). National Infrastructure Protection Plan. Partnering to enhance protection and resiliency. Washington D.C.: Department of Homeland Security.

DHS (2013). National Infrastructure Protection Plan. Partnering for Critical Infrastructure Security and Resilience. Washington D.C.: Department of Homeland Security.

Evans, Brad and Julian Reid (2014). Resilient Life: The Art of Living Dangerously. Cambridge: Polity Press.

Huysmans, Jef (2014). Security Unbound: Enacting Democratic Limits. London, New York: Routledge.

Falkenrath, Richard (2000). Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack. International Security, 25:4, pp 147-186.

FEMA (2011). A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action. Washington D.C.: Federal Emergency Management Agency.

HSDP (2003). Homeland Security Presidential Directive/HSPD-8 – National Preparedness. Washington D.C.: The White House.

Jenkins, Brian (2006). Unconquerable Nation. Knowing Our Enemy, Strengthening Ourselves. Santa Monica: RAND Cooperation.

Kaufmann, David, Bach, Robert and Jorge Riquelme (2015). Engaging the Whole Community in the United States. Bach, Robert (Ed.) Strategies for Supporting Community Resilience. Stockholm: Elanders Sverige AB, pp. 151-187.

Lakoff, Andrew and Stephen Collier (2009). Infrastructure and Event: The Political Technology of Preparedness. Braun, Bruce and Sarah Whatmore (Ed.). *The Stuff of Politics: Technoscience, Democracy, and Public Life.* Minnesota: University of Minnesota Press, pp. 243-266.

Lesser, Ian (1999). Countering the New Terrorism: Implications for Strategy. Lesser, Ian, Hoffman, Bruce, Arquilla, John, Ronfeldt, David, Zanin, Michelle (Ed.). Countering the New Terrorism. Washington D.C.: RAND Cooperation, pp. 85-142.

Moynihan, Donald P. (2009): The Response to Hurricane Katrina. International Risk Governance Council Case Study, Geneva. https://irgc.org/wp content/uploads/2012/04/Hurricane_Katrina_full_case_study_web.pdf [accessed: 20/1/2017]

Oakes, Guy (1994). The Imaginary War: Civil Defence and American Cold War Culture. Oxford: Oxford University Press.

OECD DAC (2011). Supporting Statebuilding in Situations of Conflict and Fragility: Policy Guidance. Paris: OECD.

Roberts, Patrick S. (2012). Private Choices, Public Harms. The Evolution of National Disaster Organizations in the United States. Lakoff, Andrew (Ed.). Disaster and the Politics of Intervention. Columbia: Columbia University Press, pp. 42-69.

Roberts, Alasdair (2010). Building Resilience: Macrodynamic Constraints on Governmental Response to Crisis. Comfort, Luise, Boin, Arjen and Demchak, Chris (Ed.). Designing Resilience. Preparing for Extreme Events. Pittsburgh: University of Pittsburgh Press, pp. 84-106.

Selchow, Sabine (2016). Resilience and resilient in Obama's National Security Strategy 2010: Enter two 'political keywords'. Politics, pp. 1-16.

Stampnitzky, Lisa (2013). Disciplining Terror. How Experts Invented "Terrorism". Cambridge: Cambridge University Press.

Sylves, Richard and William Cumming (2004). FEMA's Path to Homeland Security 1979-2003. Journal of Homeland Security and Emergency Management, 1:2, pp. 1-21.

Wayne, Blancard (1986). American Civil Defense 1945-1984. The Evolution of Programs and Policies. National Emergency Center Emmitsburg, Maryland, Monograph Series 1985, Vol 2. Nr. 2.

White House (1987). National Security Strategy of the United States. Washington D.C.: The White House.

WH (1987). National Security Strategy of the United States. Washington D.C.: The White House.

WH (1994). A National Security Strategy of Engagement and Enlargement. Washington D.C.: The White House.

WH (1998). A National Security Strategy for a New Century. Washington D.C.: The White House.

WH (2002). The National Security Strategy of the United States of America. Washington D.C.: The White House.

WH (2002a). The National Strategy For Homeland Security. Washington D.C.: The White House.

WH (2011). National Strategy for Counterterrorism. Washington D.C.: The White House.

WH (2010). National Security Strategy. Washington D.C.: The White House.

WH (2015). National Security Strategy. Washington D.C.: The White House.

**Interviews:**

Interview Brian Zawada, Skype, 25.8.2016.

Interview Jef Gaynor, Skype, 1.9.2016.

Interview Lisa Orloff, Skype, 15.8.2016.